Domain Name Basics
WHOIS

Tobias Sattler
tobiassattler.com

What is WHOIS?

WHOIS is a **protocol** to query **databases**, such as **domain** names, **IP** addresses, or **autonomous system** (AS) and is documented in Request for Comment (RFC) 3912.

WHOIS has its roots in 1982 when the Internet Engineering Task Force (IETF) published a protocol for a directory service for ARPANET users.

The Internet Assigned Numbers Authority (IANA) runs a WHOIS service as a starting point and references to Regional Internet Registries (RIR) and Domain Name Registries.

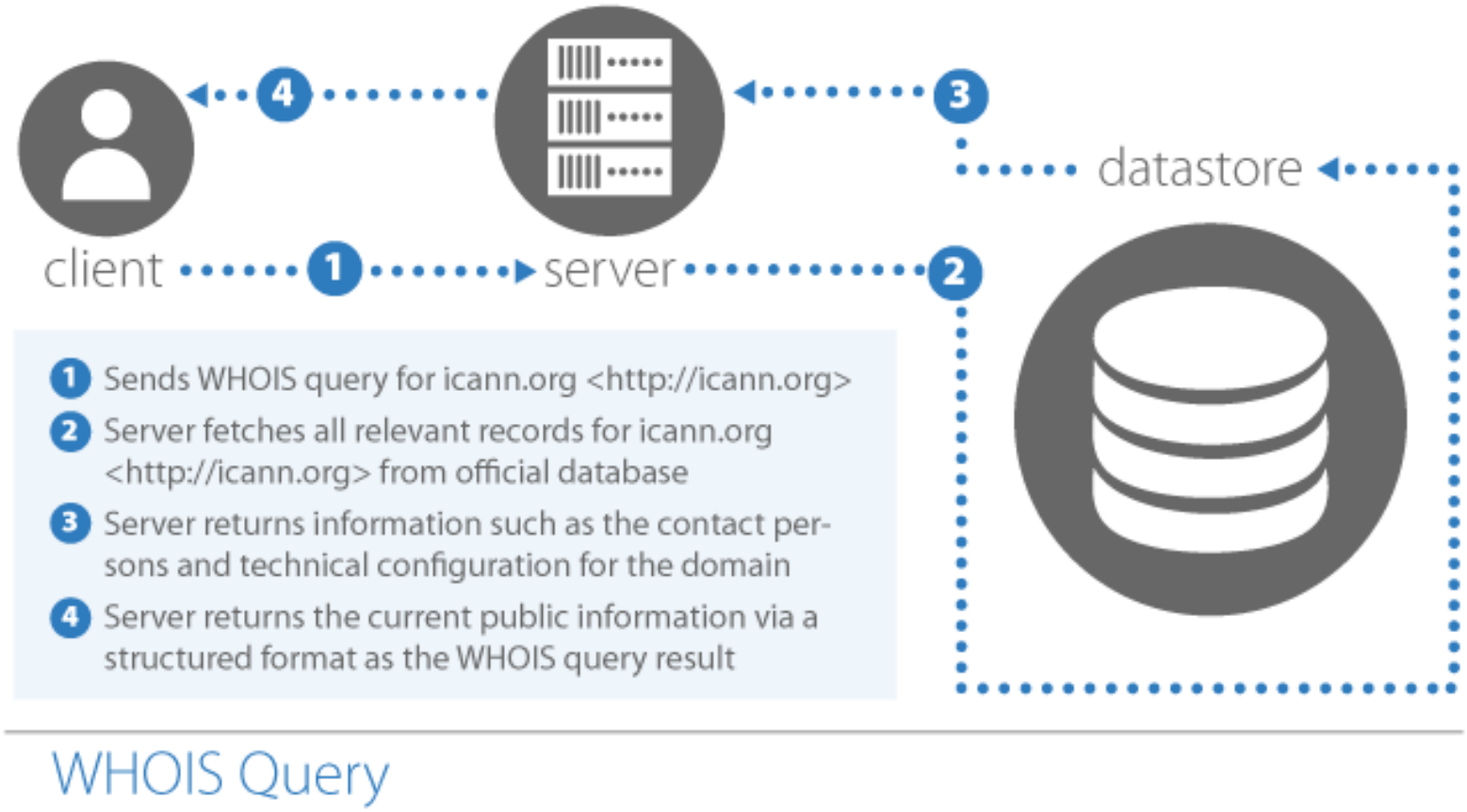
Two WHOIS models

There are two standard models to run WHOIS:

- A **thin** registry only includes **technical data** sufficient to identify the sponsoring registrar, status, and dates for each registration (e.g., .com, .net).
- **Thick** registries maintain the **registrant's contact** information and designated administrative and **technical contact** information, in addition to the sponsoring registrar and status details (e.g., .club, .org).

ICANN accredited **registrars** are **maintaining** a **WHOIS** service to sponsor gTLD domains if the operating registry is **thin**. Almost all gTLDs have a thick WHOIS.

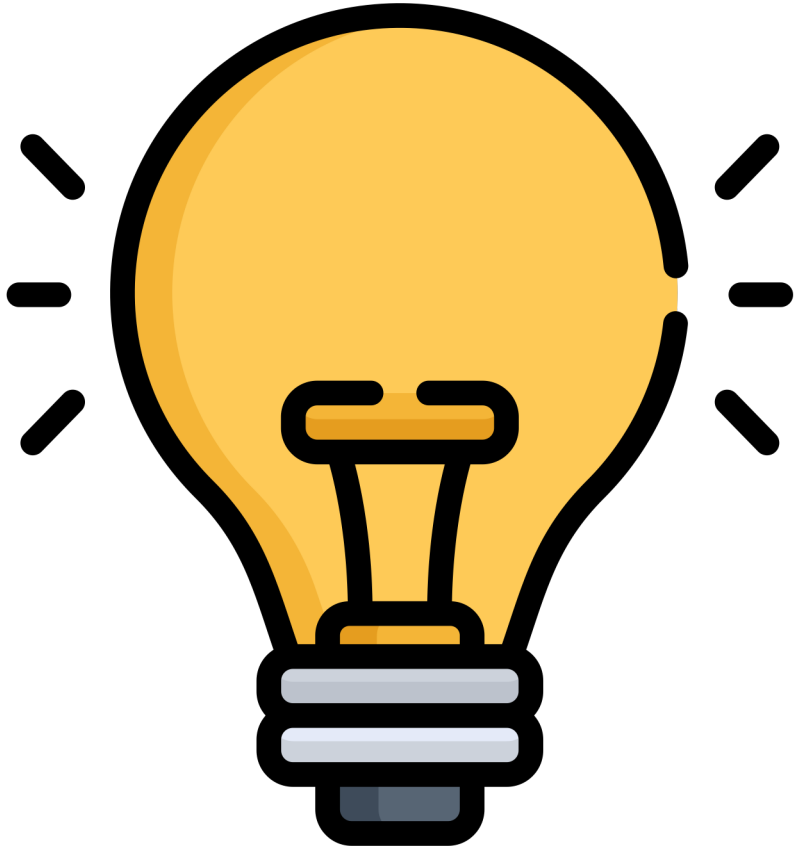
How is WHOIS working?



Source: https://whois.icann.org/en/dns-and-whois-how-it-works - Effective 03/2016

WHOIS has been in the spotlight

It can **create privacy issues** that are tied to free speech and anonymity. According to law enforcement, it is a vital tool to investigate spam and phishing and to track down the domain name holder.



Registries and registrars are restricting access to their WHOIS, and especially ccTLD registries are protecting the data by **disclosing** only the bare minimum of information. In contrast, gTLD registries and registrars are bound by ICANN contracts to provide **complete** and **validated contact details**.

Accuracy of Information #1

ICANN is enforcing Registrars to provide **complete**, **validated**, and **verified** WHOIS **data** for gTLD domains. That includes the presence of data for all fields in a proper format and to verify either the email address or the telephone number of the domain name holder.

Many ccTLDs Registries are also imposing Registrars to do the same that they are doing for gTLDs. However, some ccTLDs are preforming their checks, such as local address databases.s

Accuracy of Information #2

If WHOIS information found to be **inaccurate**, the registrant is compelled to update its data. If this fails because the registrant is not reachable, then this could **lead** to a **suspension**.

GDPR

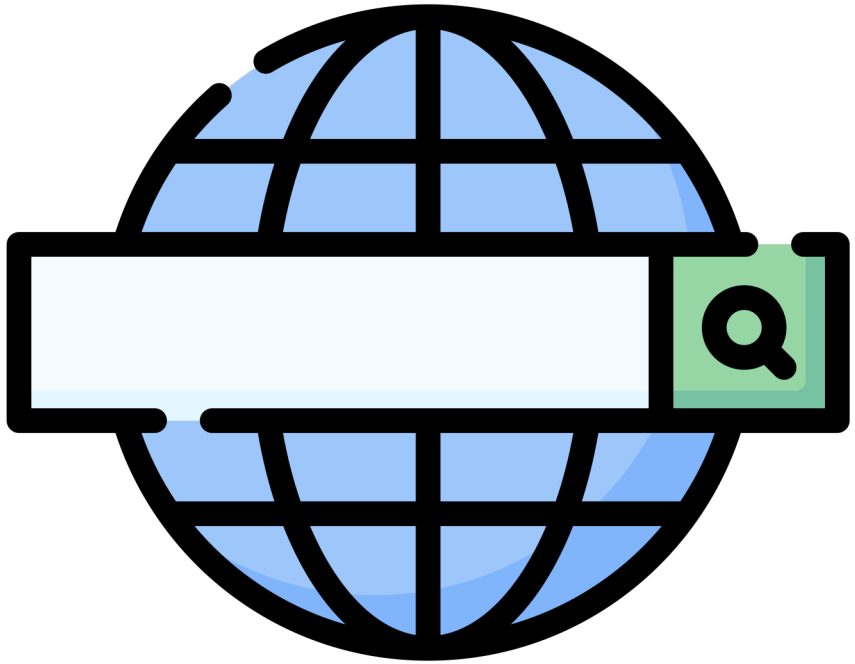
In 2018 the General Data Protection Regulation (GDPR) by the European Union came into effect.

Based on that, all most all registries and registrars were legally forced to **redact information** provided by WHOIS. ICANN took this into account with the Temporary Specification and kicked off a Policy Development Process (PDP) to address the issue.

Ways are being sought to handle legitimate information claims of third parties.

RDAP as a successor

Registration Data Access Protocol (RDAP) is a **protocol** standardized by the Internet Engineering Task Force (IETF) in 2015. It is a **successor** to the **WHOIS** protocol to look up relevant registration data from such Internet resources as domain names, IP addresses, and autonomous system numbers.



Since 2019 it is **obligated** to run an RDAP service for all Internet Corporation for Assigned Names and Numbers (ICANN) accredited Registrars and Registry Operators.

Future of WHOIS

The successor of WHOIS is already live. However, the old WHOIS system is **still up and running**. ICANN has not yet taken it out of service.

Nevertheless, the term WHOIS to look up information on domain names, IP addresses, and AS numbers will not vanish because it has become a universal language even if ICANN now calls it Registration Data Directory Services (RDDS).

Thank you!

Icon made by Freepik from www.flaticon.com