Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Technology Summaries
WHOIS and RDAP

July 2026

What WHOIS and RDAP are:

WHOIS and Registration Data Access Protocol (RDAP) are online directories that identify who is associated with specific domain names, IP addresses, and autonomous system numbers (ASNs). In many cases, public WHOIS data is required[1] to be provided and maintained accurately.

WHOIS and RDAP can be accessed via command-line programs, a web browser, or programming languages such as Python. See the References section at the bottom of this document for tools to access WHOIS and RDAP.

WHOIS and RDAP represent two different ways of delivering the same information:

- WHOIS[2] is the original registration data delivery protocol. It is a simple text-querying system that provides quasi-normalized data about various contacts associated with a domain, IP address, or ASN.
- RDAP[3], introduced in 2015, is the current registration data delivery protocol. RDAP output is delivered in JavaScript Object Notation (JSON) format[4], designed for automated parsing and processing.

As of January 27, 2025[5], the Internet Corporation for Assigned Names and Numbers (ICANN) no longer requires WHOIS in its contracted generic top-level domains (gTLDs), with RDAP serving as its replacement[6]. As a result, many gTLDs now only offer RDAP.

What WHOIS and RDAP are used for:

- Locate contact information for a "responsible person" when investigating a problem.
- Research individuals or organizations that may control or be responsible for large numbers of domains or IP addresses.
- Identify data points to enrich cyber threat intelligence investigations.

WHOIS and RDAP limitations:

- Data is often redacted due to privacy laws and regulations.
- Data may not be accurate or complete.
- IP address data usually identifies the provider, rather than the individual customer.
- Data may not be easily parsed, especially in country code top-level domains (ccTLDs). Further, with RDAP, data may not be interpreted consistently.
- Requests are often rate-limited to a small number of queries per time period and/or IP address.

References:

Sampling of tools for accessing WHOIS and RDAP:

Command Line Clients	**ICANN and Regional Internet Registry (RIR) Web Interfa**
OpenRDAP: https://www.openrdap.org/ RDAP: https://pypi.org/project/rdap/ whois-rdap: https://github.com/ntblk/whois-rdap Package managers such as apt for Linux or Homebrew for Mac can also be used to install clients.	ICANN: https://lookup.icann.org/en/lookup ARIN: https://search.arin.net/rdap/?query=*nn.nn.nn.nn* RIPE: https://rdap.db.ripe.net/ip/*nn.nn.nn.nn* APNIC: https://rdap-web.apnic.net/ip/*nn.nn.nn.nn* LACNIC: https://rdap-web.lacnic.net/rdap/ip/*nn.nn.nn.nn* AFRINIC: https://rdap.afrinic.net/rdap/ip/*nn.nn.nn.nn*

[1]ICANN Policy Issue Brief – gTLD WHOIS
[2]RCF 3912 WHOIS Protocol Specification
[3]RCF 7482 Registration Data Access Protocol (RDAP) Query Format
[4]RCF 7483 JSON Responses for the Registration Data Access Protocol (RDAP)
[5]ICANN Update: Launching RDAP; Sunsetting WHOIS
[6]Bitbucket NRO RDAP Profile

As with all documents we publish, please check the M[3]AAWG website www.m3aawg.org for updates.