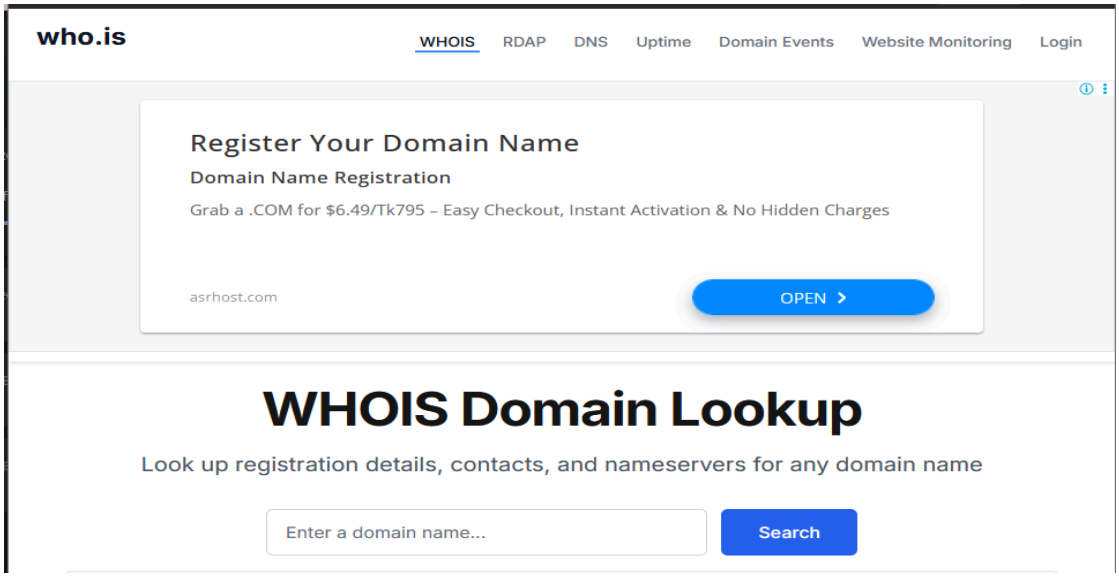
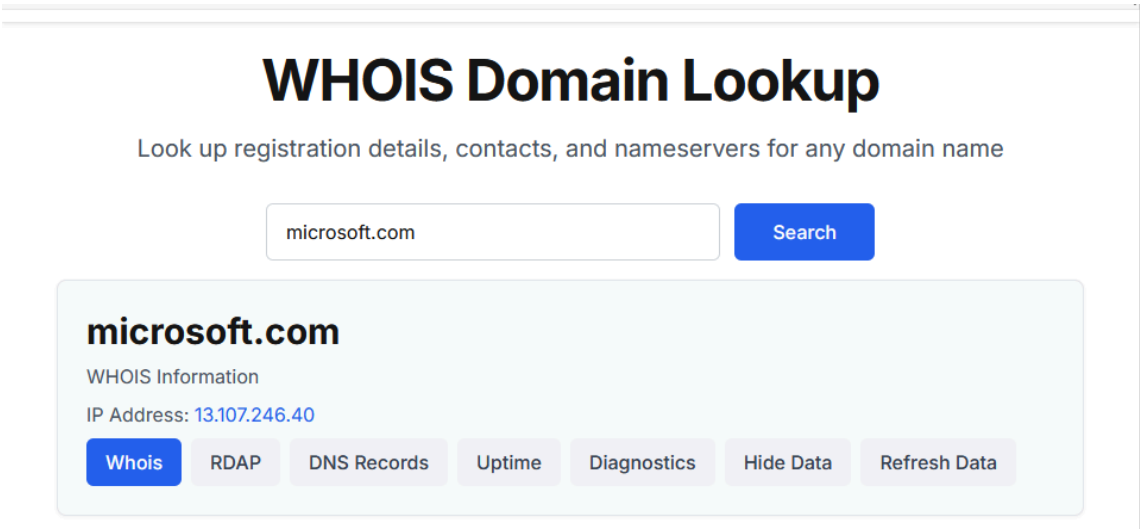
WHOIS & DNS RECON

WHAT ARE WHOIS RECORDS?
WHOIS records provided detailed info about the registered owner of a domain name, including contact details, registration dates, and the domain's status. These records are accessible through WHOIS databases maintained by domain registrars and registry organizations.

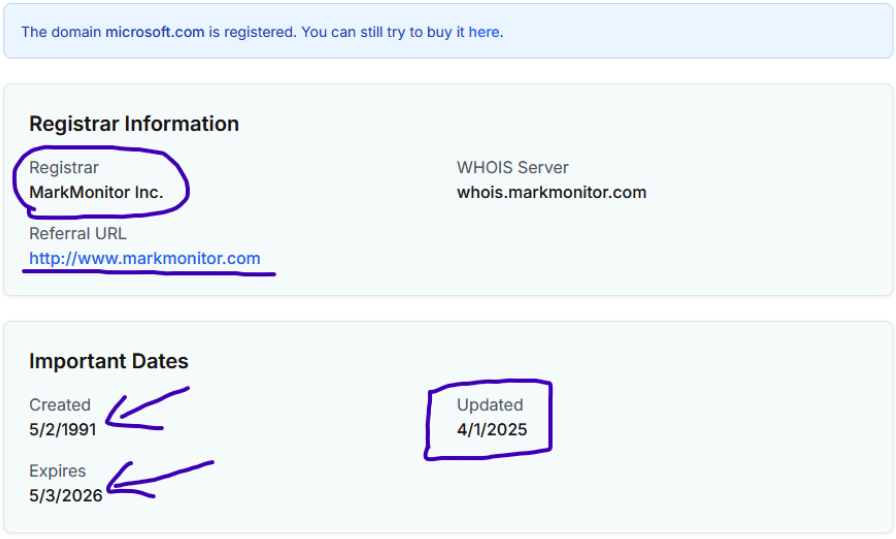
Practically check:



This is the website for looking up any domain information.



Now check about microsoft.com.



See which company are registered it and which server are they use, Also about Their expiry and create, updated date

Nameservers

Hostname	IP Address
ns1-39.azure-dns.com	150.171.10.39
ns2-39.azure-dns.net	150.171.16.39
ns3-39.azure-dns.org	13.107.222.39
ns4-39.azure-dns.info	13.107.206.39

And some DNS related information

Raw WHOIS responses from registry and registrar servers.

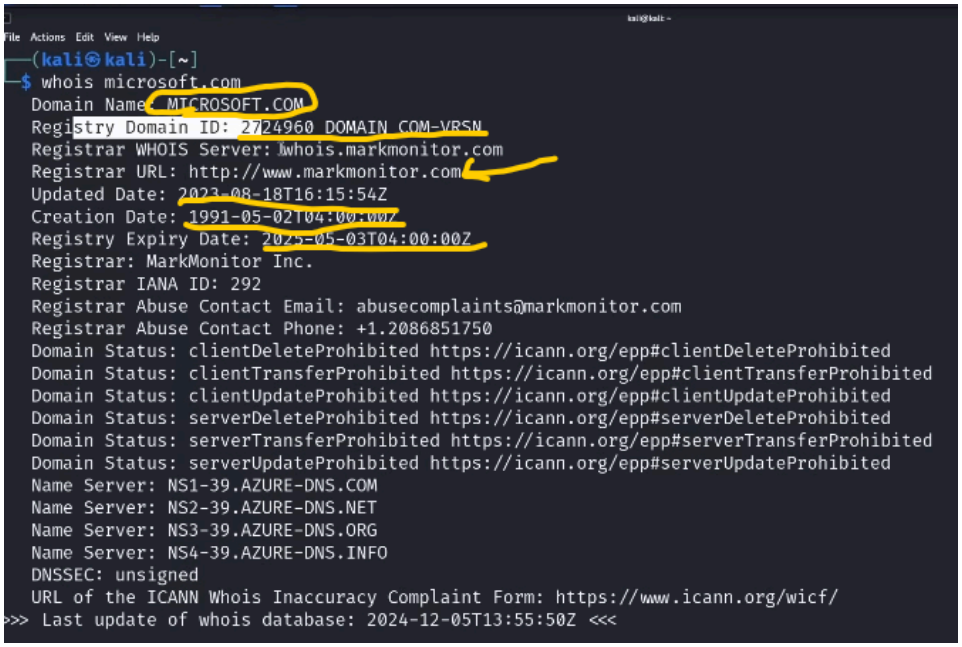
Raw Registry WHOIS Data

```
Domain Name: MICROSOFT.COM
   Registry Domain ID: 2724960_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2025-04-01T12:38:29Z
   Creation Date: 1991-05-02T04:00:00Z
   Registry Expiry Date: 2026-05-03T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1-39.AZURE-DNS.COM
   Name Server: NS2-39.AZURE-DNS.NET
   Name Server: NS3-39.AZURE-DNS.ORG
   Name Server: NS4-39.AZURE-DNS.INFO
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-10-31T08:12:28Z <<<
```

Raw Registrar WHOIS Data

```
Domain Name: microsoft.com
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2025-04-01T12:38:29+0000
Creation Date: 1991-05-02T04:00:00+0000
Registrar Registration Expiration Date: 2026-05-03T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: admin@domains.microsoft
Tech Name: MSN Hostmaster
Tech Phone: +1.4258828080
Tech Email: msnhst@microsoft.com
Name Server: ns1-39.azure-dns.com
Name Server: ns4-39.azure-dns.info
Name Server: ns3-39.azure-dns.org
Name Server: ns2-39.azure-dns.net
```

Some RAW data which contains their address, number, email etc..



Even by using the terminal of linux whois microsoft.com and it shows the same details like that website.

WHAT IS DNS?

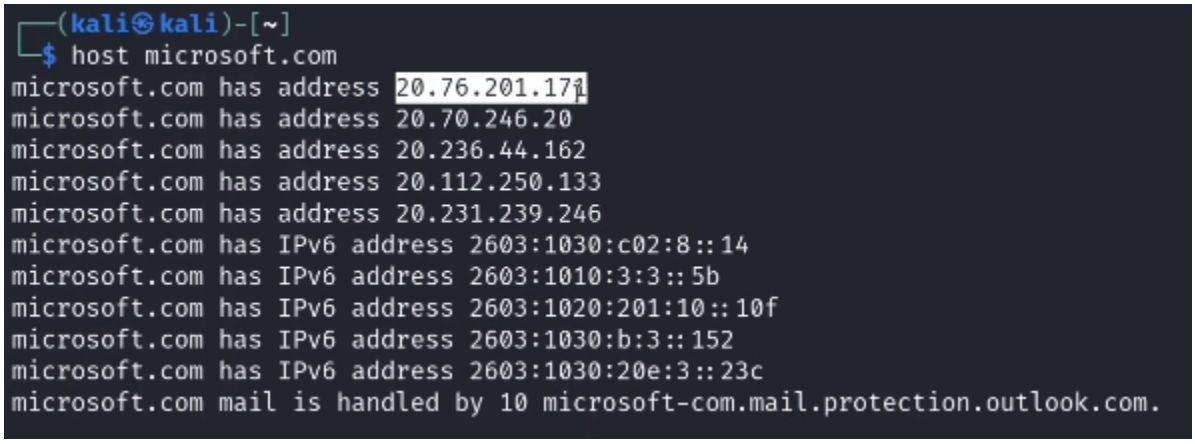
DNS (Domain Name System) records tell the internet how to reach your website, email server, or other online services by connecting human-readable domain names (like `example.com`) to IP addresses and services.

Types of DNS Records:

Record Type	Full Form	Purpose	Example
A Record	Address Record	Maps a domain to an IPv4 address.	`example.com → 192.168.1.1`
AAAA Record	IPv6 Address Record	Maps a domain to an IPv6 address	`example.com → 2400:cb00:2048:1::c629:d7a2`
CNAME Record	Canonical Name Record	Makes one domain an alias of another. Useful for subdomains.	`www.example.com → example.com`
NS Record	Name Server Record	Tells which name servers control our domain's settings.	`example.com → ns1.hosting.com`
SOA Record	Start of Authority	Stores admin info about your domain (like when DNS was last updated)..	Tracks when DNS data changes
TXT Record	Text Record	Stores text data, usually for verification or email safety.	`"v=spf1 include:_spf.google.com ~all"`
MX Record	Mail Exchange Record	Send emails to the right mail server..	`example.com → mail.example.com`

In Short:

- **A / AAAA** → Connect our domain to an IP address.
- **CNAME** → Redirects one domain/subdomain to another.
- **NS** → Points to our DNS host.
- **SOA** → Holds admin and version info for the DNS zone.
- **TXT** → Holds text data for verification/security.
- **MX** → Routes email messages.



Here is iPV4, iPV6 addresses .But it has multiple IP addresses .Maybe they are using CNAME. If we check clearly and test every ip address then we can find a real ip.

```
┌──(kali㉿kali)-[~]
└─$ host -t ns microsoft.com
microsoft.com name server ns4-39.azure-dns.info.
microsoft.com name server ns1-39.azure-dns.com.
microsoft.com name server ns2-39.azure-dns.net.
microsoft.com name server ns3-39.azure-dns.org.

┌──(kali㉿kali)-[~]
└─$ host -t mx microsoft.com
microsoft.com mail is handled by 10 microsoft-com.mail.protection.outlook.com.

┌──(kali㉿kali)-[~]
└─$ host -t mx spotify.com
spotify.com mail is handled by 1 aspmx.l.google.com.
spotify.com mail is handled by 10 aspmx3.googlemail.com.
spotify.com mail is handled by 5 alt1.aspmx.l.google.com.
spotify.com mail is handled by 10 aspmx5.googlemail.com.
spotify.com mail is handled by 10 aspmx4.googlemail.com.
spotify.com mail is handled by 10 aspmx2.googlemail.com.
spotify.com mail is handled by 5 alt2.aspmx.l.google.com.
```

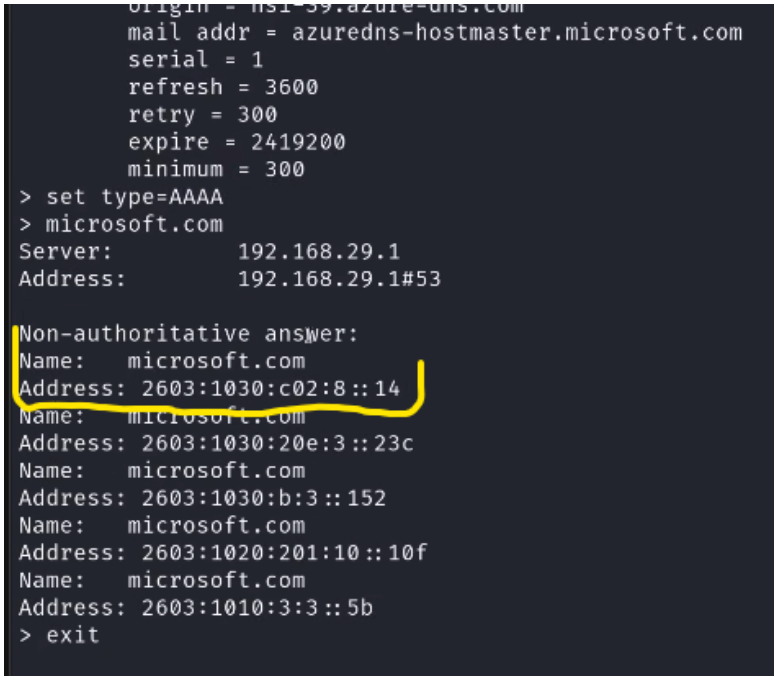
Using host -t ns microsoft.com then find some Name Server Record and that servers control microsoft domain's settings.
Using host -t mx microsoft.com find some Mail Exchange Record.

Also using this types command to collect same info:

```
┌──(kali㉿kali)-[~]
└─$ nslookup microsoft.com
Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
Name:   microsoft.com
Address: 20.231.239.246
Name:   microsoft.com
Address: 20.112.250.133
Name:   microsoft.com
Address: 20.236.44.162
Name:   microsoft.com
Address: 20.70.246.20
Name:   microsoft.com
Address: 20.76.201.171
Name:   microsoft.com
Address: 2603:1030:20e:3::23c
Name:   microsoft.com
Address: 2603:1030:b:3::152
Name:   microsoft.com
Address: 2603:1020:201:10::10f
Name:   microsoft.com
Address: 2603:1010:3:3::5b
```

```
┌──(kali㉿kali)-[~]
└─$ nslookup
> set type=ns
> microsoft.com
Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
microsoft.com   nameserver = ns4-39.azure-dns.info.
microsoft.com   nameserver = ns1-39.azure-dns.com.
microsoft.com   nameserver = ns2-39.azure-dns.net.
microsoft.com   nameserver = ns3-39.azure-dns.org.

Authoritative answers can be found from:
> set type=mx
> microsoft.com
Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
microsoft.com   mail exchanger = 10 microsoft-com.mail.protection.outlook.com.
```

```
┌──(kali㉿kali)-[~]
└─$ nslookup
> set type=CNAME
> microsoft.com
Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
*** Can't find microsoft.com: No answer

Authoritative answers can be found from:
microsoft.com
        origin = ns1-39.azure-dns.com
        mail addr = azuredns-hostmaster.microsoft.com
        serial = 1
        refresh = 3600
        retry = 300
        expire = 2419200
```


origin = ns1-39.azure-dns.com
mail addr = azuredns-hostmaster.microsoft.com
serial = 1
refresh = 3600
retry = 300
expire = 2419200
minimum = 300
> set type=AAAA
> microsoft.com
Server: 192.168.29.1
Address: 192.168.29.1#53
Non-authoritative answer:
Name: microsoft.com
Address: 2603:1030:c02:8::14
Name: microsoft.com
Address: 2603:1030:20e:3::23c
Name: microsoft.com
Address: 2603:1030:b:3::152
Name: microsoft.com
Address: 2603:1020:201:10::10f
Name: microsoft.com
Address: 2603:1010:3:3::5b
> exit