

What is WHOIS Lookup:

The **WHOIS lookup** is a way to find information about a website or domain name and when someone creates a website they must register the domain name like such as google.com and WHOIS helps us to check who registered that domain and some basic details about that website like (google.com)

→ WHOIS lookup tool means who owns the website and when it is created

Why is WHOIS Lookup Important :

- It helps to say who behind the website
 - It's some information like when the website was created and when it is expired
 - Sometime it helps to identify the fake or suspicious websites
 - It is very useful in cybersecurity and investigation fields
 - It helps to properly manages their website owners
 - The Whois lookup tool is **works like a identity card of a website**

What Information Does WHOIS Show:

- The Domain name like this example.com
 - The Registrar name (company that registered the domain)
 - The Registration date should when the domain was created
 - It tells the Expiry date like when it will expire
 - Name of the servers used by the domain
 - The Country or organization sometimes it can hidden for privacy purpose
 - Some personal details it may be hidden to protect their privacy

How WHOIS Lookup Works (Step by Step)

Step1: We you can enter a domain name into a WHOIS tool

Step2: The tool can checks the WHOIS database for target websites

Step3: The database can stores the domain registration details like

See in that picture

4. The tool can collect the available information from websites

5. The information is shown to the user for who is used for that tool like WHOIS

This process can occurs in very fast like usually in seconds.

WHOIS Lookup Legal:

Yes it is legal **WHOIS lookup is completely** anyone can use like this purposes only otherwise it is illegal

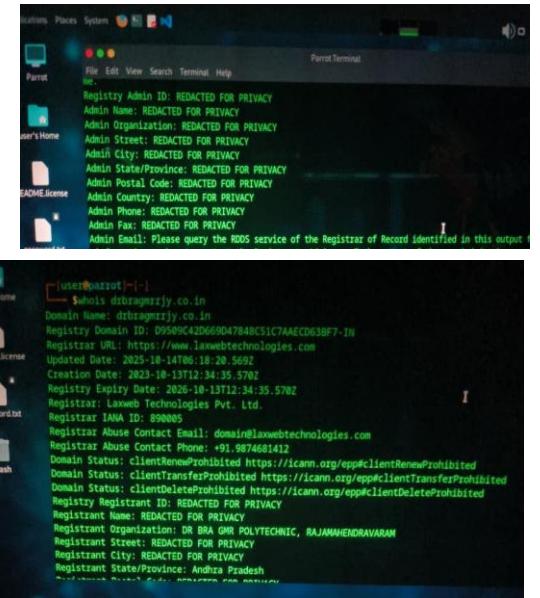
- Check domain details
 - Verify website ownership
 - Learn about domain history

But using the information for **wrong purposes** is not allowed.

Domain Registrar and Registry Details :

The **domain registrar** is a company where a website name is bought and the **registry** is the main organization that keeps records of all domain names in the database

- **Why it is important:**
It helps to know the which company can register the domain and who can manage it officially.
 - **How it works:**
When someone can buy a domain, the registrar sends the details to the registry for the internet and shows these details so people can easily check them.
→ Registrar = shop where domain is bought
→ Registry = record book that stores domain details



Domain Creation, Update, and Expiry Dates :

- When the domain was **created**
- When it was **last updated**
- When it will **expire**
- **Why it is important:**
It helps to understand **how old the website is** new domains can sometimes maybe at risky and old domains are often more trusted.
- **How it works:**
The WHOIS records the dates when the domain was registered, changed, and when it needs renewal. The dates and all website related information tells the **life history of a website**.

Privacy-Protected Registration Data :

Sometimes the owner's name, email, and phone number are **hidden** in WHOIS for security purpose

- **Why it is important:**
It protects the domain owners from spam and unwanted contact but it can also make it hard to know **who owns the website** for developing time or hosting time
- **How it works:**
the privacy service replaces real details with general or hidden information.

Registrar Abuse Contact Information :

it's a contact email or address given by the registrar to report problems.

- **Why it is important:**
It is a website is used for scams or cheating, people can report it.
- **How it works:**
The WHOIS tool shows the abuse contact users can send complaints to the registrar.
→ It is like a **complaint box** for bad websites.

How WHOIS Supports OSINT Investigations:

The OSINT means **Open Source Intelligence**, it means collecting information that is publicly available.

- **Why it is important:**
The domain can ownership patterns
 - It helps to know the domain age
 - It creates a Links between websites

How it works:

The Investigators use WHOIS tool for data to study domain history and detect suspicious activity.

THANK YOU