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
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/registrator/

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

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

---

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):

<table>
<thead>
<tr>
<th>Organization</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICANN</td>
<td><a href="http://www.icann.org">http://www.icann.org</a></td>
</tr>
<tr>
<td>AfriNIC</td>
<td><a href="http://www.afrinic.net/">http://www.afrinic.net/</a></td>
</tr>
<tr>
<td>APNIC</td>
<td><a href="http://www.apnic.net">http://www.apnic.net</a></td>
</tr>
<tr>
<td>ARIN</td>
<td><a href="http://www.arin.net">http://www.arin.net</a></td>
</tr>
<tr>
<td>European Registry of Internet Domain Names (EURid)</td>
<td><a href="http://www.eurid.eu/">http://www.eurid.eu/</a></td>
</tr>
<tr>
<td>LACNIC</td>
<td><a href="http://lacnic.net/en">http://lacnic.net/en</a></td>
</tr>
<tr>
<td>RIPE</td>
<td><a href="http://www.ripe.net">http://www.ripe.net</a></td>
</tr>
</tbody>
</table>

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

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." IPv6 migration will happen—it's only a matter of when, not if.

IPv6 Information Page

http://www.ipv6.org/

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 (TLDs) .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 registries around the world

The list below contains the two-letter TLDs according to IANA's 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.

```plaintext
TLDs  | .au | .at | .be | .bg | .by | .cz | .de | .dk | .ee | .es | .fi | .fr | .gb | .gr | .hu | .ie | .in | .int | .it | .jp | .kr | .lt | .lu | .lv | .mc | .md | .me | .mg | .mk | .ml | .mn | .mr | .ms | .mt | .nu | .no | .nl | .pl | .pt | .qa | .ro | .ru | .sa | .sc | .se | .si | .sk | .sl | .sn | .so | .sr | .st | .su | .sv | .tk | .tj | .tm | .tn | .to | .tr | .tt | .tw | .tz | .ua | .uk | .us | .uy | .uz | .va | .ve | .vi | .vn | .za | .zm | .zw
```

### Domain Name Registries Around the World

- [http://www.norid.no/domenenavnbaser/domreg.html](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

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 inter-
communicating computers, known as name servers, that translate domain names to IP addresses and vice versa.

**NSLookup Tools**

- Check DNS: [http://www.checkdns.net/quickcheck.aspx](http://www.checkdns.net/quickcheck.aspx)
- Multiple NSLookup: [http://www.bankes.com/nslookup.htm](http://www.bankes.com/nslookup.htm)
- SmartWhois NSLookup: [http://www.swhois.net/](http://www.swhois.net/)
- Squish DNS Lookup: [http://www.squish.net/dnscheck/](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](http://www.webreference.com/cgi-bin/nslookup.cgi)

**ZoneEdit NSLookup**


---

**NSLookup**

This DNS utility is provided by ZoneEdit.Com, the industry leader in DNS and domain management 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):
   [ ]
   (IE: 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/cqi-bin/whois

**AfriNIC Database User Manual**
http://www.afrinic.net/docs/db/afsup-dbqs200501.htm

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

**LACNIC Whois**
http://lacnic.net/cqi-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**  
**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 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

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

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

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

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 mail servers about authoritative NS for domain

Got DNS list for 'mfa.gov.ir' from ns.nic.ir or ns.nic.id
1 Found NS record: web-srv.mfa.gov.ir[82.100.96.245], was resolved to IP address by ns.nic.id or ns.nic.id or ns.nic.id
2 Found NS record: irserv1.iredco.com[194.165.0.10], was resolved to IP address by ns.nic.id
✓ Domain has 2 DNS servers

CheckDNS.NET is verifying if NS are alive
1 Error fetching SOA from web-srv.mfa.gov.ir[82.100.96.245], request timed out. Probably DNS server is offline.
2 DNS server irserv1.iredco.com[194.165.0.10] is alive and authoritative for domain mfa.gov.ir
✓ 1 server(s) are alive
2 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
✓ 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
1 Checking HTTP server www.mfa.gov.ir [217.172.99.246]
✓ Received: HTTP/1.1 200 OK (Server: Microsoft-IIS/6.0). Welcome to Ministry of Foreign Affairs of I.R of Iran. H2

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

CheckDNS.NET tests mail-servers
✓ Domain mfa.gov.ir has only one mail-server
1 Checking mail server [PRI=10] email.mfa.gov.ir[194.165.0.14]
✓ 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
1 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 smithsonian 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. 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 smithsonian 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

Domain Tools and 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 domain.

- **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**
  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 uri 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;

---

- 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 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

Website Title: ~amazon.com: Online Shopping for Electronics, Apparel, 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:

Related Sites:

Indexed Data

DMOZ: 112 listings
Alexa Trend/Rank: 19 (1 Month) 18 (3 Month)
YI Directory: 39 listings

Server Data

Server Type: Server
IP Address: 72.21.206.5
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

Domain Tools 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: 973 records have been archived since 2000-04-01
Reverse IP: 122 other sites hosted on this server.

Whois Record

Registrant:
Amazon.com, Inc
Legal Dept., P.O. Box 81226
Seattle, WA 98109-1226
US

Domain Name: AMAZON.COM
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.

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.

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 lasing lave] 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 parkavenu 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.
parking 'ave - Domain Search

Advanced Search

<table>
<thead>
<tr>
<th>Query:</th>
<th>Parking 'ave</th>
<th>Domain Length:</th>
<th>25</th>
<th>Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Numbers:</td>
<td>N</td>
<td>Hyphens:</td>
<td>N</td>
<td>Yes</td>
</tr>
<tr>
<td>Order:</td>
<td>Left Anchor</td>
<td>Right Anchor</td>
<td>N</td>
<td>Keep Word Order</td>
</tr>
<tr>
<td>Adult Filter:</td>
<td>N</td>
<td>Off</td>
<td>Show:</td>
<td>Active only</td>
</tr>
<tr>
<td>Search Results</td>
<td>20,387 results found in 0.045348 seconds.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Did you mean to search for parking 'ave?

<table>
<thead>
<tr>
<th>Domain</th>
<th>.com</th>
<th>.net</th>
<th>.org</th>
<th>.info</th>
<th>.biz</th>
<th>.us</th>
</tr>
</thead>
<tbody>
<tr>
<td>park</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>park0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>park07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>park077</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>park072</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>park0702</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>park0709</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>park0720</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>park07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>park1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>park10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>park100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>park1000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Domains for Sale

<table>
<thead>
<tr>
<th>Domain</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>AveDaRk.com</td>
<td>$50.00</td>
</tr>
<tr>
<td>FoxAve.com</td>
<td>$200.00</td>
</tr>
<tr>
<td>TopAve.com</td>
<td>$250.00</td>
</tr>
<tr>
<td>LinkAve.com</td>
<td>$295.00</td>
</tr>
<tr>
<td>FastAve.com</td>
<td>$400.00</td>
</tr>
<tr>
<td>AveBu.com</td>
<td>$700.00</td>
</tr>
<tr>
<td>HD4ve.com</td>
<td>$941.00</td>
</tr>
<tr>
<td>PetAve.com</td>
<td>$1,000.00</td>
</tr>
<tr>
<td>AudioAve.com</td>
<td>$1,000.00</td>
</tr>
</tbody>
</table>

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?

Whoix? Advanced Search

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/

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
  [D]emon.co.uk

- Examine the DNS Data on a Particular Domain
  [D]emon.net

- Generic Whois Lookup on Domain / IP Address
  [D]emon.nl

- Query the InterNIC (Domain Registry/Whois) Database
  [D]emon.net

- Lookup a .CO.UK/ORG.UK Domain in the UK Database
  [G]reenpeace.org.uk

- Query the RIPE Database
  193.193.1.1

- Show DNS Data on an Individual Host
  [S]ample.demon.co.uk

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

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

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

[begin response]

HTTP/1.1 200 OK
Date: Wed, 17 Nov 2004 17:56:44 GMT
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</title>
<link rel="stylesheet" href="http://us.i1.yimg.com/us.yimg.com/lib/s/ysch_hp_041018.css" type="text/css">
<style>em {font:normal 100% arial;display:block;}</style>
</head>
<body>
<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.
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, kaspersky.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:
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 01.176.69.78

Domain Whois record
Queried whois.ripn.net with "avp.ru"...
1) By submitting a query to RIPE's Whois Service
2) you agree to abide by the following terms of use:
3) http://www.ripe.net/about/servpol.html#3.2 (in Russian)
4) http://www.ripe.net/about/en/servpol.html#3.2 (in English).

domain: AVP.RU
type: CORPORATE
nservers: ns1.kasperskylabs.net.
nserver: ns2.kasperskylabs.net.
nserver: ns3.gidn.net.
state: REGISTERED, DELEGATED
org: Joint Stock Company
org: "Kaspersky Lab"
phone: +7 095 7978700
phone: +7 095 7978701
fax-no: +7 095 9484331
fax-no: +7 095 9494331
e-mail: vemaaster@avp.ru
e-mail: sales@kaspersky.com
e-mail: support@kaspersky.com
registrar: AGREETER-REC-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 kaspersky.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-LABS
descr:        Kaspersky Labs
descr:        Garoyev Panfilovtsev St., 10 Moscow, 123363, RU
country:      RU
admin-c:      SF1624-RIPE
tech-c:       SF1624-RIPE
status:       ASSIGNED PA
notify:       registry@rt.ru
notify:       iasw@kaspersky.com
mnt-by:       AS19342-INT
changed:      luda@st.ru 20030730
source:       RIPE

route:        81.176.0.0/15
descr:        RTCOMM-RU
origin:       AS19342
notify:       noc@tccom.ru
mnt-by:       AS19342-INT
changed:      rus@ct.ru 20030120
changed:      rus@ct.ru 20031105
changed:      rus@ct.ru 20040809
source:       RIPE

person:     Sergey Foamin
address:     System Administrator /Kaspersky Lab Ltd
address:     10, Garoyev Panfilovtsev Str.,
address:     123363, Moscow, Russia
e-mail:      sergey@kaspersky.com
phone:       +7 095 727 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).
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.

**DNS records**

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data:</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>avp.ru</td>
<td>IN</td>
<td>A</td>
<td>81.176.69.78</td>
<td>3600s (01:00:00)</td>
</tr>
<tr>
<td>avp.ru</td>
<td>IN</td>
<td>MX</td>
<td>preference: 10 exchange: sf.kaspersky.com</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>avp.ru</td>
<td>IN</td>
<td>MX</td>
<td>preference: 400 exchange: relay1.macomnet.ru</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>avp.ru</td>
<td>IN</td>
<td>MX</td>
<td>preference: 500 exchange: relay2.macomnet.ru</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>avp.ru</td>
<td>IN</td>
<td>NS</td>
<td>ns.kasperskylabs.net</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>avp.ru</td>
<td>IN</td>
<td>NS</td>
<td>ns1.kasperskylabs.net</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>avp.ru</td>
<td>IN</td>
<td>NS</td>
<td>ns.macomnet.ru</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>avp.ru</td>
<td>IN</td>
<td>NS</td>
<td>ns2.gldn.net</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>avp.ru</td>
<td>IN</td>
<td>NS</td>
<td>ns3.gldn.net</td>
<td>86400s (1.00:00:00)</td>
</tr>
<tr>
<td>78.69.176.81.in-addr.arpa</td>
<td>IN</td>
<td>CNAME</td>
<td>78.64/26.69.176.81.in-addr.arpa</td>
<td>86399s (23:59:59)</td>
</tr>
<tr>
<td>78.64/26.69.176.81.in-addr.arpa</td>
<td>IN</td>
<td>PTR</td>
<td>proxy2.ru.kaspersky-labs.com</td>
<td>86400s (1.00:00:00)</td>
</tr>
</tbody>
</table>
CheckDNS.NET is testing kaspersky.com

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

Get DNS list for kaspersky.com from a good servers net

- Found NS record: kasperskylabs.net[195.170.248.13] was resolved to IP address by a good servers net.
- Found NS record: kasperskylabs.net[212.5.80.3] was resolved to IP address by a good servers net.
- Domain has 2 DNS servers.

**CheckDNS.NET is testing if NS are alive**

- DNS server ns2.kaspersky.com[212.5.80.3] is alive and authoritative for domain kaspersky.com.
- 2 servers are alive.

**CheckDNS.NET checks if all NS have the same version**

- All 2 servers have the same zone version 2004092021.

**CheckDNS.NET is testing if NS are alive**

- NS list manually, registration authority reports that domain is hosted on the following servers: ns1.kaspersky.com[195.170.248.13], ns2.kaspersky.com[212.5.80.3], ns3.gidn.net, ns4.gidn.net, ns5.kaspersky.com[212.5.80.3]. Please make sure that you configure the same DNS servers in registration database and on your DNS.

**CheckDNS.NET verifyst.evers.net**

- Checking HTTP server www.kaspersky.com[61.176.69.78].

**CheckDNS.NET tests mail-servers**

- Domain kaspersky.com has 3 mail-servers:
  - Checking mail server (PRI=10) of kaspersky.com[212.5.80.6].
  - Mail server of kaspersky.com[212.5.80.6] answers on port 25.
  - 220 at kaspersky.com ESMTP service ready
  - HELO www.checkdns.net
  - 250 at kaspersky.com
  - MAIL FROM: <check@uniplace.com>
  - 250 Ok
  - RCPT TO: <postmaster@kaspersky.com>
  - 250 Ok
  - QUIT

- Mail server of kaspersky.com[212.5.80.1] accepts mail to kaspersky.com.
  - Checking mail server (PRI=110) relay=maconnet.ru[195.126.64.2].
  - Mail server relay=maconnet.ru[195.126.64.2] answers on port 25.
  - 220 mail@maconnet.ru ESMTP Sendhul 8 12 10/6 12 19. Thu, 8 Feb 2001 20:25:11 -0200 (MST)
  - HELO www.checkdns.net
  - 250 relay=maconnet.ru with MIB [195.60.98.252], clearence to meet you
  - MAIL FROM: <check@uniplace.com>
  - 250 2 1 0 <check@uniplace.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.macornnet.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

<table>
<thead>
<tr>
<th>hop</th>
<th>rtt</th>
<th>rtt</th>
<th>ip address</th>
<th>fully qualified domain name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>216.46.228.229</td>
<td>port-216-3073253-es128.devices.datareturn.com</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>64.29.192.145</td>
<td>port-64-1949841-2zt0prespect.devices.datareturn.com</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>64.29.192.226</td>
<td>daa.g921.ispb.datareturn.com</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>168.215.241.133</td>
<td>haag-01-a0-1001.dfw.twtelecom.net</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>66.192.253.124</td>
<td>core-02-ge-0-3-1-504.dfw.twtelecom.net</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>168.215.54.74</td>
<td>tran-02-ge-0-3-0-0.dfw.twtelecom.net</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>2</td>
<td>160.81.227.105</td>
<td>sl-gw40-fw-4-2.sprintlink.net</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>2</td>
<td>144.232.8.245</td>
<td>sl-bb21-fw-4-3.sprintlink.net</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>2</td>
<td>144.232.11.217</td>
<td>sl-bb20-fw-14-0.sprintlink.net</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>3</td>
<td>144.232.20.17</td>
<td>sl-st21-dal-1-0.sprintlink.net</td>
</tr>
<tr>
<td>11</td>
<td>3</td>
<td>3</td>
<td>144.232.9.134</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>3</td>
<td>3</td>
<td>152.63.97.57</td>
<td>0.so-1-0-0.xx1.dfw9.alter.net</td>
</tr>
<tr>
<td>13</td>
<td>3</td>
<td>3</td>
<td>152.63.0.193</td>
<td>0.so-0-0-0.t1.dfw9.alter.net</td>
</tr>
<tr>
<td>14</td>
<td>36</td>
<td>36</td>
<td>152.63.9.193</td>
<td>0.so-7-0-0.xl1.dca6.alter.net</td>
</tr>
<tr>
<td>15</td>
<td>36</td>
<td>36</td>
<td>146.188.13.38</td>
<td>so-1-0-0.ir1.dca4.alter.net</td>
</tr>
<tr>
<td>16</td>
<td>123</td>
<td>123</td>
<td>146.189.8.162</td>
<td>so-5-0-0.tr1.fft1.alter.net</td>
</tr>
<tr>
<td>17</td>
<td>123</td>
<td>123</td>
<td>146.188.8.141</td>
<td>so-0-1-0.xr2.fft4.alter.net</td>
</tr>
<tr>
<td>18</td>
<td>123</td>
<td>123</td>
<td>149.227.48.30</td>
<td>pos6-0.gw9.fft4.alter.net</td>
</tr>
<tr>
<td>19</td>
<td>168</td>
<td>168</td>
<td>139.4.174.210</td>
<td>macomnet.frankfurt1.de.alter.net</td>
</tr>
<tr>
<td>20</td>
<td>168</td>
<td>168</td>
<td>195.128.64.80</td>
<td>ncc-3-eth-100.msk.macomnet.net</td>
</tr>
<tr>
<td>21</td>
<td>179</td>
<td>170</td>
<td>195.128.75.89</td>
<td>macom-i010301193-lab.kasper.macomnet.net</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>AS Number</th>
<th>[8342]</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC (optional)</td>
<td></td>
</tr>
<tr>
<td>Search</td>
<td></td>
</tr>
</tbody>
</table>

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

**Results from Reseaux IP Europeans**

<table>
<thead>
<tr>
<th>Registrant</th>
<th>RTComm.RU Autonomous System Moscow, Russia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Contact</td>
<td>F.T.PL</td>
</tr>
<tr>
<td>Tech Contact</td>
<td>F.T.PL</td>
</tr>
<tr>
<td>Maintainer Contact</td>
<td>AS8342: MNT</td>
</tr>
</tbody>
</table>

from AS702 146 188 66 49 at 195.161.1.152 action pref=200; from AS702 146 186 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

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
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:\(^{156}\)


\(^{156}\) The Internetipaddress.com website is currently unavailable.
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.

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 node (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).

<table>
<thead>
<tr>
<th>Node</th>
<th>Time 1</th>
<th>Time 2</th>
<th>Time 3</th>
<th>Country/Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0 ms</td>
<td>0 ms</td>
<td>0 ms</td>
<td>67.16.26.185</td>
</tr>
<tr>
<td>2</td>
<td>0 ms</td>
<td>0 ms</td>
<td>0 ms</td>
<td>68.41.225.73</td>
</tr>
<tr>
<td>3</td>
<td>0 ms</td>
<td>0 ms</td>
<td>0 ms</td>
<td>15.74.140.10</td>
</tr>
<tr>
<td>4</td>
<td>1 ms</td>
<td>1 ms</td>
<td>1 ms</td>
<td>70.85.127.74</td>
</tr>
<tr>
<td>5</td>
<td>0 ms</td>
<td>0 ms</td>
<td>0 ms</td>
<td>70.85.127.5</td>
</tr>
<tr>
<td>6</td>
<td>1 ms</td>
<td>1 ms</td>
<td>1 ms</td>
<td>64.210.104.67</td>
</tr>
<tr>
<td>7</td>
<td>32 ms</td>
<td>32 ms</td>
<td>32 ms</td>
<td>67.17.67.94</td>
</tr>
<tr>
<td>8</td>
<td>32 ms</td>
<td>32 ms</td>
<td>33 ms</td>
<td>206.50.13.152</td>
</tr>
<tr>
<td>9</td>
<td>45 ms</td>
<td>45 ms</td>
<td>45 ms</td>
<td>213.248.80.74</td>
</tr>
<tr>
<td>10</td>
<td>141 ms</td>
<td>141 ms</td>
<td>141 ms</td>
<td>213.249.84.33</td>
</tr>
<tr>
<td>11</td>
<td>142 ms</td>
<td>142 ms</td>
<td>142 ms</td>
<td>213.249.64.1</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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)
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.\textsuperscript{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.

TraceRoute to host thing.net

Timeout 5
Start from hop 1
Maximum Hops 30

<table>
<thead>
<tr>
<th>#</th>
<th>Address</th>
<th>Host Name</th>
<th>Msg Type</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>193.156.142.213</td>
<td>Unavailable</td>
<td>TTL Exceeded</td>
<td>33 ms</td>
</tr>
<tr>
<td>2</td>
<td>217.5.112.254</td>
<td>Unavailable</td>
<td>TTL Exceeded</td>
<td>302 ms</td>
</tr>
<tr>
<td>3</td>
<td>194.25.7.175</td>
<td>KN-nqi.KN.net.OTAG.DE</td>
<td>TTL Exceeded</td>
<td>31 ms</td>
</tr>
<tr>
<td>4</td>
<td>212.185.11.129</td>
<td>KN-gwi.KN.net.OTAG.DE</td>
<td>TTL Exceeded</td>
<td>37 ms</td>
</tr>
<tr>
<td>5</td>
<td>212.185.8.177</td>
<td>F-gwi.F.net.OTAG.DE</td>
<td>TTL Exceeded</td>
<td>37 ms</td>
</tr>
<tr>
<td>6</td>
<td>194.25.6.110</td>
<td>NYC-gwi2.USA.net.OTAG.DE</td>
<td>TTL Exceeded</td>
<td>141 ms</td>
</tr>
<tr>
<td>7</td>
<td>194.25.6.90</td>
<td>dc.nyc1.verio.net</td>
<td>TTL Exceeded</td>
<td>141 ms</td>
</tr>
<tr>
<td>8</td>
<td>129.250.16.210</td>
<td>p1-0-0-0.cgo.nycnmy02.us.ca.verio.net. TTL Exceeded</td>
<td>146 ms</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>129.250.126.137</td>
<td>d3-0-1-0.a03.nycnmy05.us.ca.verio.net. TTL Exceeded</td>
<td>147 ms</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>209.14.148.161</td>
<td>fa-5-0.a00.nycnmy05.us.ca.verio.net. TTL Exceeded</td>
<td>153 ms</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>209.217.40.182</td>
<td>thing-gv.spacelab.net</td>
<td>TTL Exceeded</td>
<td>156 ms</td>
</tr>
<tr>
<td>12</td>
<td>209.14.143.4</td>
<td>thing.net</td>
<td>Echo Reply</td>
<td>157 ms</td>
</tr>
</tbody>
</table>

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.gu.com [64.12.187.22] over a maximum of 30 hops:

<table>
<thead>
<tr>
<th>Hop</th>
<th>Time (ms)</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>18</td>
<td>18</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>4</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>6</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>8</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>9</td>
<td>* Request timed out</td>
<td></td>
</tr>
</tbody>
</table>

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 gu-crann1.nerc.logix.cs (217.11251.284) 0.347 ms 0.000 ms 0.000 ms
2 24.0.255.5 0.348 ms 0.000 ms 0.000 ms
3 TH-HE10-get-0-3.com.ip-anywhere.net (217.11254.224) 1.689 ms 2.577 ms 1.683 ms
4 oxz.interoute.cz (194.50.100.127) 0.779 ms 5.694 ms 0.501 ms
5 P06-0.prg-001-access-1.interoute.net (212.23.50.77) 36.447 ms 37.910 ms 36.427 ms
6 P010-0.fm-006-core-2.interoute.net (212.23.50.70) 231.174 ms 233.089 ms 219.003 ms
7 P06-0.0w-001-access-1.interoute.net (84.233.146.13) 45.621 ms 36.716 ms 36.627 ms
8 P07-0.lan-001-access-1.interoute.net (84.233.146.10) 36.040 ms 36.687 ms 36.540 ms
9 P06-0.poo-002-access-1.interoute.net (84.233.146.15) 36.635 ms 36.877 ms 36.512 ms
10 P09-0.slo-002-access-2.interoute.net (212.23.43.73) 37.064 ms 36.947 ms 36.612 ms
11 P09-0.slo-002-access-1.interoute.net (212.23.43.69) 36.522 ms 36.570 ms 36.550 ms
12 84.233.146.16 38.608 ms 37.867 ms 38.036 ms
13 Vian102-g0-1.e.3-sthl.net.1onip.ru (195.7.95.116) 38.973 ms 38.901 ms 38.424 ms
14 194.88.115.226 63.148 ms 65.553 ms 62.652 ms
15 Vian1-c5高手.1onip.ru (213.152.128.79) 61.280 ms 63.313 ms 63.261 ms
16 ronitors-gu.1onip.ru (213.152.129.94) 81.480 ms 62.137 ms 80.945 ms
```

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:

<table>
<thead>
<tr>
<th>Hop</th>
<th>Time</th>
<th>Time</th>
<th>Time</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>&lt;10 ms</td>
<td>&lt;10 ms</td>
<td>&lt;10 ms</td>
<td>186.217.33.1</td>
</tr>
<tr>
<td>2</td>
<td>60 ms</td>
<td>70 ms</td>
<td>60 ms</td>
<td>rtr-2.confusion.net [186.40.64.94]</td>
</tr>
<tr>
<td>3</td>
<td>70 ms</td>
<td>71 ms</td>
<td>70 ms</td>
<td>rtr-1.confusion.net [186.40.64.93]</td>
</tr>
<tr>
<td>4</td>
<td>60 ms</td>
<td>70 ms</td>
<td>60 ms</td>
<td>rtr-2.confusion.net [186.40.64.94]</td>
</tr>
<tr>
<td>5</td>
<td>70 ms</td>
<td>70 ms</td>
<td>70 ms</td>
<td>rtr-1.confusion.net [186.40.64.93]</td>
</tr>
<tr>
<td>6</td>
<td>60 ms</td>
<td>70 ms</td>
<td>61 ms</td>
<td>rtr-2.confusion.net [186.40.64.94]</td>
</tr>
<tr>
<td>7</td>
<td>70 ms</td>
<td>70 ms</td>
<td>70 ms</td>
<td>rtr-1.confusion.net [186.40.64.93]</td>
</tr>
<tr>
<td>8</td>
<td>60 ms</td>
<td>70 ms</td>
<td>60 ms</td>
<td>rtr-2.confusion.net [186.40.64.94]</td>
</tr>
<tr>
<td>9</td>
<td>70 ms</td>
<td>70 ms</td>
<td>70 ms</td>
<td>rtr-1.confusion.net [186.40.64.93]</td>
</tr>
</tbody>
</table>

... ...

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 gu-casa@blanca.logix.cz (217.11.251.254) 0.000 ms 0.000 ms 0.000 ms
2 81.0.225.5 0.408 ms 1.803 ms 0.855 ms
3 vip.com.ip-anywhere.net (217.11.224.240) 1.005 ms 2.848 ms 0.490 ms
4 ** ** **
5 ** ** **
6 ** ** **
7 ** ** **
8 ** ** **
9 vip.com.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.*
The private address 10.1.2.5 in 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.
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.

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  

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  

Multiple Traceroute Gateway  
http://www.tracert.com/cgi-bin/trace.pl

UNCLASSIFIED//FOR OFFICIAL USE ONLY

494
New York Internet Traceroute Links
Opus One Traceroute
SixXs IPv4 and IPv6 Traceroute
Traceroute.org
Tracerouters Around the World
BGPNet IPv4 Wiki
BGPNet IPv6 Wiki

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

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Traceroute IPv6</th>
<th>Run</th>
</tr>
</thead>
</table>

**Logix.cz IPv6 site**

Convert address to nibble format for DNS

<table>
<thead>
<tr>
<th>Address</th>
<th>Convert</th>
</tr>
</thead>
</table>

```
traceroute to 3ffe:ffff:1234 (3ffe:ffff:1234), 30 hops max, 40 byte packets
1 casablanca.ipv6.logix.cz (2001:1528:104:3::ffff)  6.074 ms  0.000 ms  0.000 ms
3 tech.ipv4.cas.ip-anywhere.net (2001:1528::100)  1.170 ms  1.567 ms  1.427 ms
4 casablanca.ipv6.logix.cz (2001:1528:106::1)  1.659 ms  3.038 ms  1.216 ms
5 tech.ipv4.cas.ip-anywhere.net (2001:1528::100)  2.176 ms  2.047 ms  2.151 ms
6 * * *
7 * * *
8 * tech.ipv6.cas.ip-anywhere.net (2001:1528::100)  1.737 ms  *
9 * tech.ipv6.cas.ip-anywhere.net (2001:1528::100)  1.737 ms  *
10 * * *
11 * * *
13 tech.ipv4.cas.ip-anywhere.net (2001:1528::100)  4.121 ms  3.319 ms  4.200 ms
15 tech.ipv4.cas.ip-anywhere.net (2001:1528::100)  4.714 ms  3.577 ms  3.351 ms
16 * * *
17 * * *
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


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

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

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:

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.

The following results were generated using GeoSelect version II.

Address to locate: 212.5.80.6

| Country Code | City | Latitude | Capital City | Longitude | TimeZone | Population | Currency Code | Currency
|--------------|------|----------|--------------|-----------|----------|------------|--------------|---------
| RU           | RU   | 55.7500  | Moscow       | 37.5830   | +03:00   | 145470197  | RUB          | Russian Ruble

Distance to Nearby Cities

0 0 Moscow, MC, RU
34 21 Tver, MS, RU
55 28 Konakovo, MS, RU

Geobytes IP Locator

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
If you want to see the original site where Geobytes began collecting its data, visit NetWorldMap.

**NetWorldMap**
http://www.networldmap.com/Trylt.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).

---

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

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.
IP2Location


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.

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

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.
The following nine ISP associations are Members of EuroISPA:

- AEPI: Asociacion Española de Proveedores de Servicios de Internet
- AEA: Association des Fournisseurs d'Acces et de Services Internet
- AIP: Associazione Italiana Internet Providers
- ISPA Austria: Internet Service Providers Austria
- ECOS: Verband der deutschen Internetwirtschaft

Here are the members of the ISP Association of Ireland

http://www.euroispa.org/32.htm
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](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.

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

The Internet Service Providers’ Association of South Africa

Africa Top Level Domains (AFTLD) Members

Internet Service Providers’ Association of Nigeria

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

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":

506
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.


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

African Internet Connectivity

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.


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.satsiq.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/

AR Riyadh, Saudi Arabia

Hotspot Finder

10 locations found

Home page & Search

Search locations by Wi-Fi access

Search for selected Wi-Fi access

Intel's Mobile Technology Hotspot Finder

- Home - Search Results
- AR Riyadh, Saudi Arabia
- Search locations by Wi-Fi access
- Search for selected Wi-Fi access

Location (A-Z)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Al-Faisaliah Tower - Alaa Adden

Hotspot Detail

Al-Faisaliah Tower - Alaa Adden
King Fahd Road
Riyadh, Al Riyadh 11669

Location Type:

Restaurant

Access Type:

Independent Provider

Wi-Fi Hotspot List

http://www.wi-fihotspotlist.com/

Hotspotpothaven

http://www.hotspotpothaven.com/

JiWire Global WiFi Hotspot Finder

http://www.jiwire.com/search-hotspot-locations.htm

WiFinder

http://www.wifinder.com/

WiFi411

http://www.wifi411.com/

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:

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

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.

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:
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.

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.

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  
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]

Scott MacNealy's now-infamous quote,—"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." 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."  

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.

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." 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." 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."

Security experts believe most spam—in fact more than 80 percent—is now sent by bots. 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. 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"

---


167 Markoff.

168 Markoff.

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.\textsuperscript{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."\textsuperscript{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\% of e-mail, and has continued its growth each month since May of this year [2004].\textsuperscript{172} December 2006 saw a new record: according to one tracking system, spam accounted for 94\% of all email that month.\textsuperscript{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.


✓ 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://gemai.dk/browserspy/]
Russ Haynal’s Persona Check [http://navigators.com/cgi-bin/navigators/persona.pl]
   especially the Browser Leakage and Quick Scan for open ports
   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:

<table>
<thead>
<tr>
<th>Pushchino Radio Astronomy Observatory, Russia, Access Statistics:</th>
<th><a href="http://psun32.prao.pn.university.html">http://psun32.prao.pn.university.html</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>0.03 0.06 82579</td>
<td>15</td>
</tr>
<tr>
<td>0.03 0.03 38850</td>
<td>17</td>
</tr>
<tr>
<td>0.01 0.02 29682</td>
<td>6</td>
</tr>
<tr>
<td>0.00 0.01 10854</td>
<td>2</td>
</tr>
<tr>
<td>0.00 0.02 20170</td>
<td>3</td>
</tr>
<tr>
<td>0.00 0.01 10890</td>
<td>2</td>
</tr>
<tr>
<td>0.01 0.01 12598</td>
<td>4</td>
</tr>
<tr>
<td>0.00 0.00 3197</td>
<td>2</td>
</tr>
<tr>
<td>0.01 0.01 8808</td>
<td>6</td>
</tr>
<tr>
<td>0.00 0.00 1574</td>
<td>1</td>
</tr>
<tr>
<td>0.01 0.01 11033</td>
<td>4</td>
</tr>
<tr>
<td>0.00 0.01 10054</td>
<td>2</td>
</tr>
<tr>
<td>0.00 0.01 10854</td>
<td>2</td>
</tr>
<tr>
<td>0.01 0.02 21378</td>
<td>5</td>
</tr>
<tr>
<td>0.01 0.01 14129</td>
<td>4</td>
</tr>
<tr>
<td>0.01 0.01 12062</td>
<td>4</td>
</tr>
<tr>
<td>0.01 0.00 703</td>
<td>1</td>
</tr>
<tr>
<td>0.01 0.00 15560</td>
<td>5</td>
</tr>
<tr>
<td>0.00 0.00 883</td>
<td>2</td>
</tr>
<tr>
<td>0.00 0.00 703</td>
<td>1</td>
</tr>
<tr>
<td>0.00 0.00 703</td>
<td>1</td>
</tr>
<tr>
<td>0.01 0.00 10854</td>
<td>2</td>
</tr>
<tr>
<td>0.04 0.04 48281</td>
<td>19</td>
</tr>
<tr>
<td>0.01 0.01 16789</td>
<td>4</td>
</tr>
<tr>
<td>0.00 0.01 14270</td>
<td>2</td>
</tr>
</tbody>
</table>

Network administrators use these statistics to glean general information about where visitors to their website are coming from, peak activity times, and which internal uris 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_Front" 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.

JUNKBUSTERS 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 online than they actually are according to a survey of 329 computer users by America Online and the National Cyber Security Alliance (NCSA) during 2004. 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).

➢ 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/
Get Safe Online http://www.getsafeonline.org/
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
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

---

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.

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,\textsuperscript{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 \textit{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.


\textsuperscript{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
    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”

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

Kim Komando’s Firefox 2 and IE7’s Security Settings

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.**
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]
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.” In fact, any ActiveX control downloaded over the web might be a Trojan horse or a virus.

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 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_qci887624,00.html> (14 November 2006).
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

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.” 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.

---

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”
Choose Remember Passwords.

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

Set Master Password...
Remove Master Password...

View Saved Passwords

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

- Do you want Firefox to remember this password?
- Remember
- Never for This Site
- Not Now

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. 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.

![Clear Private Data](image)

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.

You will also need to clear your cache to clean out old user data.

**Manage Your Cookies**

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.


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

Disable or Defeat the HTTP-Referrer

The "http referrer" variable (often misspelled "referer") 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.

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

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.


186 Webwasher Classic is now owned by Cyberguard and is still free, though the company does request a donation.
0—do not send referer for anything

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