Whois Lookup

Overview

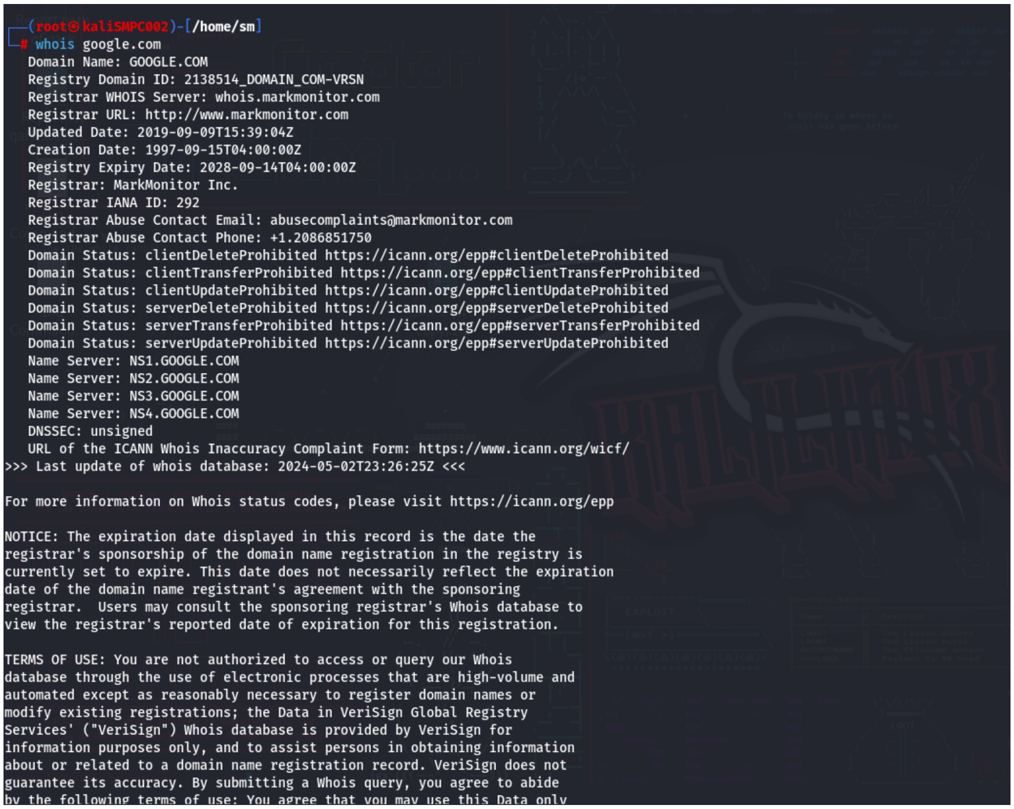
Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them. The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership. Whois records have proven to be extremely useful and have developed into an essential resource for maintaining the integrity of the domain name registration and website ownership process.

What is in a Whois record?

A Whois record contains all of the contact information associated with the person, group, or company that registers a particular domain name. Typically, each Whois record will contain information such as the name and contact information of the Registrant (who owns the domain), the name and contact information of the registrar Registrar (the organization or commercial entity that registered the domain name), the registration dates, the name servers, the most recent update, and the expiration date. Whois records may also provide the administrative and technical contact information (which is often, but not always, the registrant).

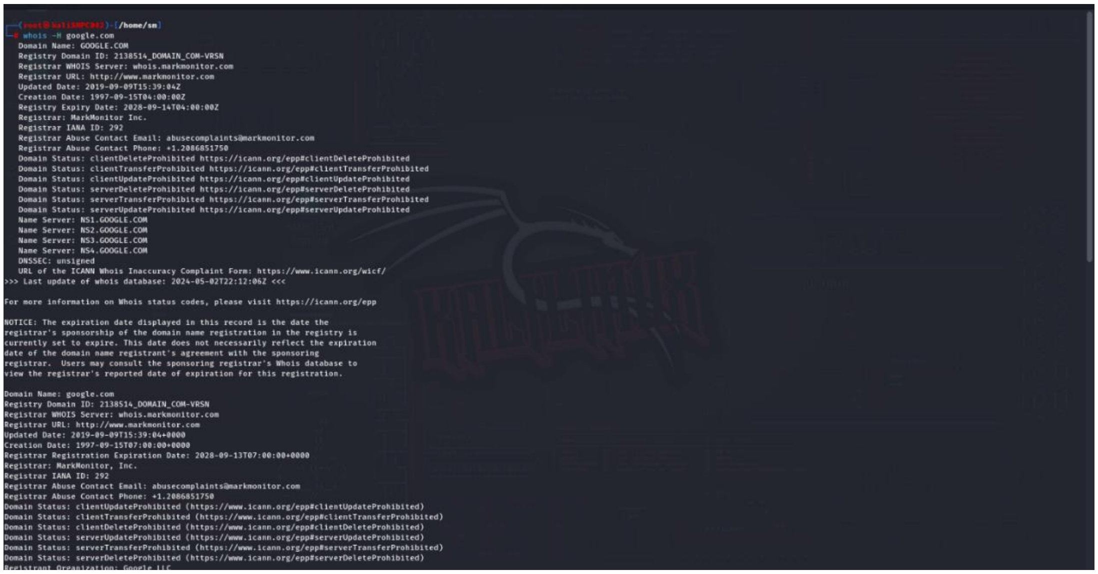
Whois Flags:

1. **whois:** The 'whois' command in Linux queries WHOIS servers to retrieve registration details like domain ownership, registrar, and expiration date for a specified domain name.



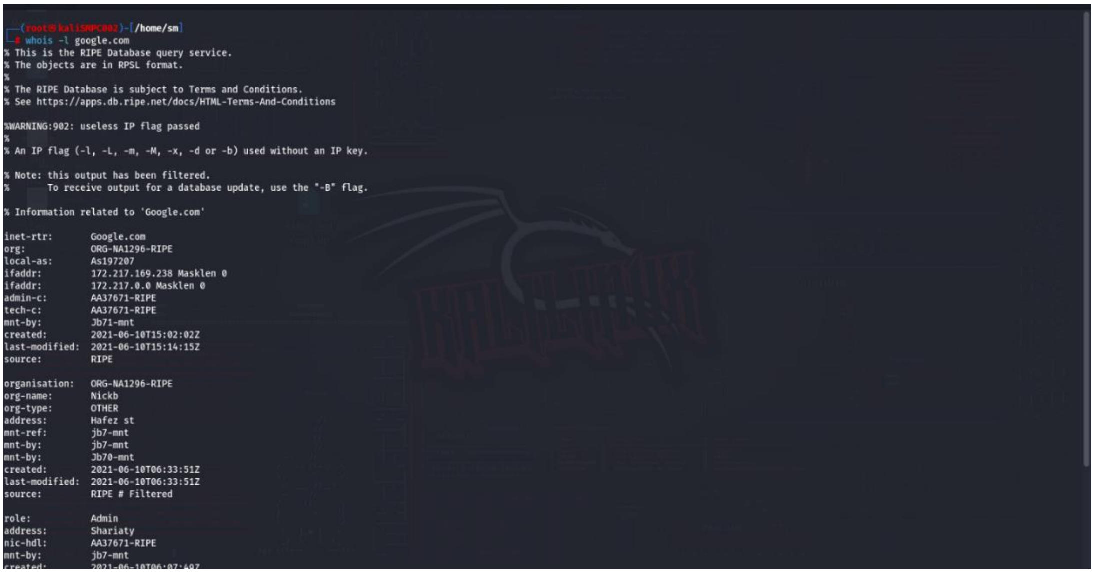
```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   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.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-05-02T23:26:25Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
```

2. **-H:** The -H option in the whois command allows specifying a custom WHOIS server to query for domain registration information, providing flexibility in server selection.



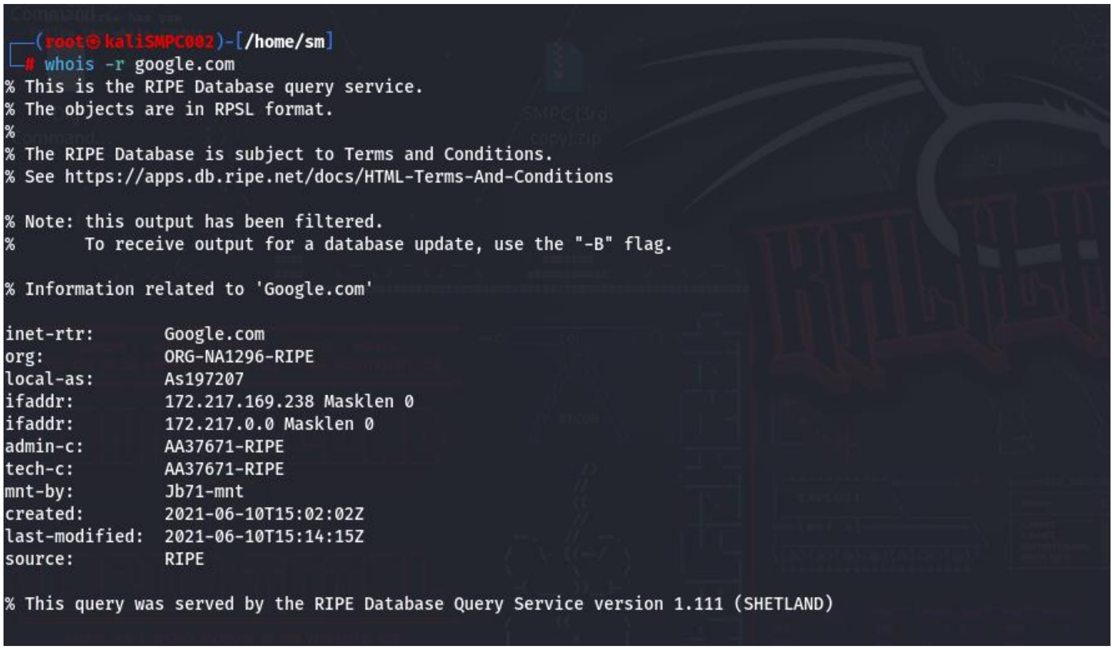
```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# whois -H google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   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.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-05-02T22:12:06Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+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 Organization: Google LLC
```

3. **-l:** The -l option in the whois command specifies the desired language for the WHOIS output, allowing users to retrieve information in a specific language if supported by the server.



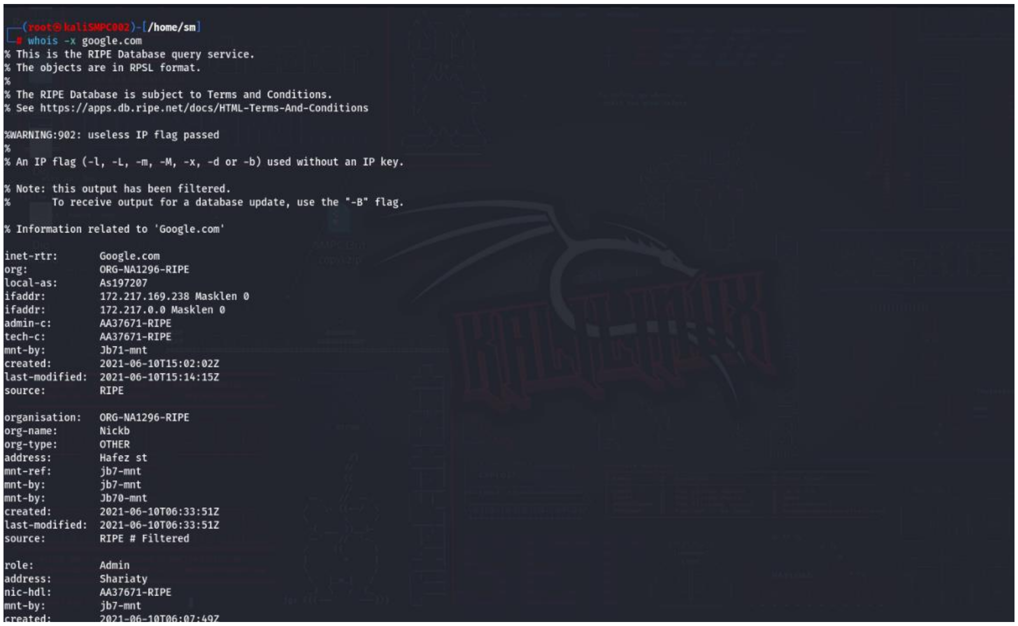
```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# whois -l google.com
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions

%WARNING:902: useless IP flag passed
%
% An IP flag (-l, -L, -m, -M, -x, -d or -b) used without an IP key.

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to 'Google.com'

inet-rtr:       Google.com
org:            ORG-NA1296-RIPE
local-as:       As197207
ifaddr:         172.217.169.238 Masklen 0
ifaddr:         172.217.0.0 Masklen 0
admin-c:        AA37671-RIPE
tech-c:         AA37671-RIPE
mnt-by:         Jb71-mnt
created:        2021-06-10T15:02:02Z
last-modified:  2021-06-10T15:14:15Z
source:         RIPE

organisation:   ORG-NA1296-RIPE
org-name:       Nickb
org-type:       OTHER
address:        Hafez st
mnt-ref:        jb7-mnt
mnt-by:         jb7-mnt
mnt-by:         Jb70-mnt
created:        2021-06-10T06:33:51Z
last-modified:  2021-06-10T06:33:51Z
source:         RIPE # Filtered

role:           Admin
address:        Shariaty
nic-hdl:        AA37671-RIPE
mnt-by:         jb7-mnt
created:        2021-06-10T06:07:49Z
```

4. **-r:** The -r option in the whois command enables referral mode, allowing the client to follow referrals to other WHOIS servers for more detailed information.



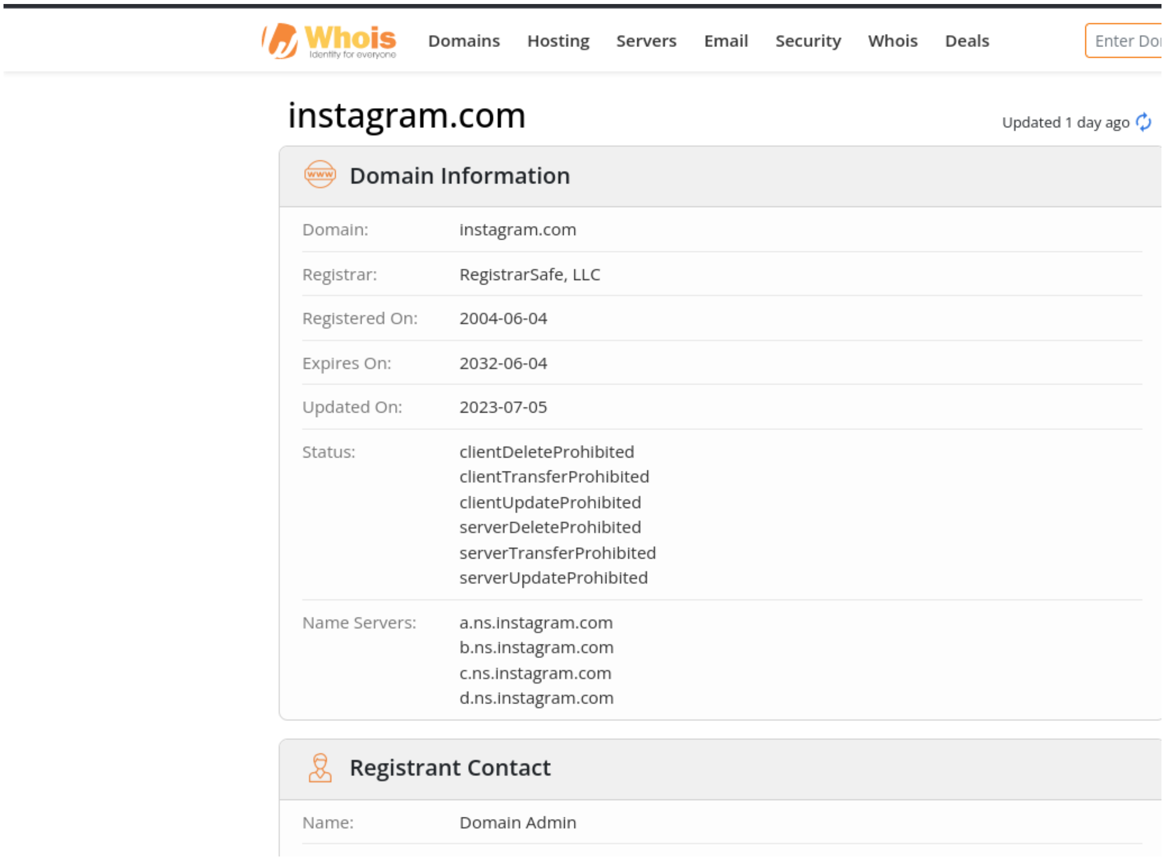
```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# whois -r google.com
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to 'Google.com'

inet-rtr:       Google.com
org:            ORG-NA1296-RIPE
local-as:       As197207
ifaddr:         172.217.169.238 Masklen 0
ifaddr:         172.217.0.0 Masklen 0
admin-c:        AA37671-RIPE
tech-c:         AA37671-RIPE
mnt-by:         Jb71-mnt
created:        2021-06-10T15:02:02Z
last-modified:  2021-06-10T15:14:15Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.111 (SHETLAND)
```

5. **-x:** The -x option in the whois command allows performing a reverse lookup, querying WHOIS servers for information based on an IP address rather than a domain name.



```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# whois -x google.com
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions

%WARNING:902: useless IP flag passed
%
% An IP flag (-l, -L, -m, -M, -x, -d or -b) used without an IP key.

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to 'Google.com'

inet-rtr:       Google.com
org:            ORG-NA1296-RIPE
local-as:       As197207
ifaddr:         172.217.169.238 Masklen 0
ifaddr:         172.217.0.0 Masklen 0
admin-c:        AA37671-RIPE
tech-c:         AA37671-RIPE
mnt-by:         Jb71-mnt
created:        2021-06-10T15:02:02Z
last-modified:  2021-06-10T15:14:15Z
source:         RIPE

organisation:   ORG-NA1296-RIPE
org-name:       Nickb
org-type:       OTHER
address:        Hafez st
mnt-ref:        jb7-mnt
mnt-by:         jb7-mnt
mnt-by:         Jb70-mnt
created:        2021-06-10T06:33:51Z
last-modified:  2021-06-10T06:33:51Z
source:         RIPE # Filtered

role:           Admin
address:        Shariaty
nic-hdl:        AA37671-RIPE
mnt-by:         jb7-mnt
created:        2021-06-10T06:07:49Z
```

6. **Web Interface**: Whois also provide a web based interface for user to have insight of domain scanning



instagram.com

Updated 1 day ago

Domain Information

Domain:	instagram.com
Registrar:	RegistrarSafe, LLC
Registered On:	2004-06-04
Expires On:	2032-06-04
Updated On:	2023-07-05
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	a.ns.instagram.com b.ns.instagram.com c.ns.instagram.com d.ns.instagram.com

Registrant Contact

Name:	Domain Admin