ETHICAL HACKING

INFORMATION GATHERING

PASSIVE INFORMATION GATHERING

WHOIS Lookup

Whois Lookup

- What is whois Lookup?

WHOIS lookup is a query to retrieve information about a domain name, IP address, or other internet resource from a WHOIS database, which contains registration details such as the domain owner, registrar, registration date, and contact information. Below, I’ll provide demonstrations of WHOIS lookup using various tools and methods, covering command-line, online tools, and programmatic approaches. These demos will show how to perform WHOIS lookups for a domain (e.g., example.com) or an IP address (e.g., 8.8.8.8). I’ll also explain how to interpret results and provide practical examples.

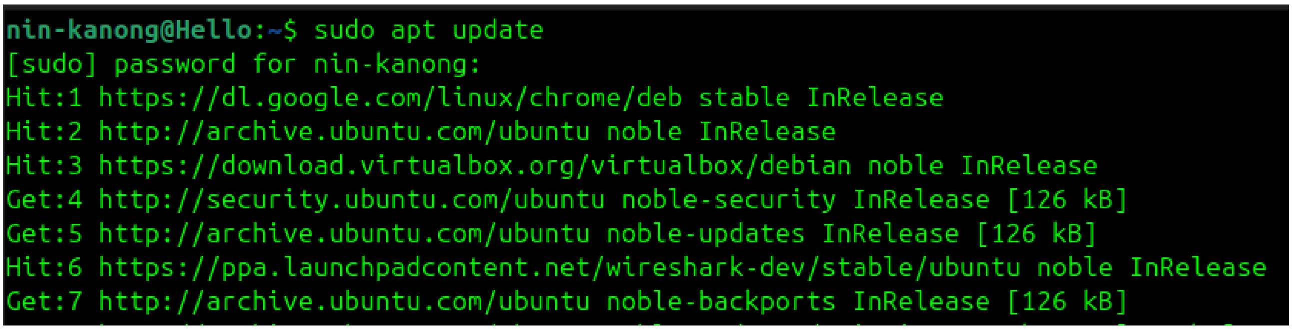
Whois is a command-line utility used in Linux systems to retrieve information about domain names, IP addresses, and network devices registered with the Internet Corporation for Assigned Names and Numbers (ICANN). The data received by Whois consists of the name and contact information of the domain or IP address owner, the registration and expiration date, the domain registrar, and the server information. Whois command can be very useful for network administrators, web developers, and security professionals for achieving various tasks like checking network connectivity or troubleshooting. In this article, we will go through the usage of the Whois command on Linux (Ubuntu system).

1. Installing Whois Command on Linux

Follow the below number of steps to install the Whois command on Ubuntu.

Step 1: Firstly, update the system using the below command. Execute the below command in the terminal to update the system.

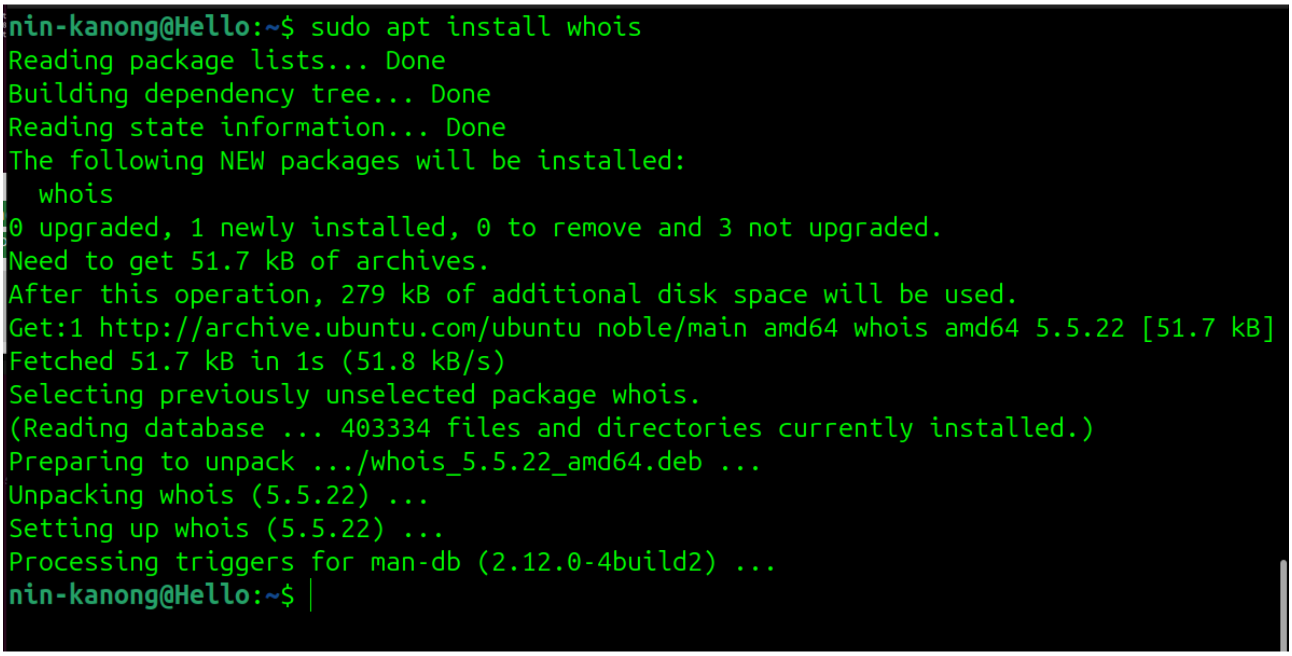
- kali> sudo apt update



```
nin-kanong@Hello:~$ sudo apt update
[sudo] password for nin-kanong:
Hit:1 https://dl.google.com/linux/chrome/deb stable InRelease
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:3 https://download.virtualbox.org/virtualbox/debian noble InRelease
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:6 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu noble InRelease
Get:7 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
```

Step 2: Now, by using the apt manager, install the whois command utility, so that we can retrieve the information about domains, IP Addresses, etc.

- kali> sudo apt install whois



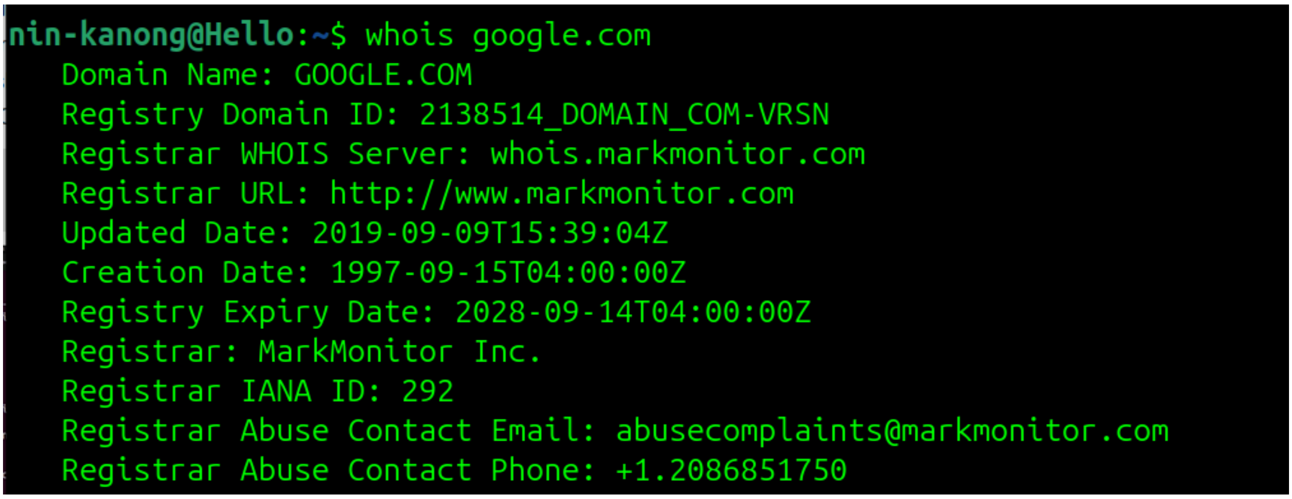
```
nin-kanong@Hello:~$ sudo apt install whois
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  whois
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 51.7 kB of archives.
After this operation, 279 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 whois amd64 5.5.22 [51.7 kB]
Fetched 51.7 kB in 1s (51.8 kB/s)
Selecting previously unselected package whois.
(Reading database ... 403334 files and directories currently installed.)
Preparing to unpack .../whois_5.5.22_amd64.deb ...
Unpacking whois (5.5.22) ...
Setting up whois (5.5.22) ...
Processing triggers for man-db (2.12.0-4build2) ...
nin-kanong@Hello:~$
```

+ Usage of Whois Command on Ubuntu

Example 1: Getting Information on Domain Name (geeksforgeeks.org).

In this example, we will extract the information about the domain (geeksforgeeks.org). In the below screenshot, you can see that we have information like Registry Domain ID, WHOIS Server, Updated Date, etc.

- kali> whois example.com

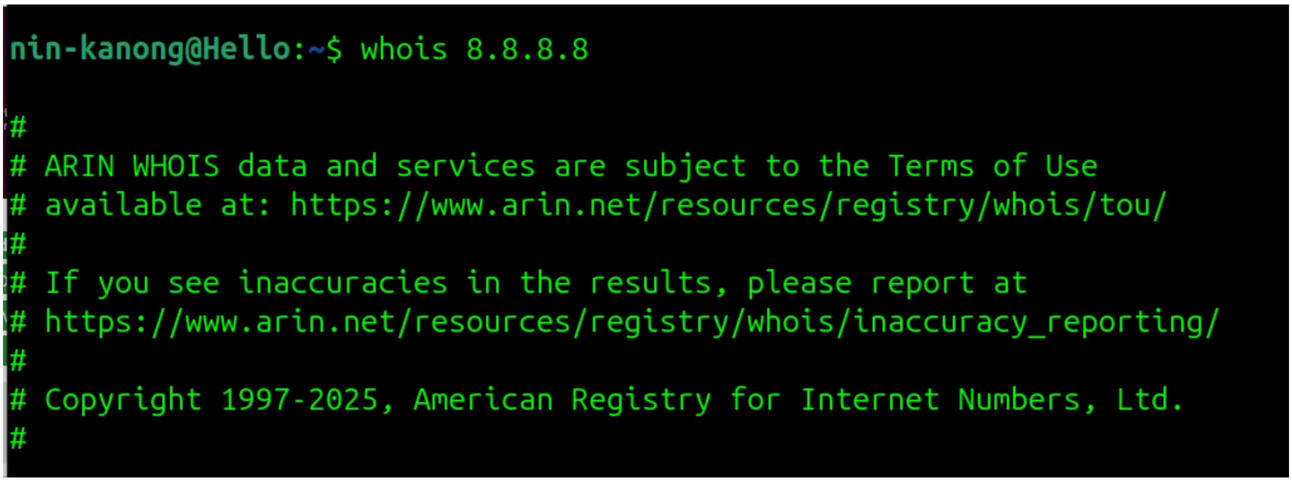


```
nin-kanong@Hello:~$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
```

+ Getting Information about IP Address.

In this example, we will be extracting information by giving the IP Address as input to the whois command. In the below screenshot, we have got the information about the IP Address such as NetRange, CIDR, etc.

- kali> whois {IP }



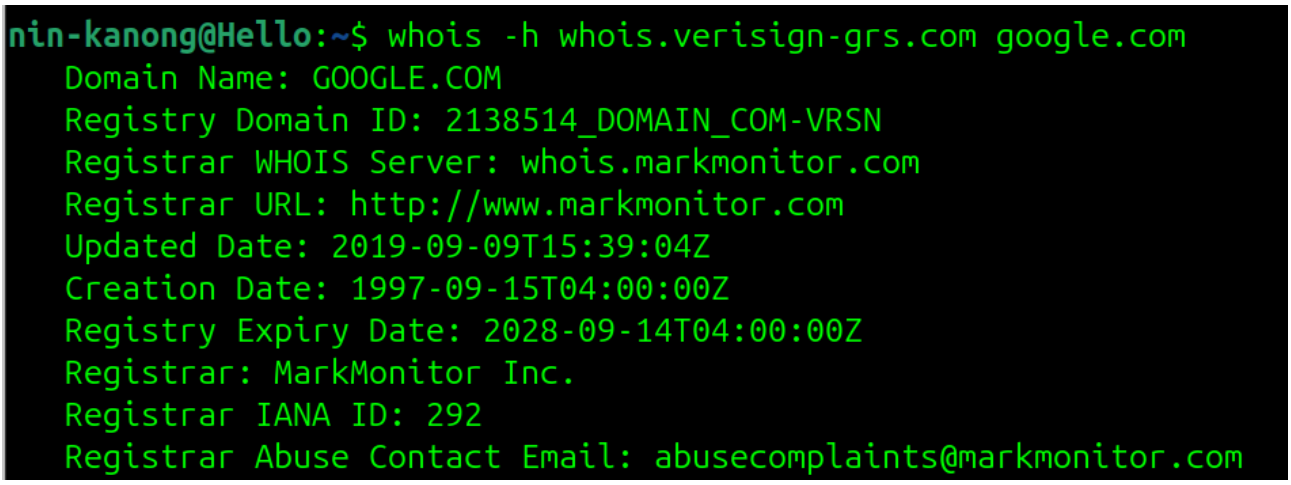
```
nin-kanong@Hello:~$ whois 8.8.8.8

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
```

+ Getting Information about some specific WHOIS server set up by an ICANN.

WHOIS command is not limited to standard domain or IP address, even we can extract the information of some specific WHOIS server set up by an ICANN. In the below screenshot, we have given the input of the WHOIS Server along with the domain name. We have got the detailed information for this.

-kali> whois -h whois.verisign-grs.com google.com

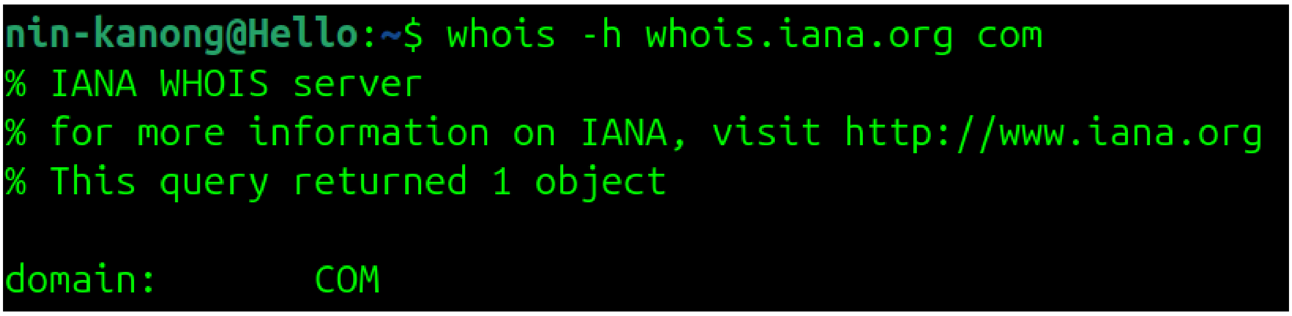


```
nin-kanong@Hello:~$ whois -h whois.verisign-grs.com google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
```

+ Getting Information about a domain name from a specific registrar.

In this example, we will fetch the information about a domain name from a specific registrar. We have given the domain name (**whois.iana.org**) and the registrar (**com**).

-kali> whois -h whois.iana.org com

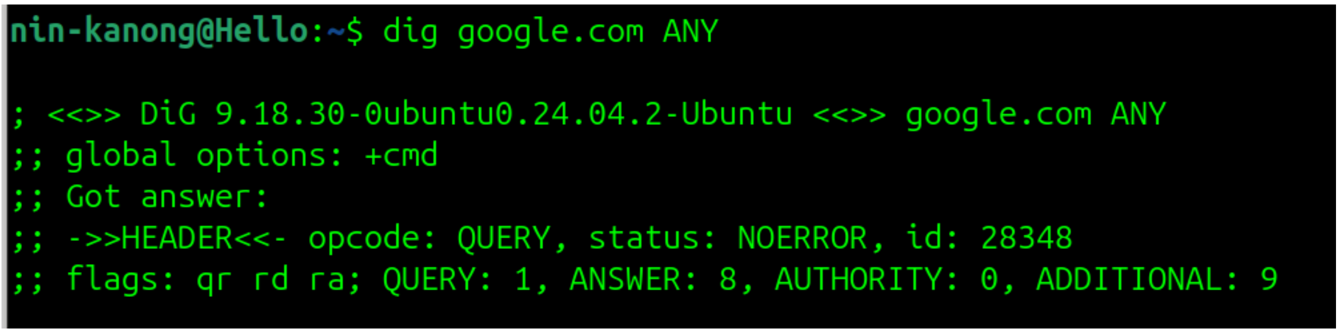


```
nin-kanong@Hello:~$ whois -h whois.iana.org com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:       COM
```

+ Query DNS records, which can complement WHOIS data:

- kali> dig {example.com} ANY



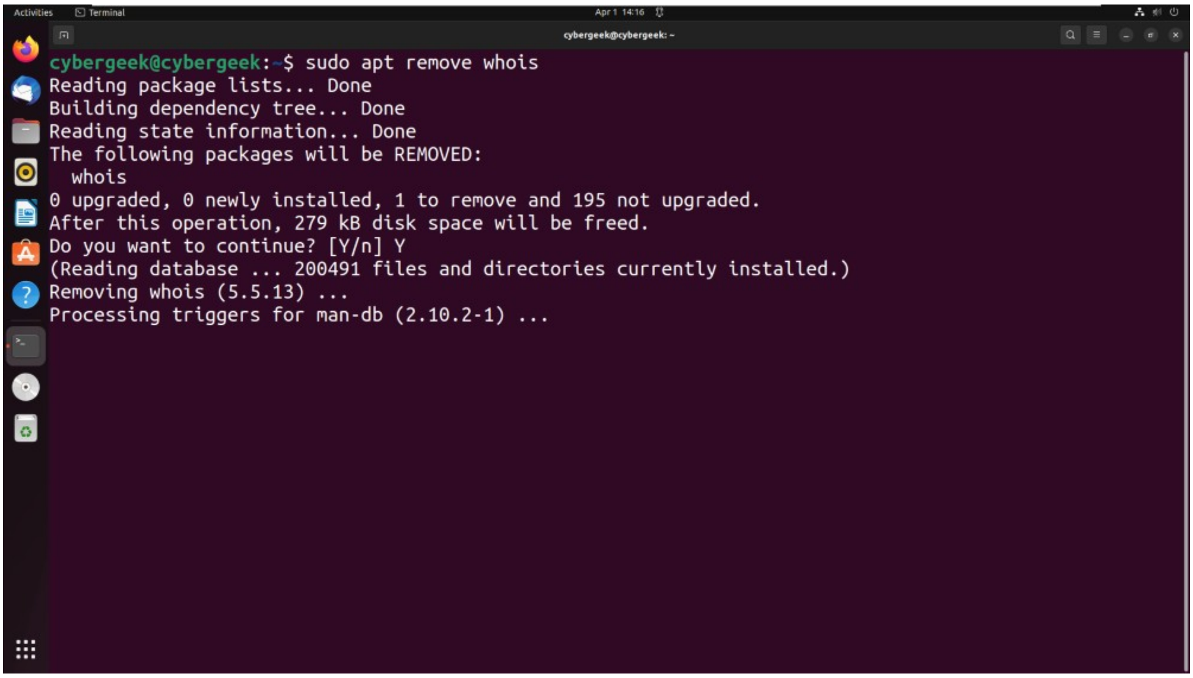
```
nin-kanong@Hello:~$ dig google.com ANY

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> google.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28348
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 9
```

+ Uninstalling Whois Command on Ubuntu

After usage, we can remove the command by uninstalling it. Execute the below command in the terminal to remove the whois command from Ubuntu.

-kali> sudo apt remove whois



```
cybergeek@cybergeek:~$ sudo apt remove whois
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  whois
0 upgraded, 0 newly installed, 1 to remove and 195 not upgraded.
After this operation, 279 kB disk space will be freed.
Do you want to continue? [Y/n] Y
(Reading database ... 200491 files and directories currently installed.)
Removing whois (5.5.13) ...
Processing triggers for man-db (2.10.2-1) ...
```

2. Online WHOIS Lookup Tools

Online tools provide user-friendly interfaces for WHOIS queries, ideal for non-technical users.

Demo : Using ICANN Lookup

Tool: ICANN Lookup (https://lookup.icann.org/)

Steps:

1. Visit https://lookup.icann.org/.
2. Enter example.com in the search bar.
3. Click “Lookup.”
4. Review the results, which include:
    - Domain name, registrar, registration/expiration dates, name servers, and contact details (if not redacted).

Sample Output (simplified):

- Domain: example.com
- Registrar: IANA Reserved
- Created: 1995-08-14
- Expires: 2025-08-13
- Name Servers: a.iana-servers.net, b.iana-servers.net

Notes:

- ICANN Lookup is authoritative for generic top-level domains (gTLDs) like .com, .org.
- GDPR may hide registrant details unless you’re authorized to access them.

Demo : Using WHOIS.com

Tool: WHOIS.com (https://www.whois.com/whois/)

Steps:

1. Go to https://www.whois.com/whois/.
2. Enter example.com or 8.8.8.8.
3. Submit the query.
4. View details like registrar, contact info, and registration history.

Sample Output:

- Similar to ICANN but may include additional data like registrar abuse contact info.

Notes:

- WHOIS.com aggregates data from multiple WHOIS servers.
- Useful for checking domains and IPs across different registries.

Demo : Using DomainTools

Tool: DomainTools (https://whois.domaintools.com/)

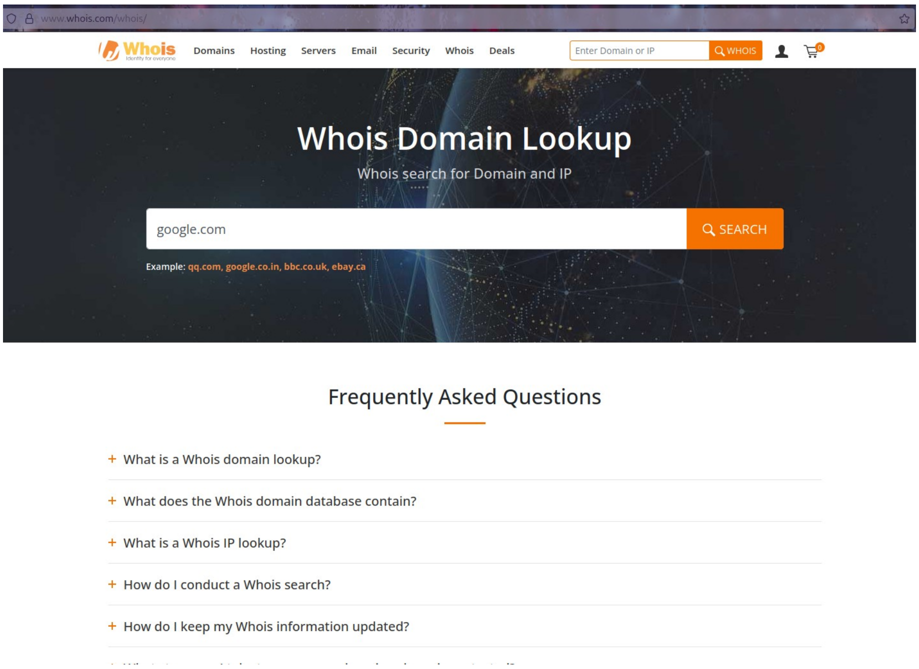
Steps:

1. Visit https://whois.domaintools.com/.
2. Enter a domain or IP.
3. Review enhanced WHOIS data, including historical records (premium feature).

Notes:

- DomainTools offers advanced features like WHOIS history and domain monitoring for a fee.
- Free lookups provide basic information similar to ICANN.

Go to this website: https://www.whois.com/whois/



Whois Domain Lookup

Whois search for Domain and IP

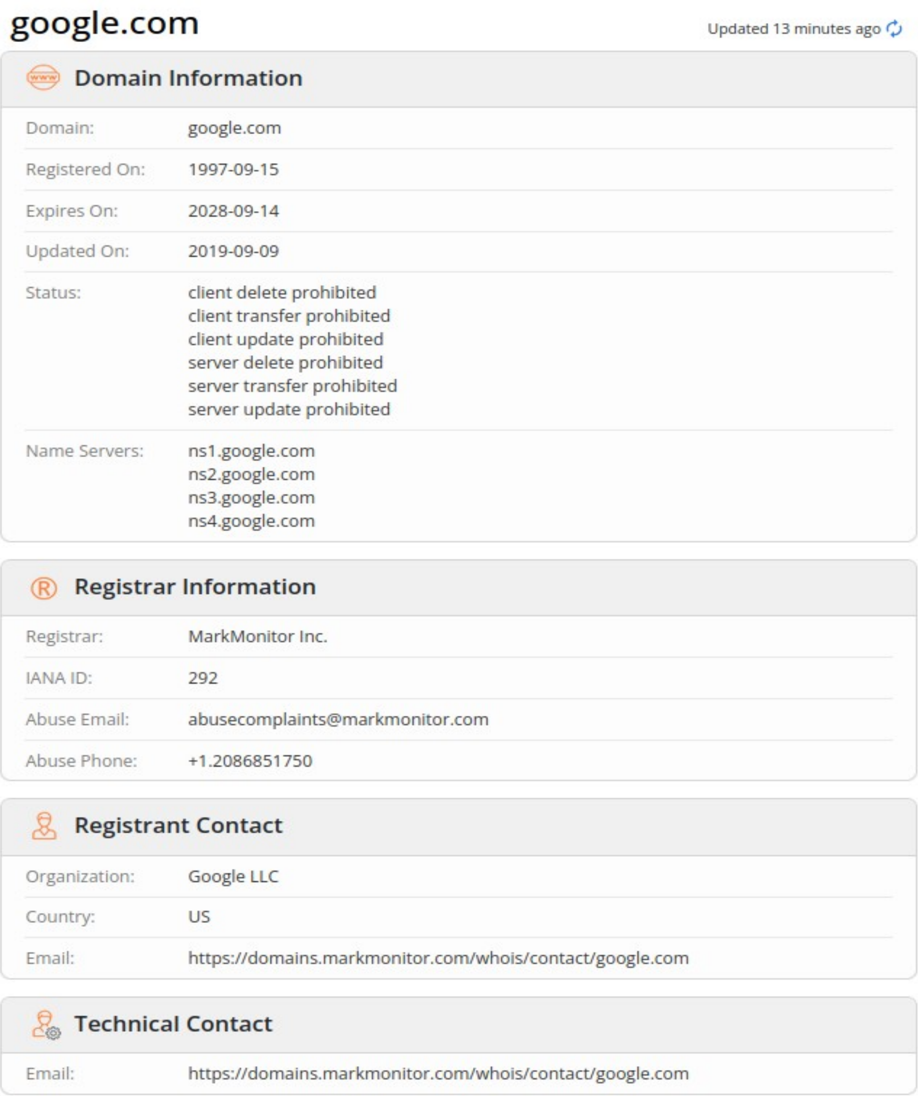
google.com

Example: qq.com, google.co.in, bbc.co.uk, ebay.ca

Frequently Asked Questions

- What is a Whois domain lookup?
- What does the Whois domain database contain?
- What is a Whois IP lookup?
- How do I conduct a Whois search?
- How do I keep my Whois information updated?

Result:



google.com

Updated 13 minutes ago

Domain Information

Domain:	google.com
Registered On:	1997-09-15
Expires On:	2028-09-14
Updated On:	2019-09-09
Status:	client delete prohibited client transfer prohibited client update prohibited server delete prohibited server transfer prohibited server update prohibited
Name Servers:	ns1.google.com ns2.google.com ns3.google.com ns4.google.com

Registrar Information

Registrar:	MarkMonitor Inc.
IANA ID:	292
Abuse Email:	abusecomplaints@markmonitor.com
Abuse Phone:	+1.2086851750

Registrant Contact

Organization:	Google LLC
Country:	US
Email:	https://domains.markmonitor.com/whois/contact/google.com

Technical Contact

Email:	https://domains.markmonitor.com/whois/contact/google.com