whois — Professional Cheat Sheet

> **Compact professional reference** for `whois` and RDAP — domain & IP registration lookup. Quick commands, server details, interpretation tips, automation notes, and OPSEC for investigators and pentesters.

---

1) At-a-glance

- **Tools:** `whois` (traditional port 43 WHOIS protocol) and **RDAP** (Registration Data Access Protocol — JSON over HTTPS, replaces WHOIS in many registries).
- **Primary uses:** Identify domain registrant, registrar, creation/expiry dates, name servers, registrar contacts, registry-specific data, and abuse contacts for takedown/coordination.
- **Note:** WHOIS output is unstandardized and varies by TLD; RDAP provides structured JSON and is preferred for automation where supported.

---

2) Install / availability

```
# Debian/Ubuntu
sudo apt update && sudo apt install whois

# macOS (Homebrew)
brew install whois

# Windows
# Use Sysinternals 'whois.exe' or PowerShell modules / online RDAP APIs
```

---

3) Basic usage

```
# Query a domain
whois example.com

# Query an IP (registrar/owner info depends on RIR)
whois 8.8.8.8

# Query a specific WHOIS server
whois -h whois.verisign-grs.com example.com
```

RDAP (JSON) examples (use curl):

```
# Query RDAP for a domain (ICANN RDAP service)
curl https://rdap.org/domain/example.com

# Query RIR RDAP for IP information
curl https://rdap.arin.net/registry/ip/8.8.8.8
```

---

4) Important flags & options (BSD/Linux `whois`)

- `-H` : hide legal disclaimers in output.
- `-h server` : query specific WHOIS server.
- `-p port` : specify non-standard port.
- `-i` : inverse lookup (find domains by registrant; availability depends on server).
- `-r` : disable recursion (don't follow referrals).
- `--verbose` / `-V` : show additional debug info (varies by implementation).
- `--version` : show version.

Note: flags vary between whois implementations — check `man whois` on your system.

---

5) Who answers WHOIS queries (registry architecture)

- **Registrar WHOIS:** registrar (e.g., GoDaddy) often provides enriched contact info.
- **Registry WHOIS:** TLD operator (e.g., Verisign for .com) is authoritative for certain fields and typically returns referrals to registrars.
- **RIR WHOIS / RDAP:** Regional Internet Registries (ARIN, RIPE, APNIC, AFRINIC, LACNIC) handle IP allocation data.

---

6) What to look for (interpretation)

- **Registrar & Registry:** who registered the domain and where to manage it.
- **Registrant / Org:** WHOIS may show a person/org (but often redacted or privacy-protected).
- **Dates:** `Creation`, `Updated`, `Expiry` — use expiry to detect abandoned domains.
- **Name servers:** used to find hosting / CDN providers.
- **Referral/Registrar WHOIS server:** follow to get more fields.
- **Abuse/contact email:** for reporting malicious content.
- **Status codes:** e.g., `clientTransferProhibited`, `ok`, `redemptionPeriod` — indicate lock or redemption states.

---

7) RDAP advantages (automation)

- **Structured JSON** makes parsing reliable (no brittle regex).

- Supports standardized roles, event history, and links.
- Use `curl` + `jq` for programmatic data extraction:

```
curl -s https://rdap.org/domain/example.com | jq '.entities[] |
{role: .roles, vcard: .vcardArray}'
```

---

8) Practical examples & one-liners

```
# Domain WHOIS quick (default server)
whois example.com

# Follow registrar referral (show full chain)
whois -H example.com

# Query Verisign for .com data
whois -h whois.verisign-grs.com example.com

# RDAP + jq: extract registrant name and emails
curl -s https://rdap.org/domain/example.com | jq '.entities[] | select(.roles!
=null) | {roles: .roles, vcard: .vcardArray[1]}

# IP owner (ARIN/RDAP)
curl -s https://rdap.arin.net/registry/ip/8.8.8.8 | jq
'.name, .handle, .entities'

# Bulk whois (list of domains)
while read d; do echo "--- $d ---"; whois "$d" | egrep 'Registrant|Registrar|
Name Server|Creation Date|Expiry'; done < domains.txt
```

---

9) Rate limiting & throttling

- Public WHOIS/RDAP services often rate-limit queries. Respect limits and cache results for repeated lookups.
- Use official RDAP endpoints where possible and respect `Retry-After` headers.
- For bulk investigations, consider paid APIs (whoisxmlapi, DomainTools, SecurityTrails) that offer higher throughput and structured output.

---

10) Use cases in investigations & pentests

- **Attribution:** map registrant, registrar, and hosting to find responsible parties.

- **Phishing takedown:** identify abuse contact and registrar to request removal.
- **Asset inventory:** discover related domains by registrant contact, name servers, or contact patterns.
- **Temporal analysis:** compare `creation` / `expiry` dates to spot domain reuse.

---

11) Privacy, GDPR & redaction

- Many registrars redact personal registrant data (GDPR/PrivacyShield) and show privacy/relay contacts instead.
- RDAP may include role-based contacts and limited info; use registrar abuse contacts for takedowns.

---

12) Automation & tooling recommendations

- **RDAP + jq** for structured lookups.
- **APIs**: WhoisXMLAPI, DomainTools, SecurityTrails for bulk / historical whois / reverse WHOIS.
- **Chain with other OSINT**: feed whois/RDAP outputs to SpiderFoot, theHarvester, or custom scripts to enrich results.

---

13) Common pitfalls & troubleshooting

- **Inconsistent fields:** WHOIS text formats differ by TLD — avoid brittle parsing.
- **Privacy-protected data:** registrantメールs often replaced by privacy service — use registrar for escalation.
- **Registry referrals:** a WHOIS client that follows referrals (or explicit `-h` queries) will reveal more fields.
- **Internationalized domain names (IDN):** query punycode form (`xn--...`) to get accurate WHOIS.

---

14) Quick checklist before reporting abuse

1. Verify ownership via registrar/rdap.
2. Identify registrar abuse contact and registry abuse contact.
3. Collect evidence (screenshots, timestamps, HTTP headers).
4. Send polite, factual takedown request including proof and preferred remediation.

---

15) One-line cheats (copy-paste)

```
whois example.com
whois -h whois.verisign-grs.com example.com
curl -s https://rdap.org/domain/example.com | jq
curl -s https://rdap.arin.net/registry/ip/8.8.8.8 | jq
```

```
while read d; do whois $d | egrep 'Registrar|Registrant|Name Server|Creation
Date|Expiry'; done < domains.txt
```

This cheat sheet is for lawful investigations, incident handling and reconnaissance in authorized engagements. Always comply with local laws and registrar policies.