Vidyavardhini's College of Engineering and Technology, Vasai

Department of Computer Science & Engineering (Data Science)

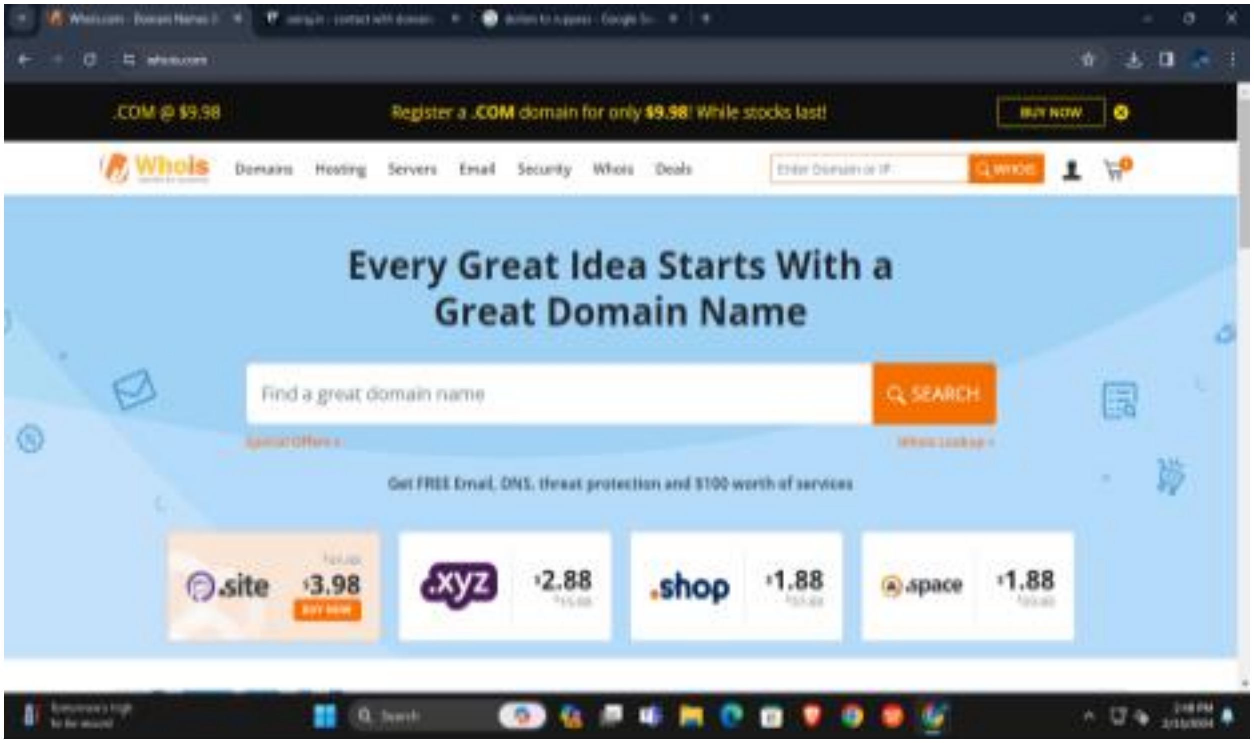
EXPERIMENT 06

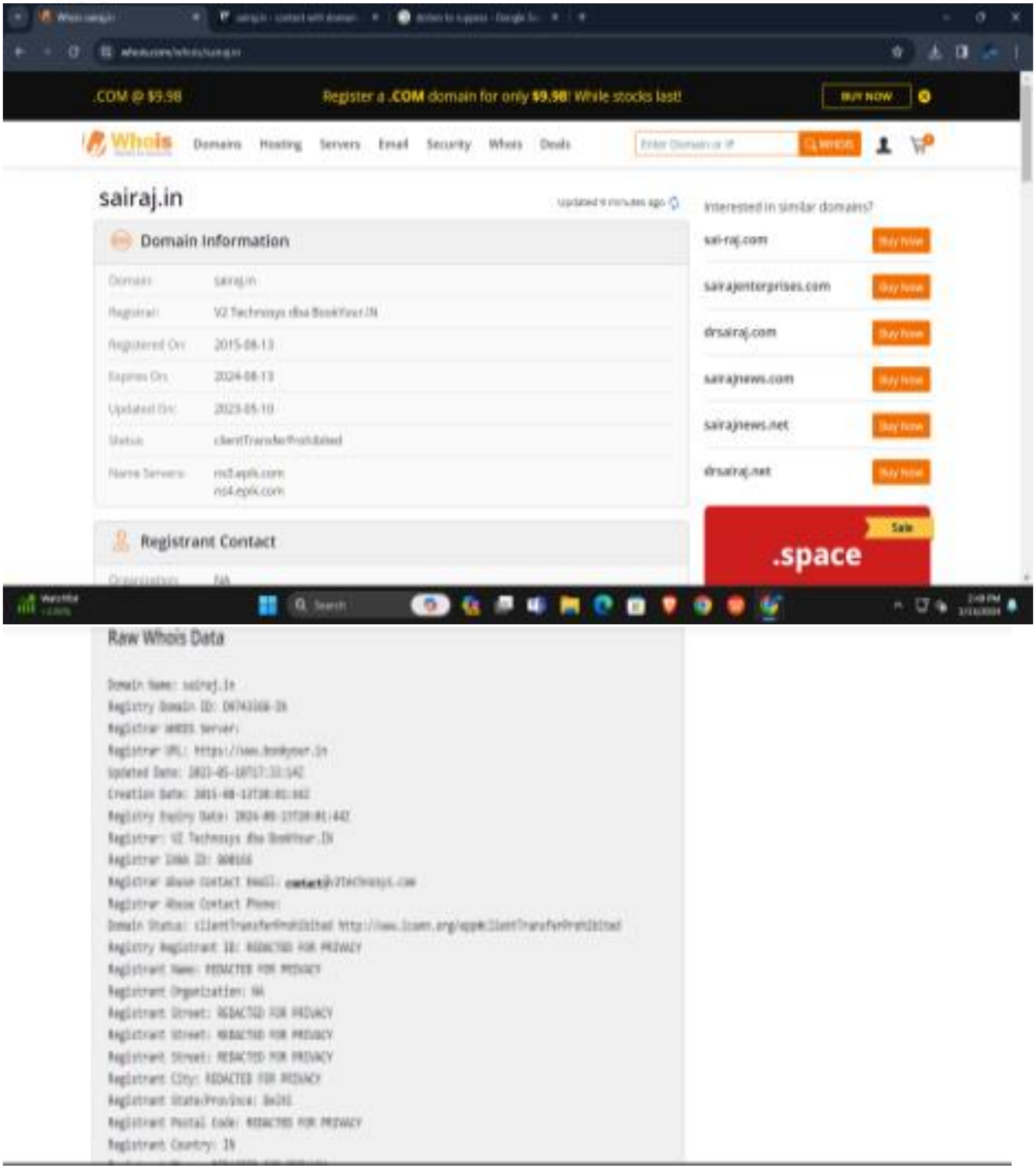
Aim:- Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.

Theory:-

WHOIS:

A Whois domain lookup allows you to trace the ownership and tenure of a domain name. Similar to how all houses are registered with a governing authority, all domain name registries maintain a record of information about every domain name purchased through them, along with who owns it, and the date till which it has been purchased.





sairaj.in

Updated 9 minutes ago

Domain Information

Domain:	sairaj.in
Registrar:	V2 Technosys dba BookYour.IN
Registered On:	2015-08-13
Expires On:	2024-08-13
Updated On:	2023-05-10
Status:	clientTransferProhibited
Name Servers:	ns3.epik.com ns4.epik.com

Registrant Contact

Organization:	NA

Interested in similar domains?

sai-raj.com	Buy Now
sairajenterprises.com	Buy Now
drsairaj.com	Buy Now
sairajnews.com	Buy Now
sairajnews.net	Buy Now
drsairaj.net	Buy Now

Raw Whois Data

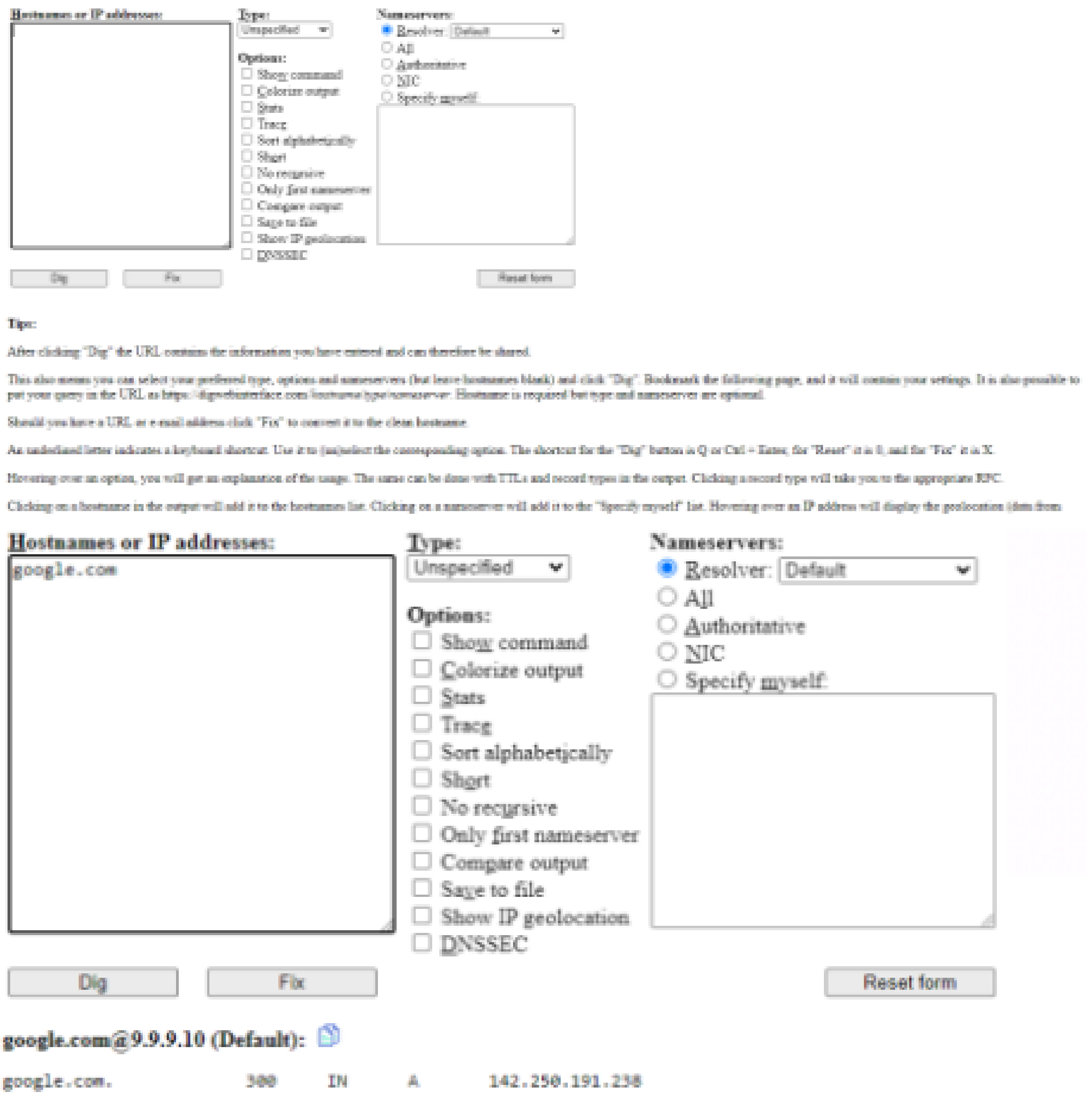
```
Domain Name: sairaj.in
Registry Domain ID: D9743168-IN
Registrar WHOIS Server:
Registrar URL: https://www.bookyour.in
Updated Date: 2023-05-10T17:33:14Z
Creation Date: 2015-08-13T08:01:44Z
Registry Expiry Date: 2024-08-13T08:01:44Z
Registrar: V2 Technosys dba BookYour.IN
Registrar IANA ID: 800166
Registrar Abuse Contact Email: contact@v2technosys.com
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: NA
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Delhi
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
```

Dig:

The dig (domain information groper) command is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the queried name server(s). Most DNS administrators use the dig command to troubleshoot DNS problems because of its flexibility, ease of use, and clarity of output.

Although dig is normally used with command-line arguments, it also has a batch mode for reading lookup requests from a file.

The dig command provides a number of query options that affect the way in which lookups are made and the results displayed.



Tips:

After clicking "Dig" the URL contains the information you have entered and can therefore be shared.

This also means you can select your preferred type, options and nameservers (but leave hostnames blank) and click "Dig". Bookmark the following page, and it will contain your settings. It is also possible to put your query in the URL as https://digwebinterface.com/hostname/type/nameserver. Hostname is required but type and nameserver are optional.

Should you have a URL or e-mail address click "Fix" to convert it to the clean hostname.

An underlined letter indicates a keyboard shortcut. Use it to (un)select the corresponding option. The shortcut for the "Dig" button is Q or Ctrl + Enter, for "Reset" it is R, and the "Fix" it is X.

Hovering over an option, you will get an explanation of the usage. The same can be done with TTLs and record types in the output. Clicking a record type will take you to the appropriate RFC.

Clicking on a hostname in the output will add it to the hostnames list. Clicking on a nameserver will add it to the "Specify myself" list. Hovering over an IP address will display the geolocation (data from

Hostnames or IP addresses: google.com

Type: Unspecified

Options:

- □ Show command
- □ Colorize output
- □ Stats
- □ Trace
- □ Sort alphabetically
- □ Short
- □ No recursive
- □ Only first nameserver
- □ Compare output
- □ Save to file
- □ Show IP geolocation
- □ DNSSEC

Nameservers:

- ● Resolver: Default
- ○ All
- ○ Authoritative
- ○ NIC
- ○ Specify myself

google.com@9.9.9.10 (Default):

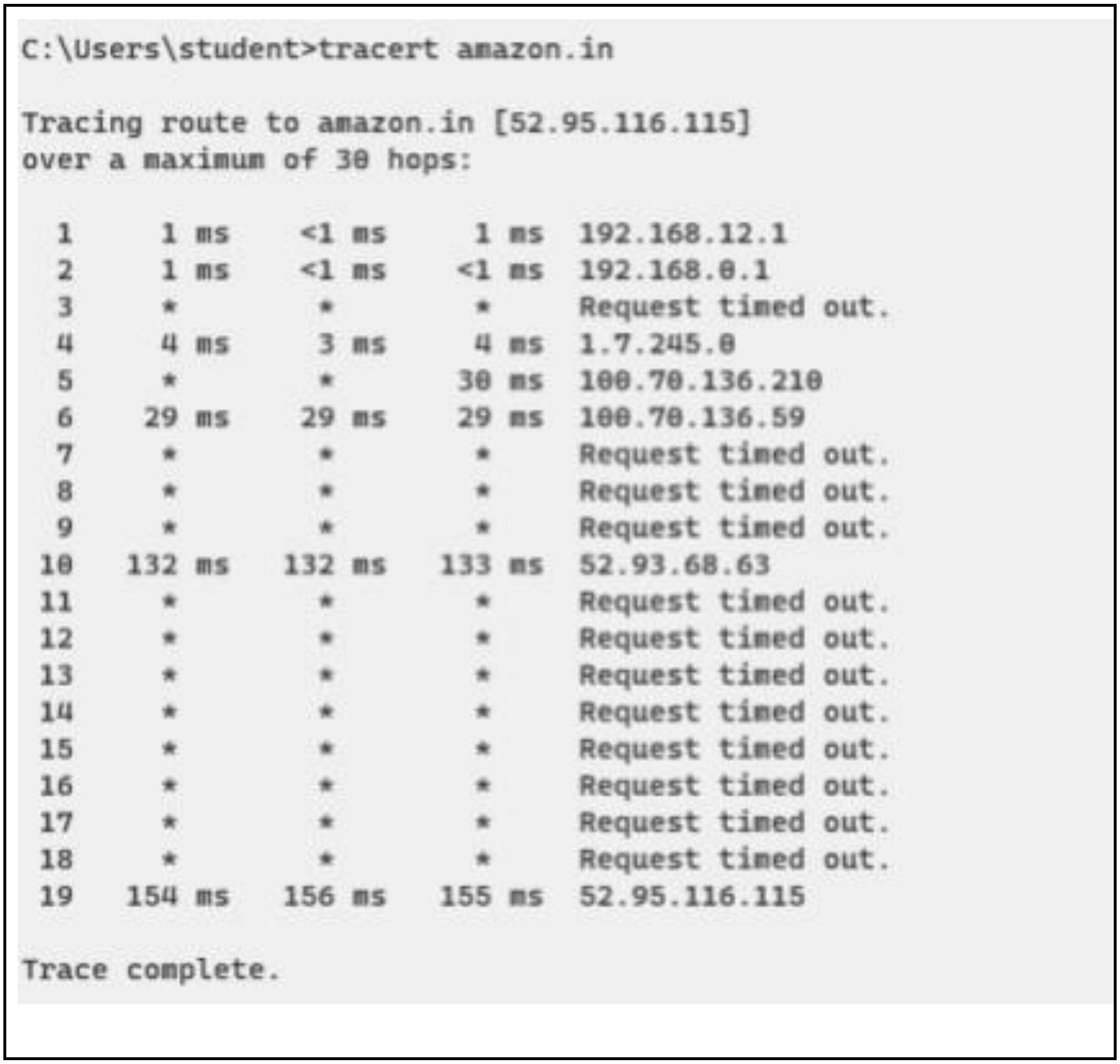
```
google.com.            300     IN      A       142.250.191.238
```

Traceroute:

A traceroute provides a map of how data on the internet travels from its source to its destination. When you connect with a website, the data you get must travel across multiple devices and networks along the way, particularly routers.

Using command prompt:

Type 'tracert' followed by a space and the domain name or IP address (for example: tracert example.com)

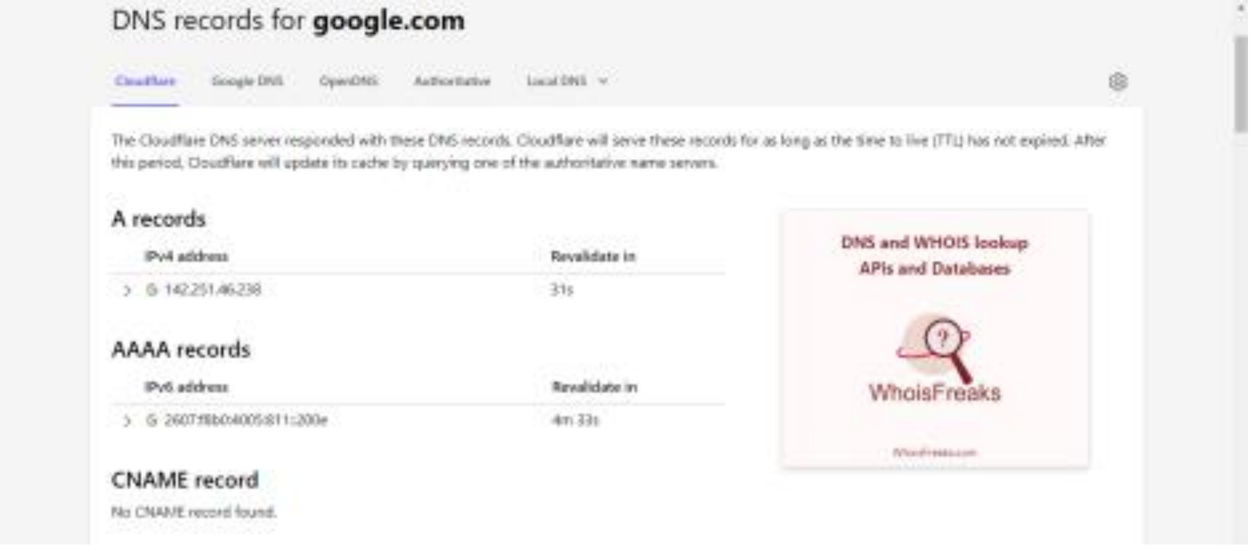


```
C:\Users\student>tracert amazon.in

Tracing route to amazon.in [52.95.116.115]
over a maximum of 30 hops:

  1     1 ms    <1 ms     1 ms  192.168.12.1
  2     1 ms    <1 ms    <1 ms  192.168.0.1
  3     *        *        *     Request timed out.
  4     4 ms     3 ms     4 ms  1.7.245.0
  5     *        *       30 ms  100.70.136.210
  6    29 ms    29 ms    29 ms  100.70.136.59
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10   132 ms   132 ms   133 ms  52.93.68.63
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19   154 ms   156 ms   155 ms  52.95.116.115

Trace complete.
```

Nslookup:

Nslookup is the name of a program that lets users enter a host name and find out the corresponding IP address or domain name system (DNS) record. Users can also enter a command in nslookup to do a reverse DNS lookup and find the host name for a specified IP address.

Network administrators use nslookup to troubleshoot server connections or for security reasons.



DNS records for **google.com**

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
142.251.46.238	31s

AAAA records

IPv6 address	Revalidate in
2607:f8b0:4005:811::200e	4m 33s

CNAME record

No CNAME record found.