The WHOIS Command on Windows, Linux, and macOS Explained

Posted on September 23, 2025

This post breaks down the whois command — how it works, how to use it, the data points it provides, the parameters you can use with it, and its limitations. We also suggest some tools and techniques that can help you work around the tool's limitations.

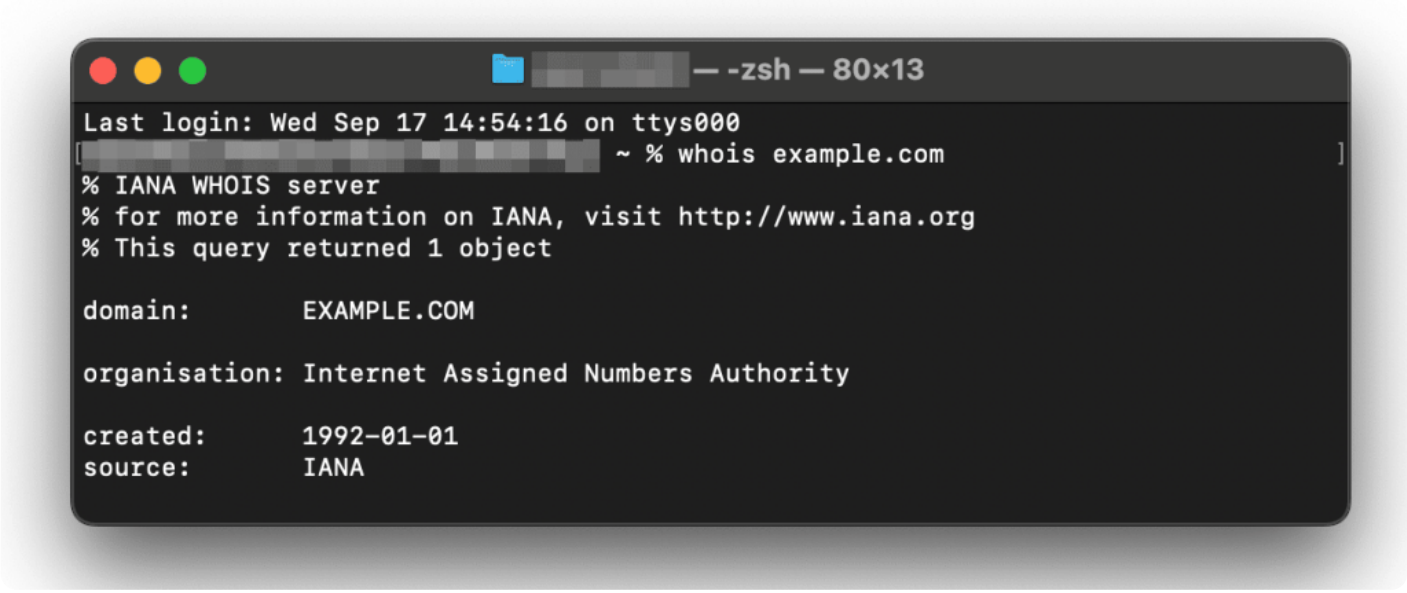
TL;DR: What You Need to Know About The WHOIS Command

The whois command is a command-line lookup tool used to query public WHOIS databases.

It provides information about the registration and ownership of an internet resource, such as a domain name, IP address, or Autonomous System Number (ASN). It's available on Windows, macOS, and Linux, and its output — a WHOIS record — includes details such as the domain registrar, registrant, registration and expiration dates, nameservers, and contact information.

Using the tool is as simple as opening the Terminal or command line and typing

```
whois example.com
```



The WHOIS command in action (on macOS)

However, it's worth noting that the Windows whois command, as well as the Linux/Unix/macOS options (even though they have more flags and parameters), have some limitations. The table below summarizes those limitations and our recommended solutions.

Limitations	Workaround
There's no standardized data format for the output, as each registry and registrar has its own format.	Use the WHOIS API — WHOIS data across all TLDs is already parsed and normalized. It also supports RDAP.
The command isn't built for bulk queries.	Use Bulk WHOIS API to query up to 500,000 domains at once.
If used too frequently for programmatic lookups, your requests will likely be rate-limited or blocked by registries to prevent abuse.	Use the WHOIS API for a more stable and reliable access to domain registration data.

Due to privacy regulations, the contact information in most WHOIS records is often hidden.	Use the WHOIS History API to see unredacted domain ownership data from before GDPR.

What Does the WHOIS Command Do?

When you use the whois command prompt on Windows or other operating systems, it tells the tool to connect to the correct WHOIS server for the target domain name's top-level domain (TLD) or the relevant Regional Internet Registry (RIR) like ARIN or RIPE for IP addresses. It uses the legacy WHOIS protocol over TCP port 43 to do this. In contrast, the newer Registration Data Access Protocol (RDAP) is a separate system that provides the same type of registration data in a standardized, machine-readable format over HTTPS, but it requires dedicated RDAP clients or API calls rather than the traditional whois command.

Once the correct server is identified, the command then sends the query (e.g., whois example.com). If available, a WHOIS record is returned. For domains, the record contains registration details found in the table below.

Type of Information	Description
Domain name	The queried resource
Registrar	The company managing the registration
Registrant	The organization or person who registered it (often redacted now)
Relevant dates	The domain's creation, last updated, and expiration dates
Nameservers	The DNS infrastructure serving the domain
Status codes	Registrar and registry restrictions, such as clientTransferProhibited
Contact details	Email address and phone number of the registrant, administrative, technical, and abuse contacts (often hidden now)

On the other hand, the WHOIS record of IP addresses and ASNs contains the allocation details (which IP block it belongs to), the owning organization (e.g., an ISP), and contact information for abuse and security issues.

However, WHOIS records are not standardized, and this results in various challenges for both human users and automated systems:

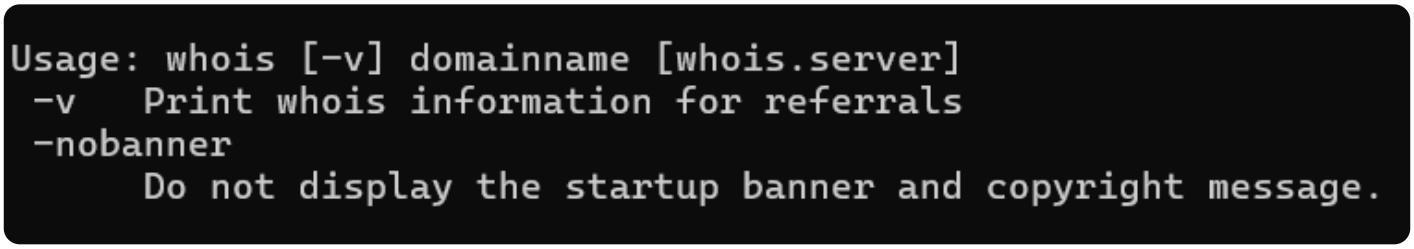
- **Different formats across registries:** Each registry or registrar can decide how to present the data. For example, dates may be written in different formats, fields may appear in a different order, or some fields may be omitted entirely.
- **Inconsistent field names:** A registrant's email might be labeled as "Registrant Email," "Email," or not shown at all, depending on the server. This makes it difficult to parse such variations programmatically.
- **Varying levels of detail:** Some WHOIS servers provide rich data including multiple contacts and technical details, while others return only the bare minimum (sometimes just the domain name and registrar).
- **Localization issues:** Records may include data in different languages or encodings, which complicates automated processing and global interoperability.
- **Unclear or missing error handling:** If a query cannot be resolved, servers often return unstructured error text or no response at all, leaving the client unable to redirect properly.

For casual users, this inconsistency makes WHOIS results confusing and hard to compare. For researchers, businesses, and security teams, it complicates large-scale analysis and automation. These challenges are one of the main reasons the industry moved toward RDAP as a replacement for the WHOIS protocol.

How to Use the WHOIS Command

Using the WHOIS command on Windows

To start using the Windows whois command, make sure that you have the WHOIS utility installed — you may need to download it from the Microsoft Sysinternals page. While the basic whois command works on Windows with this utility, the tool is somewhat limited since only the -v and -nobanner flags are available.



The Windows Sysinternals whois command accepts only two parameters

There's also a more flexible tool that requires you to install a Linux subsystem for Windows (WSL), which allows you to use other commands available on Linux-based systems. To do that, run the following PowerShell command in the command line:

```
wsl --install
```

When you have the Linux subsystem downloaded, you'll essentially be operating under Linux.

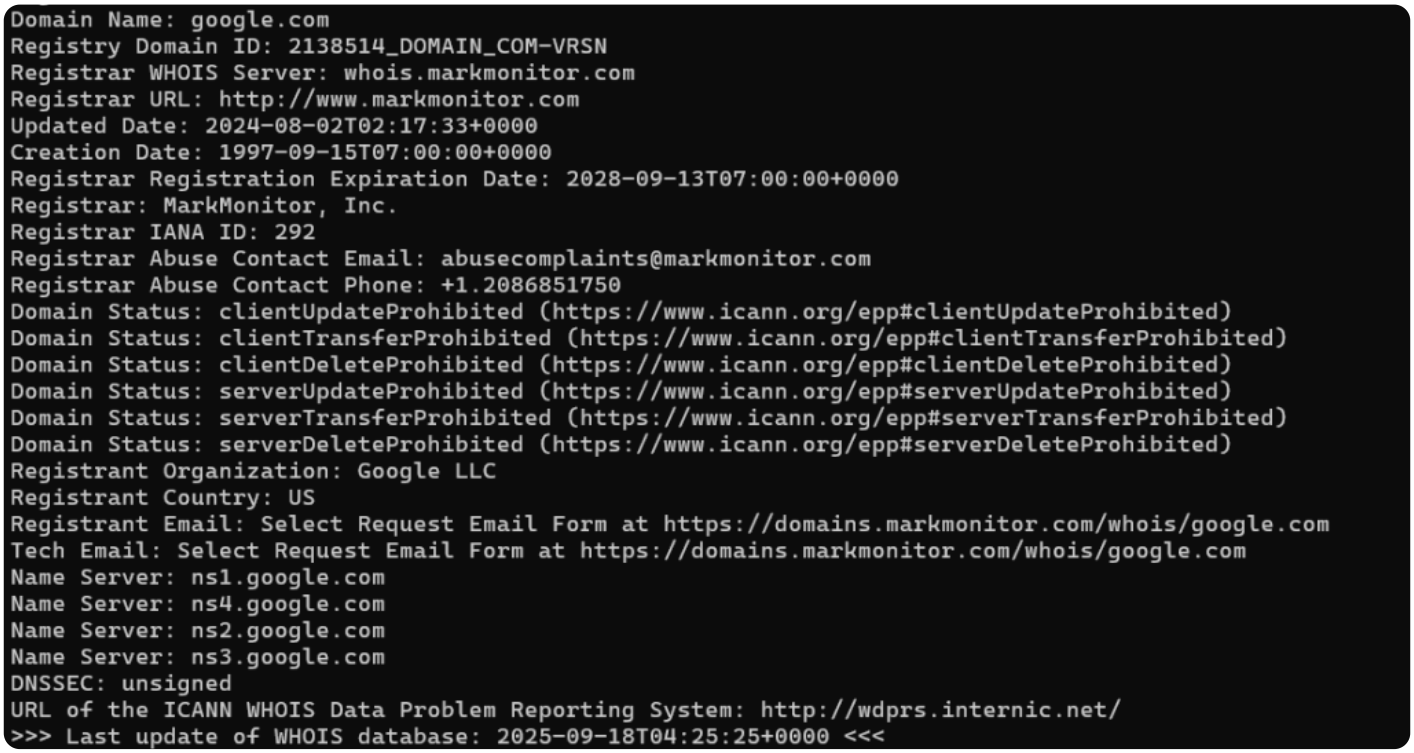
Using the WHOIS Command on Linux

Whether it's a Linux/Unix distribution or a Linux subsystem for Windows, you can install whois on it using this prompt:

```
sudo apt update && sudo apt install whois -y
```

After that, you can start using the whois command. Here's a sample output for the query

```
whois google.com
```



The WHOIS command from the WSL works differently that the Windows Sysinternals one

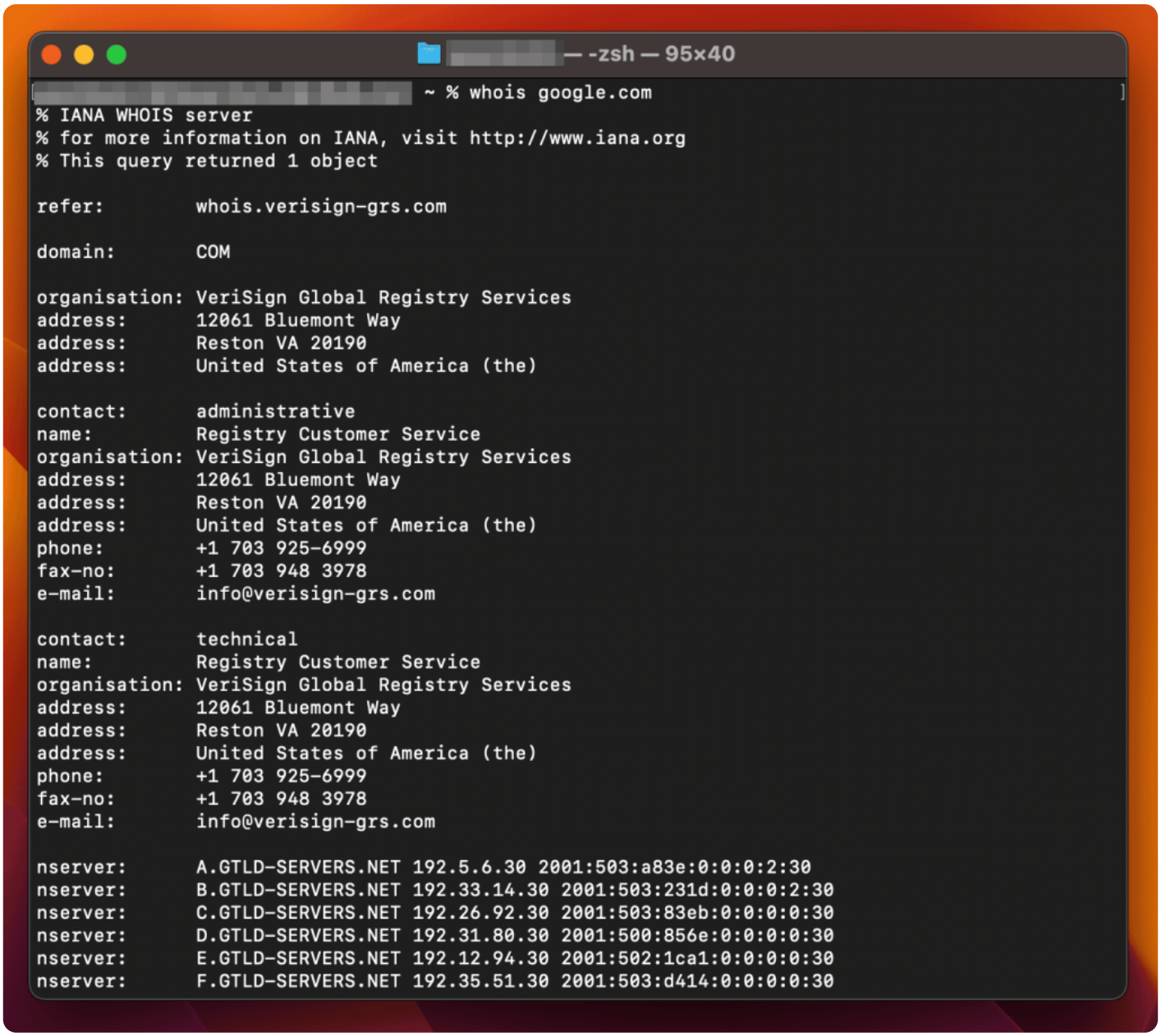
The output is similar to that of Windows' Sysinternals, as you can see below. However, the whois command for Linux (and for WSL) accepts a wider variety of different parameters and is more flexible as a result. We'll look into the different flags you can use later in this article.

```
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-08-02T02:17:33+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns1.google.com
Name Server: ns3.google.com
Name Server: ns2.google.com
Name Server: ns4.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
```

Output from the Windows Sysinternals' WHOIS utility

Using the WHOIS command on macOS

On macOS devices, setup is easier because the whois command is built in. But the query is the same — whois [domain name].



Output of the WHOIS command on macOS

WHOIS Command Parameters

As previously mentioned, the whois command on Linux is more flexible than on Windows since you can customize and refine your queries using various flags and arguments.

We tested each flag in the table below, but note that their exact behavior can vary slightly between different WHOIS client implementations (e.g., on Debian, macOS, or FreeBSD) and WHOIS databases (e.g. RIPE, ARIN, etc.)

Single-Letter Flag	Example command	Function
-H	whois -H example.com	Hide legal disclaimers from the output.
-h [HOST]	whois -h whois.iana.org example.com	Connect to a specific WHOIS server to get information.
-p [PORT]	whois -p 43 example.com	Connect to a specific port number on the server.
-I	whois -I example.com	Follow the official chain of referrals to find information.
-l	whois -l 193.0.0.0	Find the network range that's one level broader than the address.
-L	whois -L 193.0.0.0	Find all of the network ranges broader than the address.
-m	whois -m 193.0.0.0	Find all one-level more specific objects related to the query.
-M	whois -M 193.0.0.0	Find all objects that are more specific than your query.
-c	whois -c 193.0.0.0	Find the smallest network range with a maintenance attribute.
-x	whois -x example.com	Return only results that are an exact match for your query.
-b	whois -b 193.0.0.0	Return a brief list of IP ranges and abuse contact information.
-B	whois -B example.com	Show all objects in the results, including email addresses.

-G	whois -G example.com	Shows what changed after a database update.
-d	whois -d 8.8.8.8	Return DNS reverse delegation objects related to the query.
-i [ATTR]	whois -i person,mnt-by "RIPE-NCC-HM-MNT"	Perform a reverse search based on a specific attribute.
-T [TYPE]	whois -T person SMITH	Only return objects of a specific type.
-K	whois -K example.com	Return only the primary identifying keys for objects.
-r	whois -r example.com	Do not automatically find contact information for the record.
-R	whois -R example.com	Show the local copy of the domain object first.
-a	whois -a example.com	Search all of the mirrored databases for the query.
-s [SOURCE]	whois -s RIPE example.com	Search a specific mirrored database for information.
-t [TYPE]	whois -t person	Request a basic template for a specific object type.
-v [TYPE]	whois -v person	Request a verbose template for a specific object type.
-q	whois -q version	Query the server for information on its version., or any other parameters.

Understanding the WHOIS Command Output

The format of the whois command output is not standardized, so it can differ significantly depending on the registry and registrar. Let's break down a typical WHOIS record for google[.]com to understand the different sections.

```
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-08-02T02:17:33+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns1.google.com
Name Server: ns4.google.com
Name Server: ns2.google.com
Name Server: ns3.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2025-09-18T04:25:25+0000 <<<
```

The output of the WHOIS command for google.com

Registrar and Registry Information

Data Point	Description
Registry Domain ID: 2138514_DOMAIN_COM-VRSN	A unique identifier for the domain in the .com registry.
WHOIS Server: whois.markmonitor.com	The server that provided the record.

Registrar URL: http://www.markmonitor.com	The registrar's website.
Registrar: MarkMonitor, Inc.	The name of the company that manages the registration.
Registrar IANA ID: 292	The registrar's official ID assigned by the ICANN.
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com	The email to which abuse reports (e.g., spam and fraud) should be sent.
Registrar Abuse Contact Phone: +1.2086851750	Abuse hotline phone number.

Key Dates

Data Point	Description
Updated Date: 2019-09-09T15:39:04Z	The last time the registrar updated this record (e.g., when Google renewed or modified it).
Creation Date: 1997-09-15T04:00:00Z	When the domain was first registered — google[.]com has existed since 1997
Registry Expiry Date: 2028-09-14T04:00:00Z	When the current registration will expire (unless renewed).

Domain Status Codes

The Extensible Provisioning Protocol (EPP) status codes indicate the status and restrictions of the domain and are defined by the Internet Corporation for Assigned Names and Numbers (ICANN). We have a detailed video explaining these codes. For google[.]com, the assigned statuses are from both the registrar (client status codes) and registry (server status codes), and as of the timeof writing, these codes are:

- **clientDeleteProhibited**: Prevents the domain from being accidentally or fraudulently deleted.
- **clientTransferProhibited**: Stops the domain from being transferred to another registrar without Google's permission.
- **clientUpdateProhibited**: Blocks any attempts to update the domain's records, protecting them from unauthorized changes.
- **serverDeleteProhibited**: The registry has locked the domain, preventing it from being deleted by anyone.
- **serverTransferProhibited**: The domain cannot be transferred to another registrar.
- **serverUpdateProhibited**: Any updates to the domain's record are not allowed by the registry.

Registrant Details

This part of the WHOIS record identifies the owner and associated contacts.

Data Point	Description
Registrant Organization: Google LLC	The organization that owns the domain.
Registrant Country: US	The registrant's country.

Registrant and Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com	The registrant email is hidden via MarkMonitor's WHOIS Privacy Service. Instead of exposing addresses, it directs to a web form.

Name Servers (DNS Infrastructure)

This section lists the authoritative DNS servers for the domain, which are responsible for translating the domain name into an IP address. Google[.]com's name servers are:

- ns1.google[.]com
- ns2.google[.]com
- ns3.google[.]com
- ns4.google[.]com

Security

The WHOIS record indicates if the domain is signed with Domain Name System Security Extensions (DNSSEC), a security protocol designed to prevent DNS spoofing. Google's domain is not signed with DNSSEC, but the company has other security measures in place.

Administrative Notes

At the end of the WHOIS record is a link where issues with the WHOIS data can be reported (URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/).

The date and timestamp when the WHOIS database was last updated are also included. When we

did the lookup for google[.]com, the timestamp was 2025-09-07T23:18:55+0000.

Limitations of the WHOIS Command

As you've seen above, the whois command gives useful information about a domain or IP address. The -i flag even lets you do a reverse search on an attribute, which helps identify all domains or IP addresses associated with a specific entity.

However, it is not always straightforward and often very limited, and we have encountered its limitations while testing it on different systems. We detail these restrictions below.

No Standardized Data Format

WHOIS was not designed with a universal schema. That means the output for WHOIS lookups varies widely between different registries and registrars, making it difficult to automatically parse the data consistently. You've already seen a sample of a .com WHOIS record above, so let's take a look at the output for a few other TLDs:

- **.uk**

```
Domain name:
    supex-machining.co.uk

Data validation:
    Nominet was able to match the registrant's name and address against a 3rd party data source on 31-Jul-2024

Registrar:
    Ionos SE [Tag = 1AND1]
    URL: https://ionos.com

Relevant dates:
    Registered on: 02-Sep-2025
    Expiry date:  02-Sep-2026
    Last updated:  08-Sep-2025

Registration status:
    Registered until expiry date.

Name servers:
    ns1033.ui-dns.de
    ns1075.ui-dns.biz
    ns1090.ui-dns.org
    ns1112.ui-dns.com

WHOIS lookup made at 06:53:10 18-Sep-2025
```

What WHOIS outputs for .uk domains

- **.top**

```
Domain Name: 409po.top
Registry Domain ID: D20250901G10001G_55570177-top
Registrar WHOIS Server: whois.west263.com
Registrar URL: http://www.hkdns.hk
Updated Date:
Creation Date: 2025-09-01T05:58:37Z
Registry Expiry Date: 2026-09-01T05:58:37Z
Registrar: west263 International Limited
Registrar IANA ID: 1915
Registrar Abuse Contact Email: abuse@hkdns.hk
Registrar Abuse Contact Phone: +852.85330697963
Domain Status: ok https://icann.org/epp#OK
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name:
Registrant Organization:
Registrant Street:
Registrant City:
Registrant State/Province:
Registrant Postal Code:
Registrant Country:
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email:
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name:
Admin Organization:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
```

What WHOIS outputs for .top domains

- **.org**

```
root@DESKTOP-0URHTKQ:~# whois viacapitalizaca0.org
Domain Name: viacapitalizaca0.org
Registry Domain ID: REDACTED
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://www.tucows.com
Updated Date: 2025-09-05T07:19:45Z
Creation Date: 2025-08-31T07:19:23Z
Registry Expiry Date: 2026-08-31T07:19:23Z
Registrar: Tucows Domains Inc.
Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: ns1.siteground.net
Name Server: ns2.siteground.net
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://icann.org/wicf/
>>> Last update of WHOIS database: 2025-09-18T05:59:32Z <<<
```

What WHOIS outputs for .org domains

- **.de**

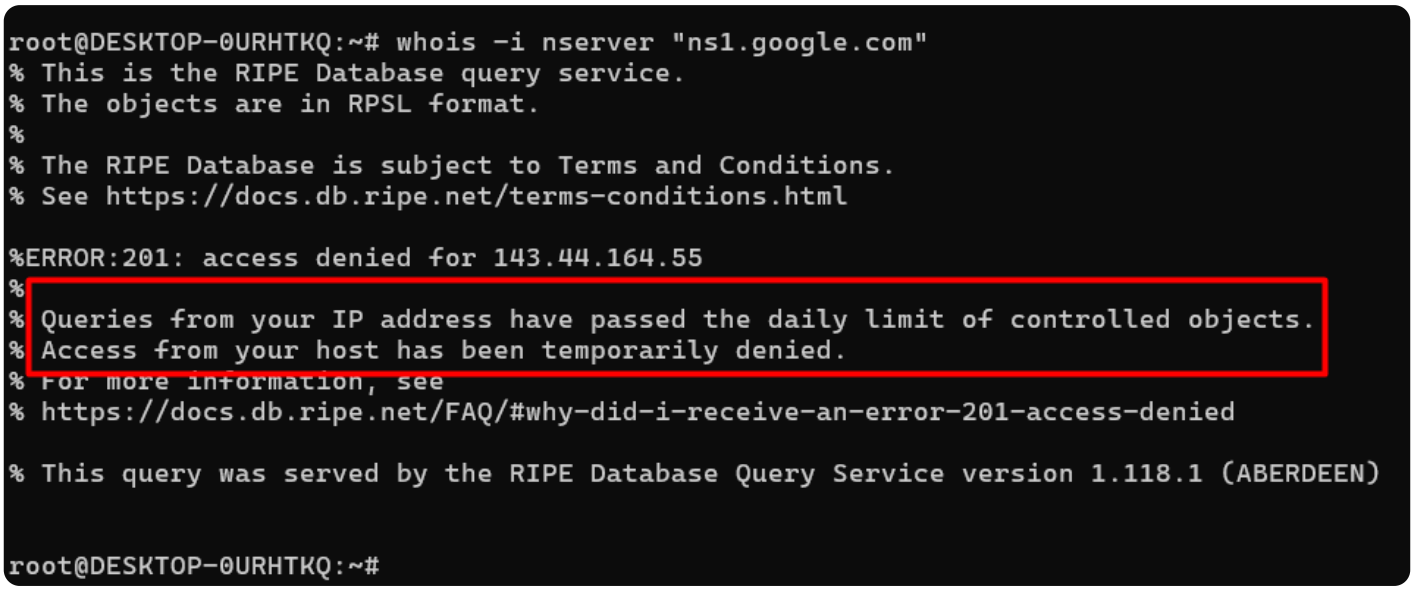
```
root@DESKTOP-0URHTKQ:~# whois fotogalerie-ms.de
% Restricted rights.
%
% Terms and Conditions of Use
%
% The above data may only be used within the scope of technical or
% administrative necessities of Internet operation or to remedy legal
% problems.
% The use for other purposes, in particular for advertising, is not permitted.
%
% The DENIC whois service on port 43 doesn't disclose any information concerning
% the domain holder, general request and abuse contact.
% This information can be obtained through use of our web-based whois service
% available at the DENIC website:
% http://www.denic.de/en/domains/whois-service/web-whois.html
%
%

Domain: fotogalerie-ms.de
Nserver: root-dns.netcup.net
Nserver: second-dns.netcup.net
Nserver: third-dns.netcup.net
Status: connect
Changed: 2012-11-12T17:19:11+01:00
root@DESKTOP-0URHTKQ:~#
```

What WHOIS outputs for .de domains

The lack of standardization makes WHOIS unreliable for automated data retrieval and parsing. A more modern alternative is the Registration Data Access Protocol (RDAP), which provides standardized JSON data. Our WHOIS API and related products support this protocol and even have a protocol selector feature that lets users choose between WHOIS and RDAP.

Inefficient Bulk WHOIS Lookups

While you can query multiple resources at once, performing bulk lookups with the whois command can get messy because many WHOIS servers implement rate limiting to prevent abuse. Sending too many requests over a short period can lead to your IP address being temporarily blocked.



WHOIS not working because of rate limiting

If you need the WHOIS records of many domain names, you can use the Bulk WHOIS API, which lets you look up up to 500,000 domains per query.

Automated Queries Are Not Allowed

Using the whois command programmatically is prohibited. In fact, it's included in the legal disclaimer attached to the command's WHOIS record output.

```
By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
  (1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
  (2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).
```

The WHOIS command does not allow automated usage

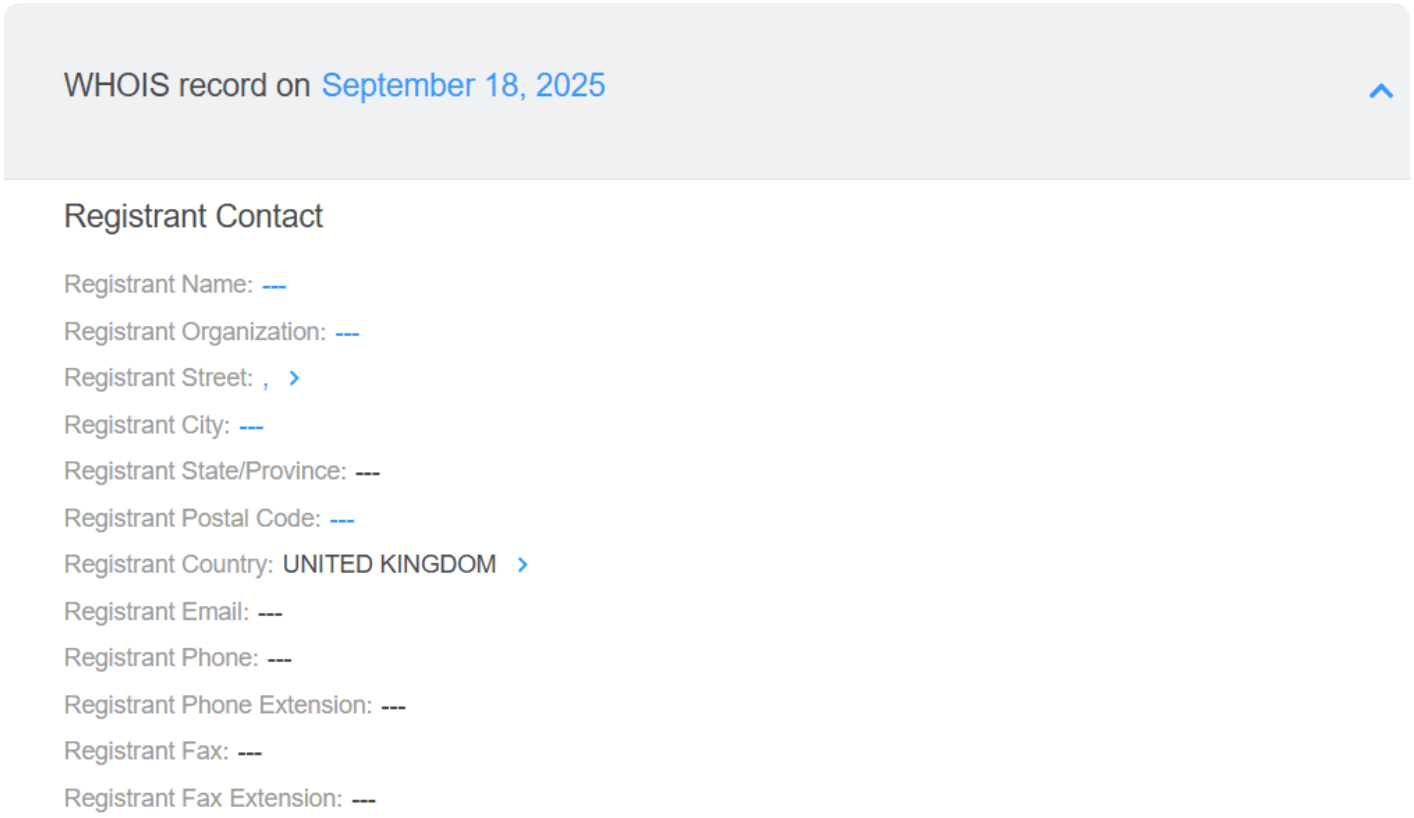
If you're building a tool that needs consistent access to WHOIS data, you are not allowed to directly query WHOIS servers with the command-line tool, so instead, you could use the WHOIS API. The API provides a more stable and reliable way to retrieve this information, especially for programmatic use. It delivers data in JSON or XML formats which are also much easier to programmatically parse than the raw text output that the whois command provides.

WHOIS Data is Often Redacted

Most WHOIS records for individual registrants now redact personal contact information for privacy reasons, a practice that became widespread around 2018 when the General Data Protection Regulation (GDPR) was implemented. This is a limitation that all WHOIS service providers face, since redaction is at the registrar level.

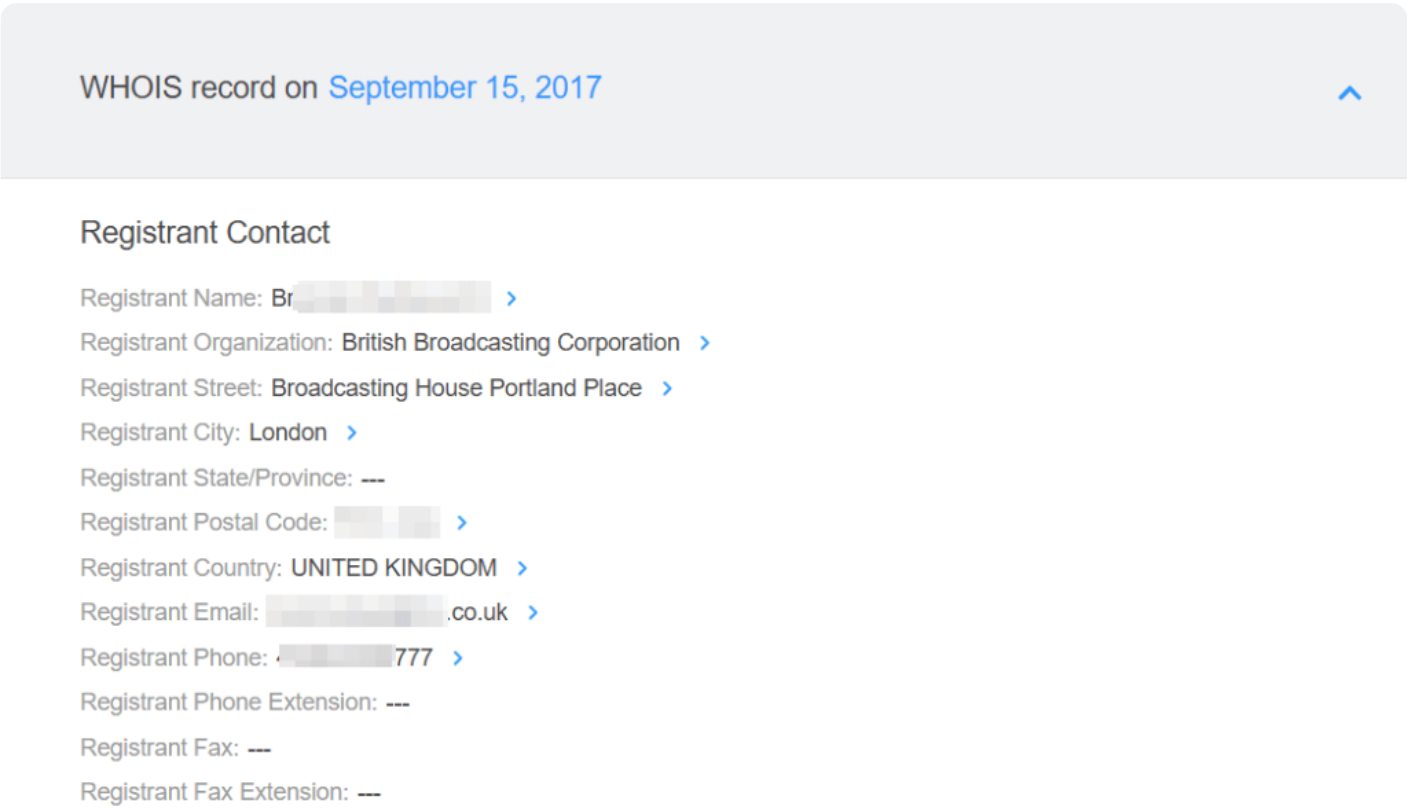
However, there is a way to see WHOIS data — at least the record before redaction — particularly if it was publicly available before, and that's through WHOIS History. This service lets you look up the historical domain registration details of any domain.

The current WHOIS data of bbc[.]com, for example, is heavily redacted. You can view key dates, registrar name, WHOIS server, name servers, and status codes, but only the registrant country is publicly available among all registrant contact details. This has been the case since 2018.



The current WHOIS record for bbc.com doesn't show much data

But when you browse through the domain's history, you'll see that in 2017 (and record updates before that), those registrant fields were filled out with a person's name, the organization's email address, and phone number.



A historical WHOIS record for bbc.com has the now missing data

Conclusion

The whois command is a quick and easy way to get registration and ownership details of any domain name. It can also provide information on IP addresses and ASNs. With different flags, you can adjust to fetch information from specific sources or even run reverse lookups.

However, it works differently on Windows, macOS, and Linux (and requires installation on some of those systems). If something that you've read in this article and decided to try doesn't work, probably, the implementation of the whois command in your operating system is to blame.

It also has its limitations:

- Non-standardized output

- Rate limiting
- Limited bulk lookups
- Data redacted due to privacy reasons

To overcome these limitations, you can use more advanced tools like our WHOIS API, Bulk WHOIS API, and the WHOIS History products.