🌐 Whois – Ultimate Cheat Sheet

🔷 1. Basics

Syntax

whois [options] domain/ip

Example

whois example.com

🔷 2. Common Use Cases

Target Type	Command Example
Domain	whois example.com
IP Address	whois 8.8.8.8
ASN (Autonomous System)	whois AS15169

🔷 3. Useful Options

Option	Description
-h host	Query specific WHOIS server
-p port	Specify port (default: 43)
-H	Suppress legal disclaimers
-r	Disable recursion (do not follow referrals)
--verbose	Verbose output

🔷 4. Query Specific WHOIS Servers

Example: Query VeriSign for .com

whois -h whois.verisign-grs.com example.com

Example: Query RIPE (for IPs in Europe)

whois -h whois.ripe.net 1.1.1.1

Example: Query ARIN (for IPs in North America)

whois -h whois.arin.net 8.8.8.8

🔷 5. Finding Correct WHOIS Server

- .com, .net → whois.verisign-grs.com
- .org → whois.pir.org
- IP (North America) → whois.arin.net
- IP (Europe) → whois.ripe.net
- IP (Asia-Pacific) → whois.apnic.net
- IP (Latin America) → whois.lacnic.net
- IP (Africa) → whois.afrinic.net

🔷 6. Advanced Usage

Get domain creation + expiry date

whois example.com | grep -Ei "Creation Date|Expiry Date|Registrar"

Extract name servers only

whois example.com | grep -Ei "Name Server"

Find owner's organization

whois 8.8.8.8 | grep -Ei "OrgName|Organization"

🔷 7. Automating Queries

Check multiple domains from a file

for domain in $(cat domains.txt); do whois $domain | grep -i "Creation Date"; done

Extract registrar info for multiple domains

for d in $(cat domains.txt); do echo "Domain: $d"; whois $d | grep -Ei "Registrar:"; done

---

🔷 8. Whois + Other Tools

Tool	Use Case
dig	DNS records lookup
nslookup	Basic DNS queries
host	Simple hostname → IP resolution
traceroute	Path analysis of IP/domain
theHarvester	OSINT automation with WHOIS & DNS

🔷 9. Example Workflow

1. Check **domain info**
2. whois example.com
3. Check **IP ownership**
4. whois 93.184.216.34
5. Extract **registrar, nameservers, expiration**
6. whois example.com | egrep "Registrar|Name Server|Expiry"

🔷 10. Tips & Notes

- Always query the **right WHOIS server** for accuracy.
- Domain privacy services may hide owner info.
- For automation, combine with grep, awk, sed.
- Use --verbose if registry provides extended data.