Day 15 - WHOIS & DNS Tools — Intro & Hands-On

What is WHOIS?

WHOIS is a protocol used to retrieve information about domain registrations.

- You can find:
  - Who owns a domain
  - Contact info (admin, tech)
  - Domain creation & expiry dates
  - Registrar (e.g., GoDaddy, Namecheap)

What is DNS?

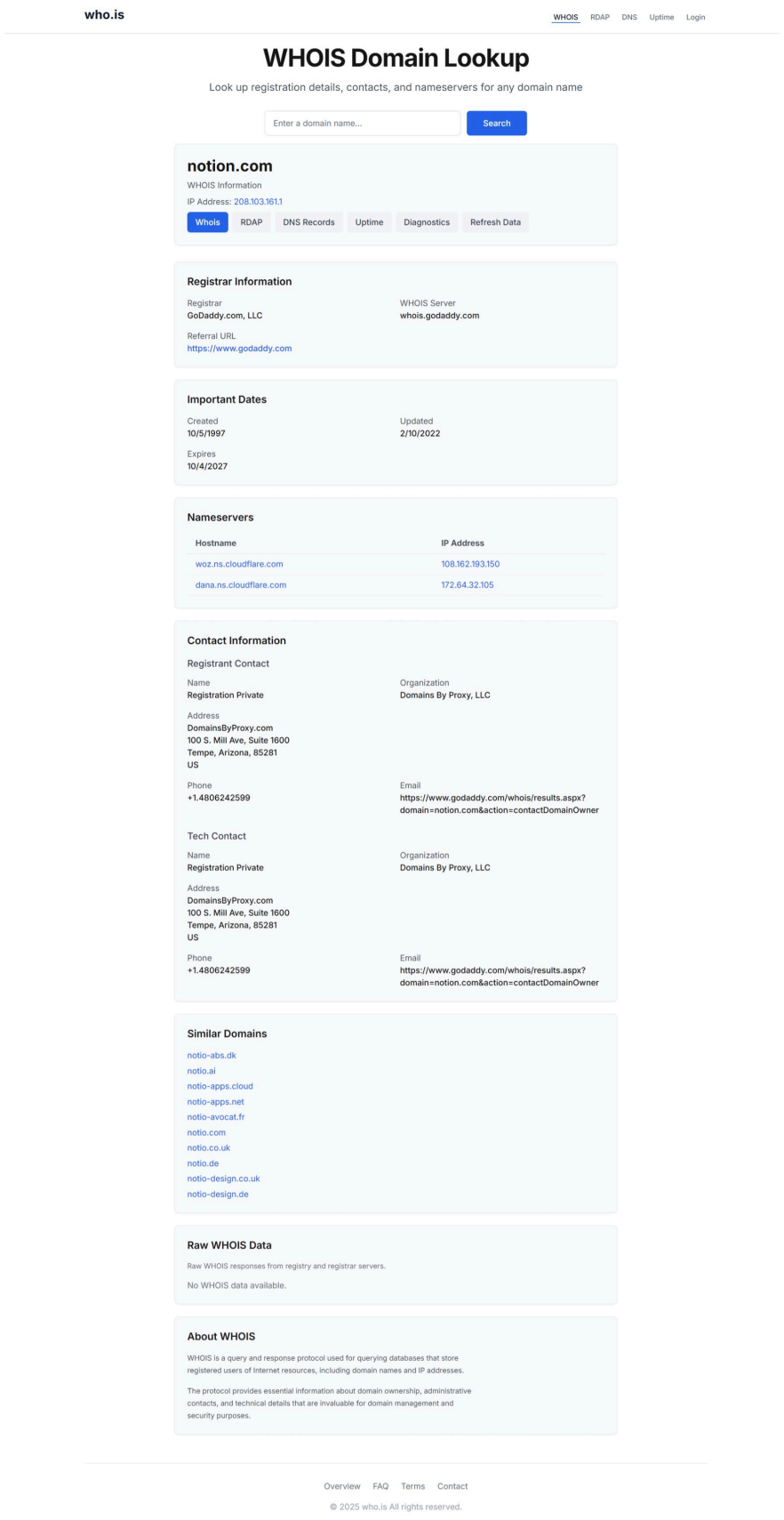
DNS (Domain Name System) converts domain names (like `google.com`) into IP addresses (like `142.250.64.14`).

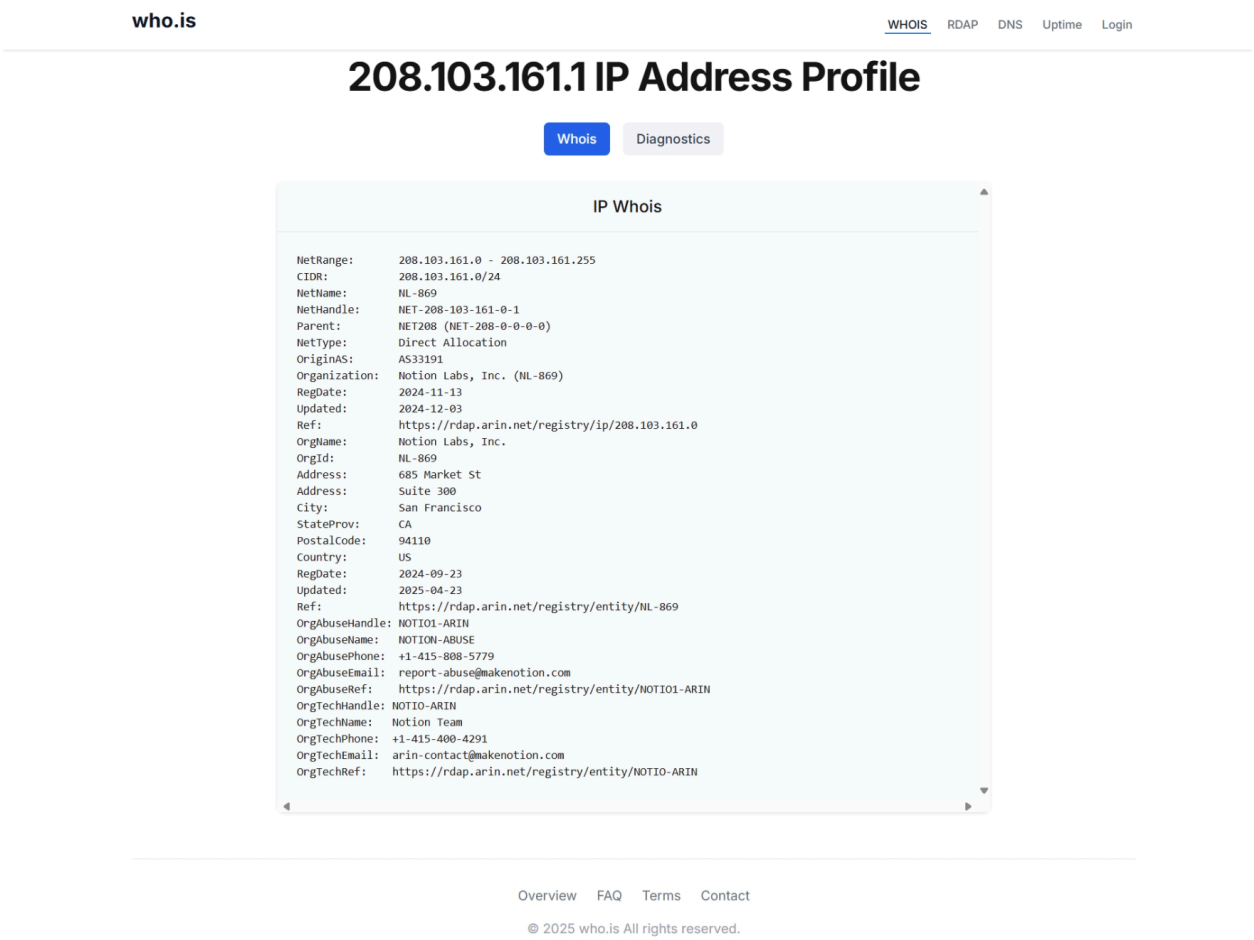
Practical Tasks

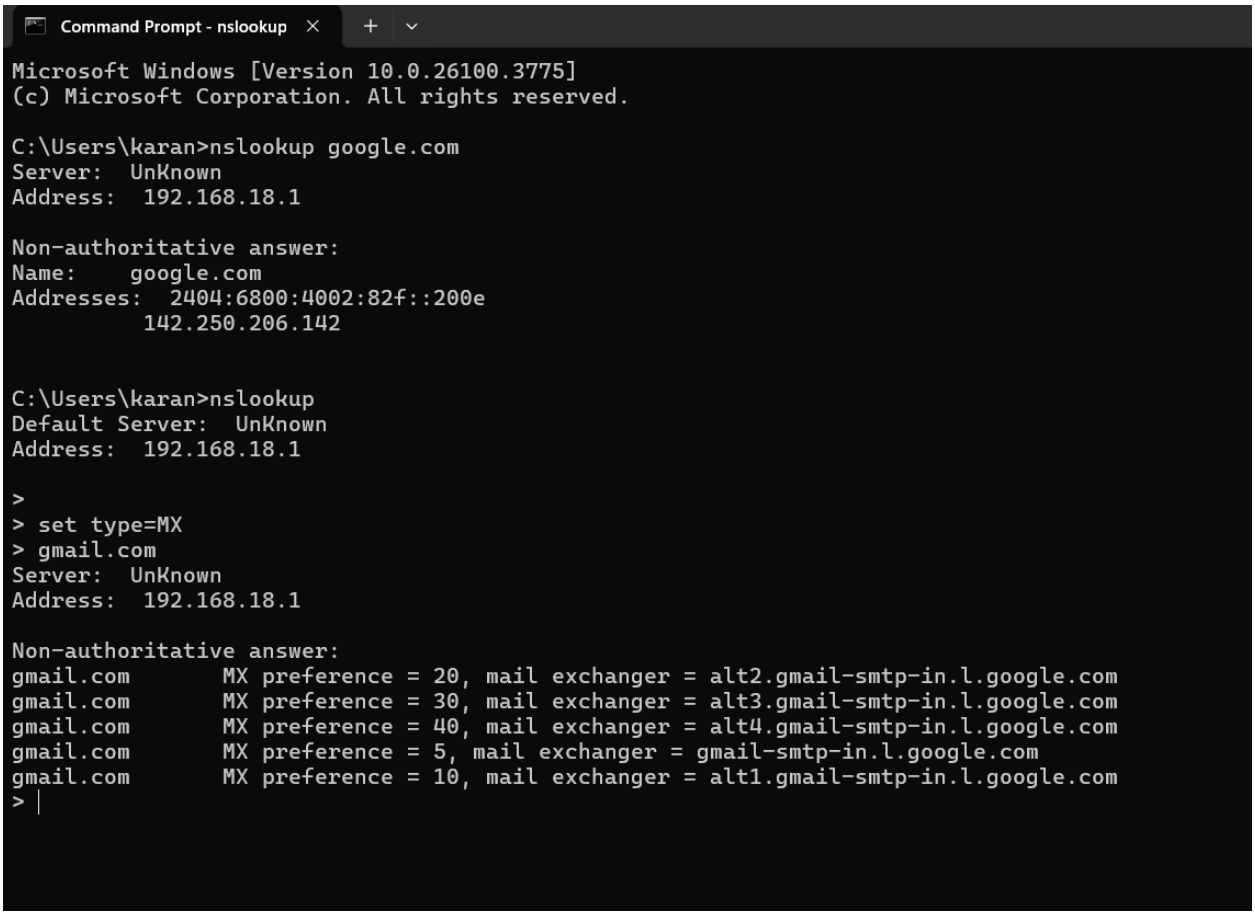
Task	Tool/Website	Description
Lookup WHOIS	who.is / ICANN WHOIS	Enter a domain and review ownership info
Use `nslookup`	Command Line	`nslookup domain.com` — check IP address

- Use `nslookup` with DNS record types:

```
nslookup
> set type=MX
> gmail.com
```


who.is
WHOIS
RDAP
DNS
Uptime
Login
WHOIS Domain Lookup
Look up registration details, contacts, and nameservers for any domain name
Enter a domain name...
Search
notion.com
WHOIS Information
IP Address: 208.103.161.1
Whois
RDAP
DNS Records
Uptime
Diagnostics
Refresh Data
Registrar Information
Registrar
GoDaddy.com, LLC
WHOIS Server
whois.godaddy.com
Referral URL
https://www.godaddy.com
Important Dates
Created
10/5/1997
Updated
2/10/2022
Expires
10/4/2027
Nameservers
Hostname
IP Address
woz.ns.cloudflare.com
108.162.193.150
dana.ns.cloudflare.com
172.64.32.105
Contact Information
Registrant Contact
Name
Registration Private
Organization
Domains By Proxy, LLC
Address
DomainsByProxy.com
100 S. Mill Ave, Suite 1600
Tempe, Arizona, 85281
US
Phone
+1.4806242599
Email
https://www.godaddy.com/whois/results.aspx?domain=notion.com&action=contactDomainOwner
Tech Contact
Name
Registration Private
Organization
Domains By Proxy, LLC
Address
DomainsByProxy.com
100 S. Mill Ave, Suite 1600
Tempe, Arizona, 85281
US
Phone
+1.4806242599
Email
https://www.godaddy.com/whois/results.aspx?domain=notion.com&action=contactDomainOwner
Similar Domains
notio-abs.dk
notio.ai
notio-apps.cloud
notio-apps.net
notio-avocat.fr
notio.com
notio.co.uk
notio.de
notio-design.co.uk
notio-design.de
Raw WHOIS Data
Raw WHOIS responses from registry and registrar servers.
No WHOIS data available.
About WHOIS
WHOIS is a query and response protocol used for querying databases that store registered users of Internet resources, including domain names and IP addresses.
The protocol provides essential information about domain ownership, administrative contacts, and technical details that are invaluable for domain management and security purposes.
Overview
FAQ
Terms
Contact
© 2025 who.is All rights reserved.


who.is
WHOIS
RDAP
DNS
Uptime
Login
208.103.161.1 IP Address Profile
Whois
Diagnostics
IP Whois
NetRange: 208.103.161.0 - 208.103.161.255
CIDR: 208.103.161.0/24
NetName: NL-869
NetHandle: NET-208-103-161-0-1
Parent: NET208 (NET-208-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS33191
Organization: Notion Labs, Inc. (NL-869)
RegDate: 2024-11-13
Updated: 2024-12-03
Ref: https://rdap.arin.net/registry/ip/208.103.161.0
OrgName: Notion Labs, Inc.
OrgId: NL-869
Address: 685 Market St
Address: Suite 300
City: San Francisco
StateProv: CA
PostalCode: 94110
Country: US
RegDate: 2024-09-23
Updated: 2025-04-23
Ref: https://rdap.arin.net/registry/entity/NL-869
OrgAbuseHandle: NOTIO1-ARIN
OrgAbuseName: NOTION-ABUSE
OrgAbusePhone: +1-415-808-5779
OrgAbuseEmail: report-abuse@makenotion.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/NOTIO1-ARIN
OrgTechHandle: NOTIO-ARIN
OrgTechName: Notion Team
OrgTechPhone: +1-415-400-4291
OrgTechEmail: arin-contact@makenotion.com
OrgTechRef: https://rdap.arin.net/registry/entity/NOTIO-ARIN
Overview
FAQ
Terms
Contact
© 2025 who.is All rights reserved.



Why It's Useful in Cybersecurity:

- You can check **who handles email** for a domain (helps detect spoofed or misconfigured servers).
- DNS tools help **trace phishing**, **detect spoofed domains**, and spot **DNS misconfigurations**.