Ishita Hardasmalani

C14-2103058

EXPERIMENT NO . 7

Aim: Study the use of network reconnaissance tools and apply the following :
WHOIS , dig , traceroute , nslookup

Theory:

Reconnaissance tools are essential components in the toolbox of security professionals and ethical hackers. They are used in the initial phase of a security assessment or penetration testing, known as reconnaissance or information gathering. This phase aims to collect as much information as possible about the target system, network, or organization. Reconnaissance can be passive, where the attacker gathers information without directly interacting with the target, or active, where the attacker engages with the target system to gather insights. Tools like Nmap, WHOIS, Shodan, and Maltego allow professionals to uncover open ports, services running on a system, domain name details, and network infrastructure information. By understanding the target's landscape, security professionals can identify potential vulnerabilities and plan their penetration testing strategies effectively, while attackers could use this information to exploit weaknesses.

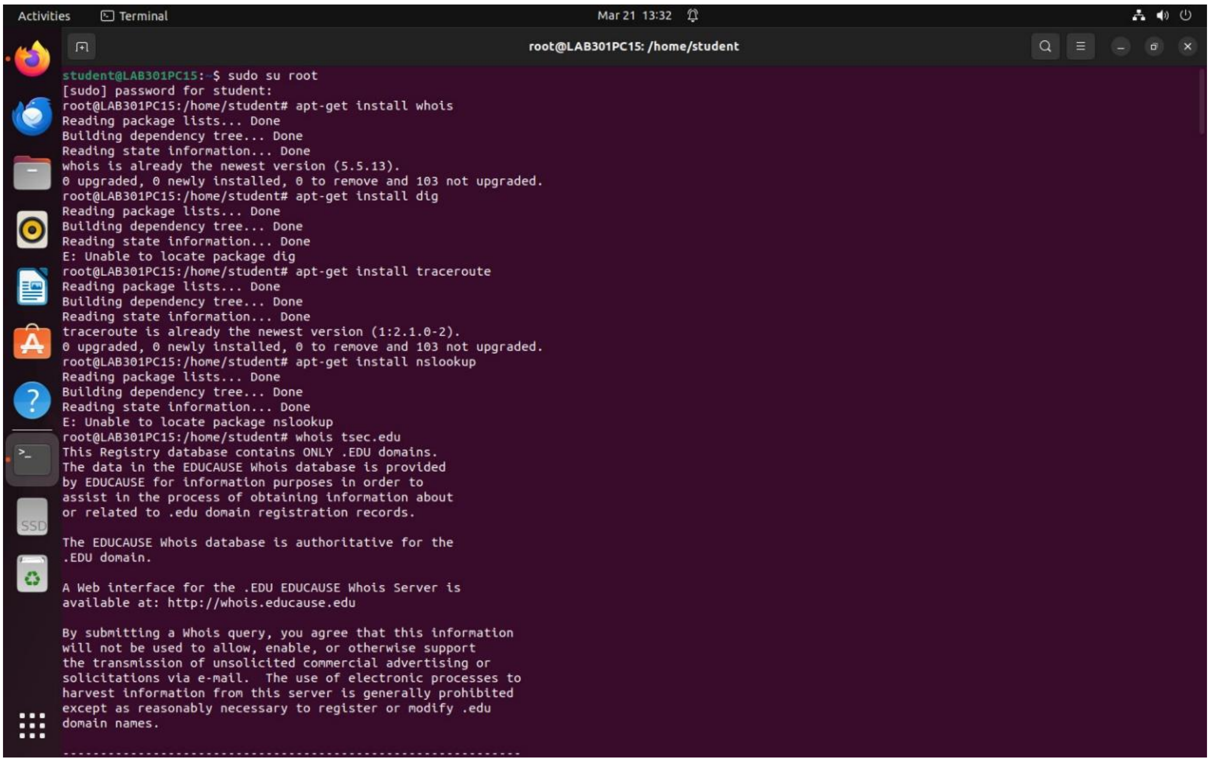
Steps:

1.Open Ubuntu terminal.

2. Get root access , by typing “sudo su root”.

3. Install the tools using the commands:

```
#apt-get install whois

#apt-get install dig

#apt-get install traceroute

#apt-get install nslookup
```



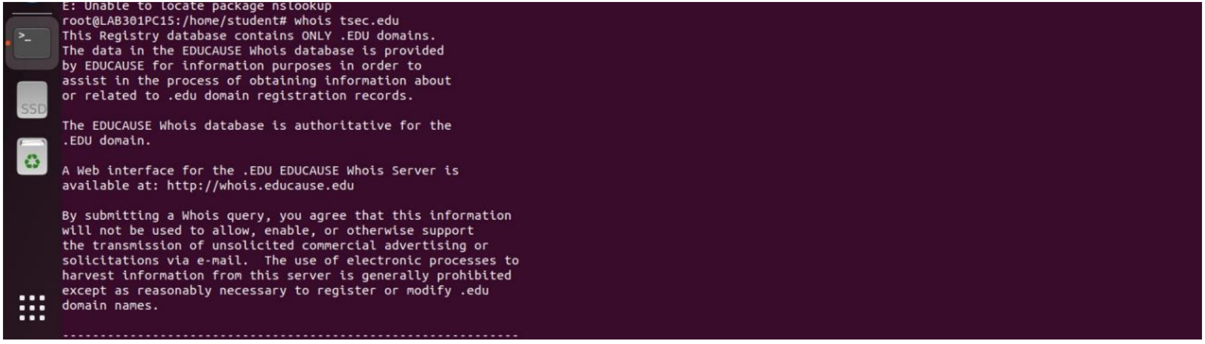
```
student@LAB301PC15:~$ sudo su root
[sudo] password for student:
root@LAB301PC15:/home/student# apt-get install whois
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
whois is already the newest version (5.5.13).
0 upgraded, 0 newly installed, 0 to remove and 103 not upgraded.
root@LAB301PC15:/home/student# apt-get install dig
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package dig
root@LAB301PC15:/home/student# apt-get install traceroute
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
traceroute is already the newest version (1:2.1.0-2).
0 upgraded, 0 newly installed, 0 to remove and 103 not upgraded.
root@LAB301PC15:/home/student# apt-get install nslookup
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package nslookup
root@LAB301PC15:/home/student# whois tsec.edu
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

-------------------------------------------------------------
```

WHOIS : WHOIS is the Linux utility for searching an object in a WHOIS database. The WHOIS database of a domain is the publicly displayed information about a domains ownership, billing, technical, administrative, and nameserver information. Running a WHOIS on your domain will look the domain up at the registrar for the domain information. All domains have WHOIS information. WHOIS database can be queried to obtain the following information via WHOIS:

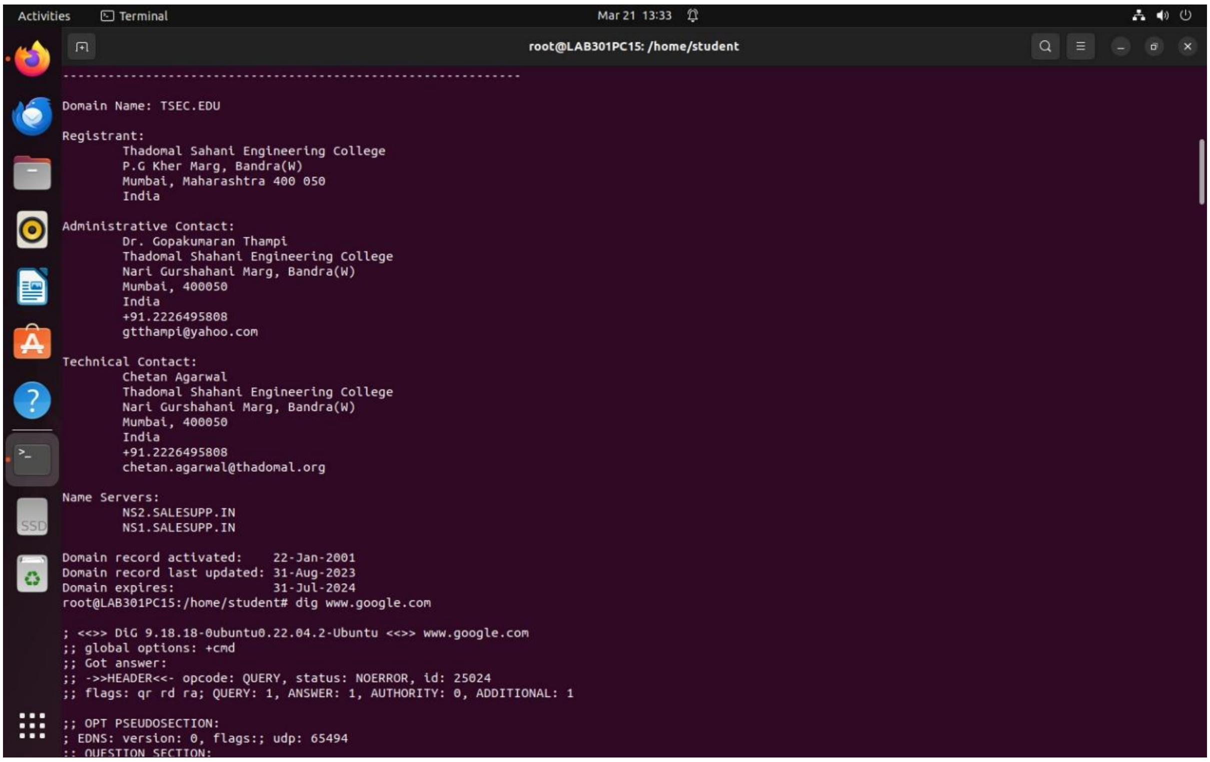
Administrative contact details, including names, email addresses, and telephone numbers
Mailing addresses for office locations relating to the target organization

Details of authoritative name servers for each given domain

Example: Querying tsec.edu



```
E: Unable to locate package nslookup
root@LAB301PC15:/home/student# whois tsec.edu
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

-------------------------------------------------------------
```



```
------------------------------------------------------------

Domain Name: TSEC.EDU

Registrant:
        Thadomal Sahani Engineering College
        P.G Kher Marg, Bandra(W)
        Mumbai, Maharashtra 400 050
        India

Administrative Contact:
        Dr. Gopakumaran Thampi
        Thadomal Shahani Engineering College
        Nari Gurshahani Marg, Bandra(W)
        Mumbai, 400050
        India
        +91.2226495808
        gtthampi@yahoo.com

Technical Contact:
        Chetan Agarwal
        Thadomal Shahani Engineering College
        Nari Gurshahani Marg, Bandra(W)
        Mumbai, 400050
        India
        +91.2226495808
        chetan.agarwal@thadomal.org

Name Servers:
        NS2.SALESUPP.IN
        NS1.SALESUPP.IN

Domain record activated:    22-Jan-2001
Domain record last updated: 31-Aug-2023
Domain expires:             31-Jul-2024
root@LAB301PC15:/home/student# dig www.google.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25024
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
```

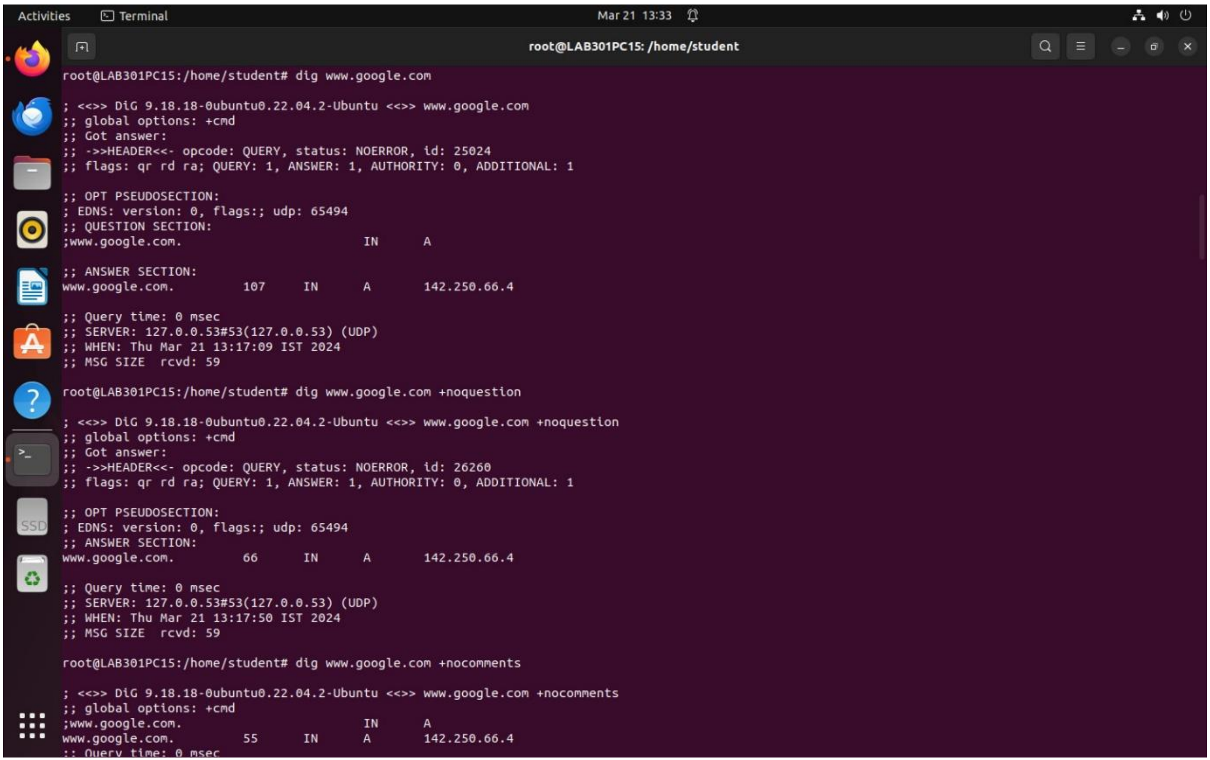
DIG: Dig (domain information groper) is a network administration commandline tool for querying Domain Name System (DNS) name servers. Dig is useful for network troubleshooting and for educational purposes. When you pass a domain name to the dig c ommand, by default it displays the A record(the ipaddress of the site that is queried) as s shown below.

1. Simple dig Command Usage student@lab:~# dig www.google.com
The dig command output has the following sections:
Header: This displays the dig command version number, the global options used by the dig command, and few additional header information. QUESTION SECTION: This displays the question it asked the DNS. i.e. input. Since we said 'dig google.com', it indicates in this section that we asked for the record of the google.com website.

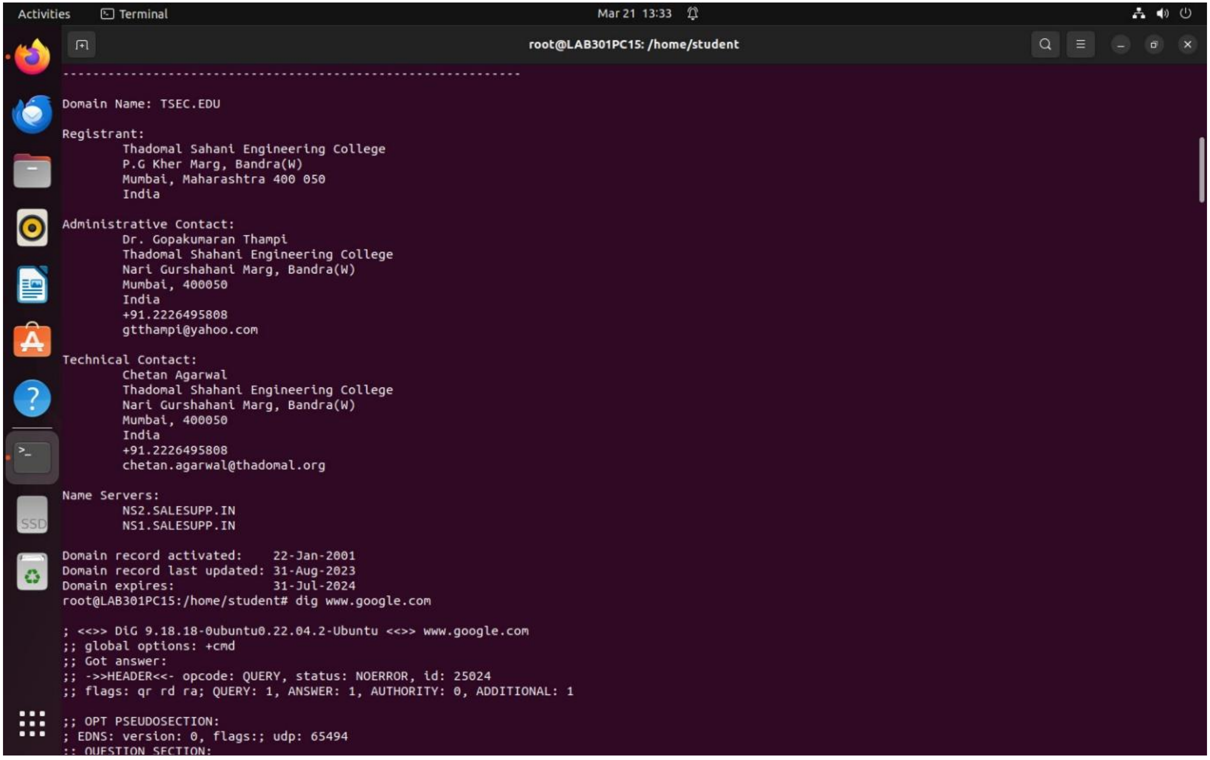
ANSWER SECTION: This displays the answer it receives from the DNS. i.e This is your output. This displays the record of google.com.

AUTHORITY SECTION: This displays the DNS name server that has the authority to re spond to this query. Basically this displays available name servers of google.com.

ADDITIONAL SECTION: This displays the ip address of the name servers listed in the AUTHORITY SECTION. Stats section at the bottom displays few dig command statistics inc luding how much time it took to execute this query

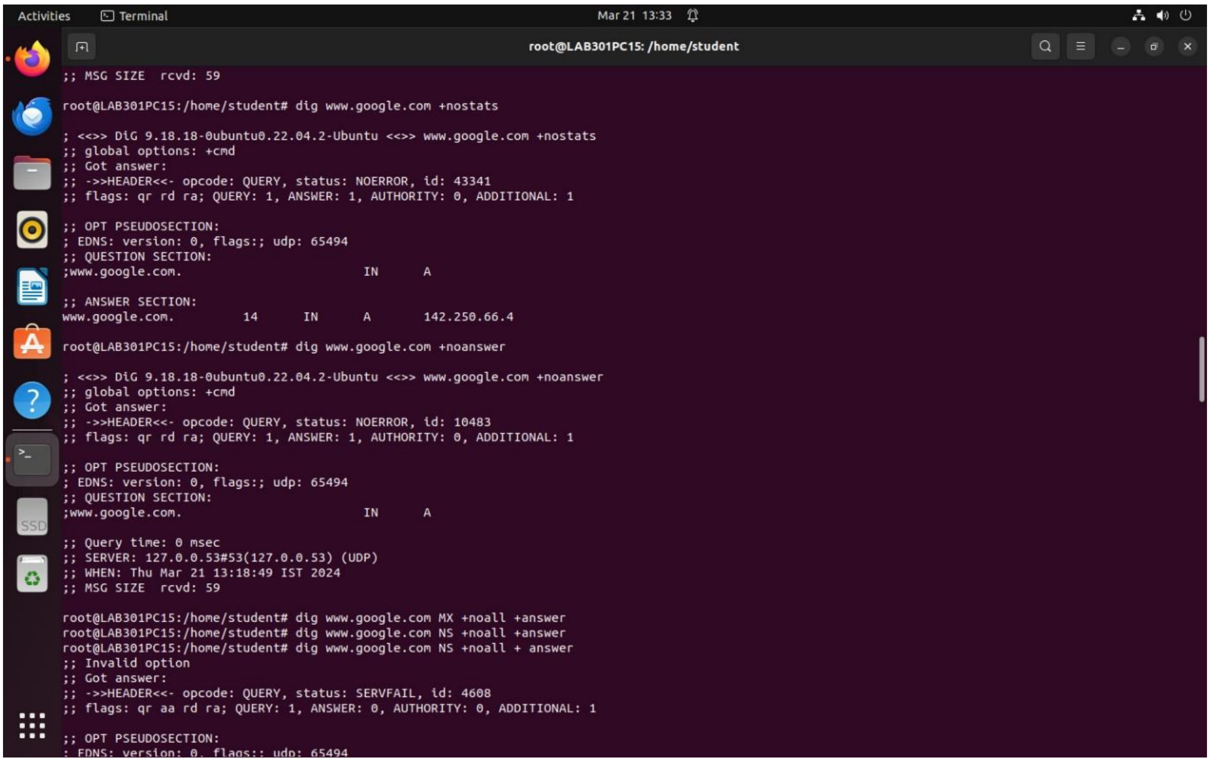


```
root@LAB301PC15:/home/student# dig www.google.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25024
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.         107     IN      A       142.250.66.4

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 21 13:17:09 IST 2024
;; MSG SIZE  rcvd: 59

root@LAB301PC15:/home/student# dig www.google.com +noquestion

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> www.google.com +noquestion
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26260
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; ANSWER SECTION:
www.google.com.         66      IN      A       142.250.66.4

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 21 13:17:50 IST 2024
;; MSG SIZE  rcvd: 59

root@LAB301PC15:/home/student# dig www.google.com +nocomments

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> www.google.com +nocomments
;; global options: +cmd
;www.google.com.                IN      A
www.google.com.         55      IN      A       142.250.66.4
;; Query time: 0 msec
```

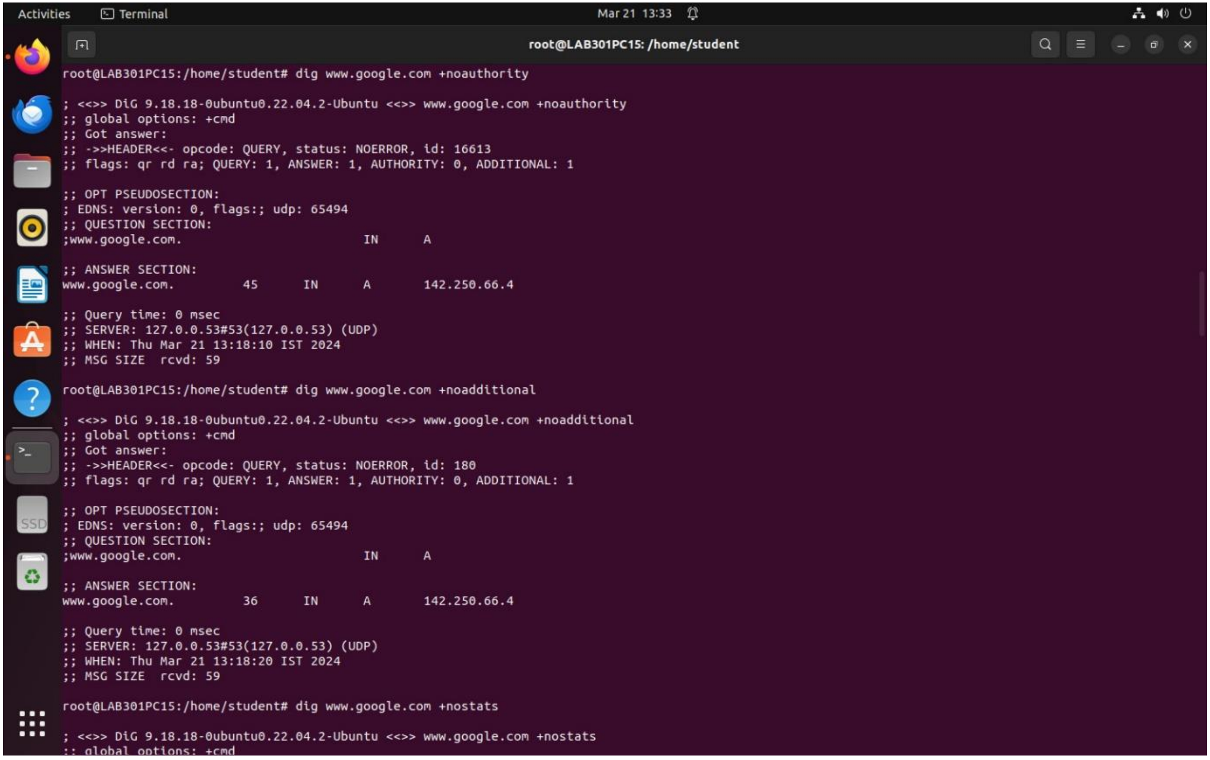


```
-------------------------------------------------------------

Domain Name: TSEC.EDU

Registrant:
        Thadomal Sahani Engineering College
        P.G Kher Marg, Bandra(W)
        Mumbai, Maharashtra 400 050
        India

Administrative Contact:
        Dr. Gopakumaran Thampi
        Thadomal Shahani Engineering College
        Nari Gurshahani Marg, Bandra(W)
        Mumbai, 400050
        India
        +91.2226495808
        gtthampi@yahoo.com

Technical Contact:
        Chetan Agarwal
        Thadomal Shahani Engineering College
        Nari Gurshahani Marg, Bandra(W)
        Mumbai, 400050
        India
        +91.2226495808
        chetan.agarwal@thadomal.org

Name Servers:
        NS2.SALESUPP.IN
        NS1.SALESUPP.IN

Domain record activated:    22-Jan-2001
Domain record last updated: 31-Aug-2023
Domain expires:             31-Jul-2024
root@LAB301PC15:/home/student# dig www.google.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25024
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
```

2. Display Only the ANSWER SECTION of the Dig command Output
All you need to look at is the "ANSWER SECTION" of the dig command. So, we can turn off all other sections as shown below. i) student@lab:~ #dig google.com +noquestion ii) student@lab:~ #dig google.com +nocomments – Turn off the comment lines iii) student@lab:~ # dig google.com +noauthority – Turn off the authority section iv) student@lab:~ #dig google.com +noadditional – Turn off the additional section v) student@lab:~ #dig google.com +nostats – Turn off the stats section vi) student@lab:~ #dig google.com +noanswer – Turn off the answer section



```
;; MSG SIZE  rcvd: 59

root@LAB301PC15:/home/student# dig www.google.com +nostats

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> www.google.com +nostats
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43341
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.         14      IN      A       142.250.66.4

root@LAB301PC15:/home/student# dig www.google.com +noanswer

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> www.google.com +noanswer
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10483
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                IN      A

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 21 13:18:49 IST 2024
;; MSG SIZE  rcvd: 59

root@LAB301PC15:/home/student# dig www.google.com MX +noall +answer
root@LAB301PC15:/home/student# dig www.google.com NS +noall +answer
root@LAB301PC15:/home/student# dig www.google.com NS +noall + answer
;; Invalid option
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 4608
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
```

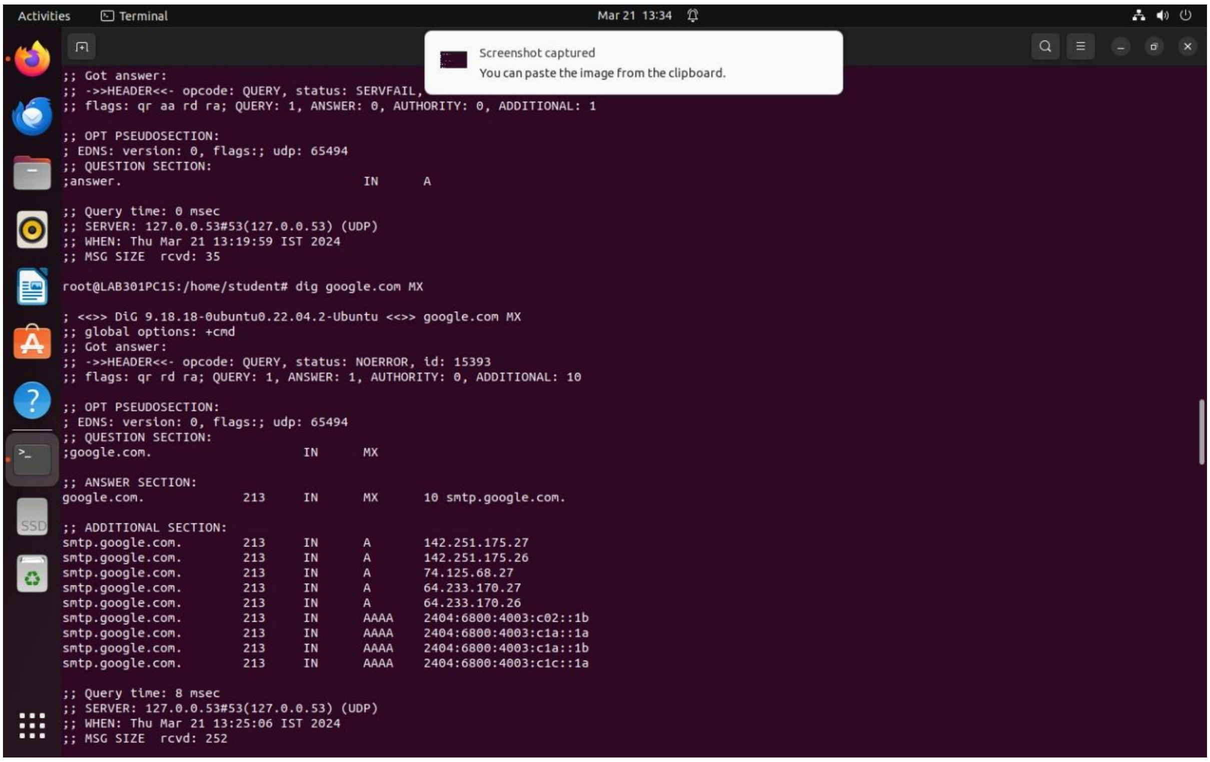


```
root@LAB301PC15:/home/student# dig www.google.com +noauthority

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> www.google.com +noauthority
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16613
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.         45      IN      A       142.250.66.4

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 21 13:18:10 IST 2024
;; MSG SIZE  rcvd: 59

root@LAB301PC15:/home/student# dig www.google.com +noadditional

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> www.google.com +noadditional
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 180
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.         36      IN      A       142.250.66.4

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 21 13:18:20 IST 2024
;; MSG SIZE  rcvd: 59

root@LAB301PC15:/home/student# dig www.google.com +nostats

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> www.google.com +nostats
;; global options: +cmd
```

3. Query MX Records Using dig MX

To query MX records, pass MX as an argument to the dig command as shown below.

student@lab:~ #dig google.com MX +noall +answer

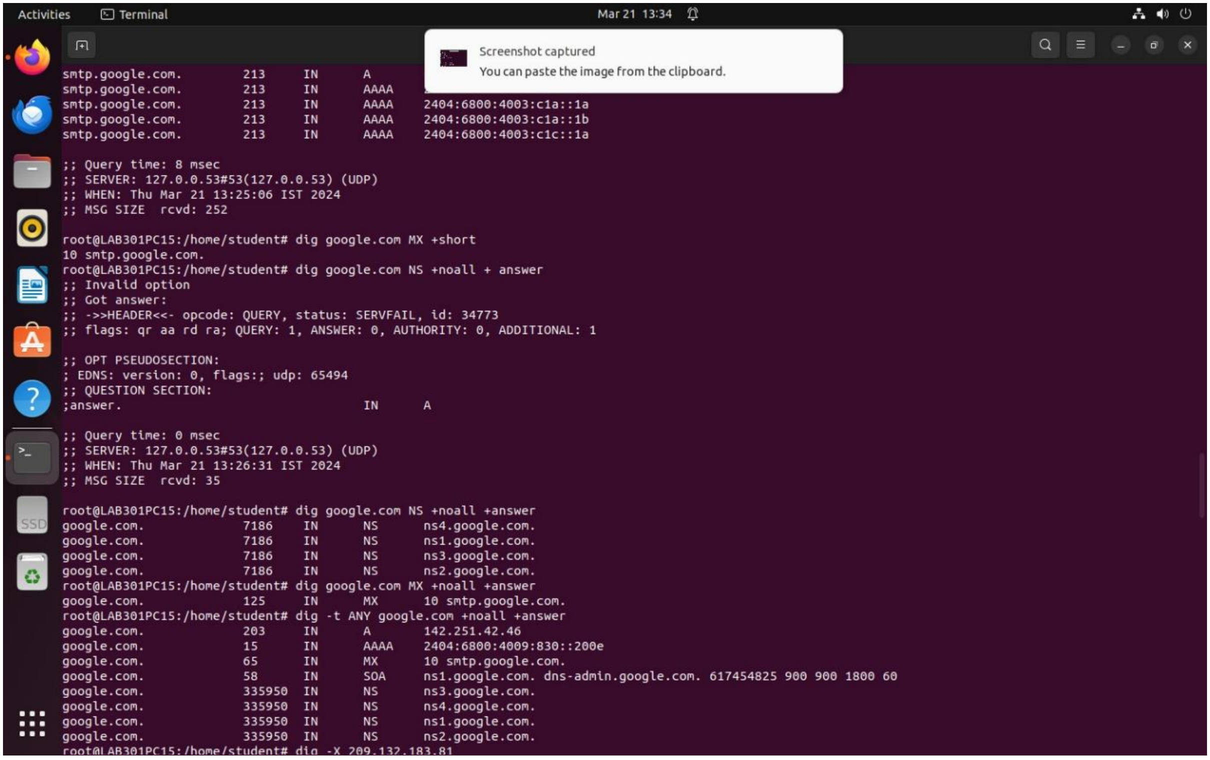


Screenshot captured
You can paste the image from the clipboard.

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL,
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;answer.                                IN      A

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 21 13:19:59 IST 2024
;; MSG SIZE  rcvd: 35

root@LAB301PC15:/home/student# dig google.com MX

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> google.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15393
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             213     IN      MX      10 smtp.google.com.

;; ADDITIONAL SECTION:
smtp.google.com.        213     IN      A       142.251.175.27
smtp.google.com.        213     IN      A       142.251.175.26
smtp.google.com.        213     IN      A       74.125.68.27
smtp.google.com.        213     IN      A       64.233.170.27
smtp.google.com.        213     IN      A       64.233.170.26
smtp.google.com.        213     IN      AAAA    2404:6800:4003:c02::1b
smtp.google.com.        213     IN      AAAA    2404:6800:4003:c1a::1a
smtp.google.com.        213     IN      AAAA    2404:6800:4003:c1a::1b
smtp.google.com.        213     IN      AAAA    2404:6800:4003:c1c::1a

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 21 13:25:06 IST 2024
;; MSG SIZE  rcvd: 252
```

4. Query NS Records Using dig NS

To query the NS record use the type NS as shown below. student@lab:~ #dig google.com NS +noall +answer



Screenshot captured
You can paste the image from the clipboard.

```
smtp.google.com.        213     IN      A
smtp.google.com.        213     IN      AAAA
smtp.google.com.        213     IN      AAAA    2404:6800:4003:c1a::1a
smtp.google.com.        213     IN      AAAA    2404:6800:4003:c1a::1b
smtp.google.com.        213     IN      AAAA    2404:6800:4003:c1c::1a

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 21 13:25:06 IST 2024
;; MSG SIZE  rcvd: 252

root@LAB301PC15:/home/student# dig google.com MX +short
10 smtp.google.com.
root@LAB301PC15:/home/student# dig google.com NS +noall + answer
;; Invalid option
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 34773
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;answer.                                IN      A

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 21 13:26:31 IST 2024
;; MSG SIZE  rcvd: 35

root@LAB301PC15:/home/student# dig google.com NS +noall +answer
google.com.             7186    IN      NS      ns4.google.com.
google.com.             7186    IN      NS      ns1.google.com.
google.com.             7186    IN      NS      ns3.google.com.
google.com.             7186    IN      NS      ns2.google.com.
root@LAB301PC15:/home/student# dig google.com MX +noall +answer
google.com.             125     IN      MX      10 smtp.google.com.
root@LAB301PC15:/home/student# dig -t ANY google.com +noall +answer
google.com.             203     IN      A       142.251.42.46
google.com.             15      IN      AAAA    2404:6800:4009:830::200e
google.com.             65      IN      MX      10 smtp.google.com.
google.com.             58      IN      SOA     ns1.google.com. dns-admin.google.com. 617454825 900 900 1800 60
google.com.             335950  IN      NS      ns3.google.com.
google.com.             335950  IN      NS      ns4.google.com.
google.com.             335950  IN      NS      ns1.google.com.
google.com.             335950  IN      NS      ns2.google.com.
root@LAB301PC15:/home/student# dig -X 209.132.183.81
```

5. View ALL DNS Records Types Using dig t ANY

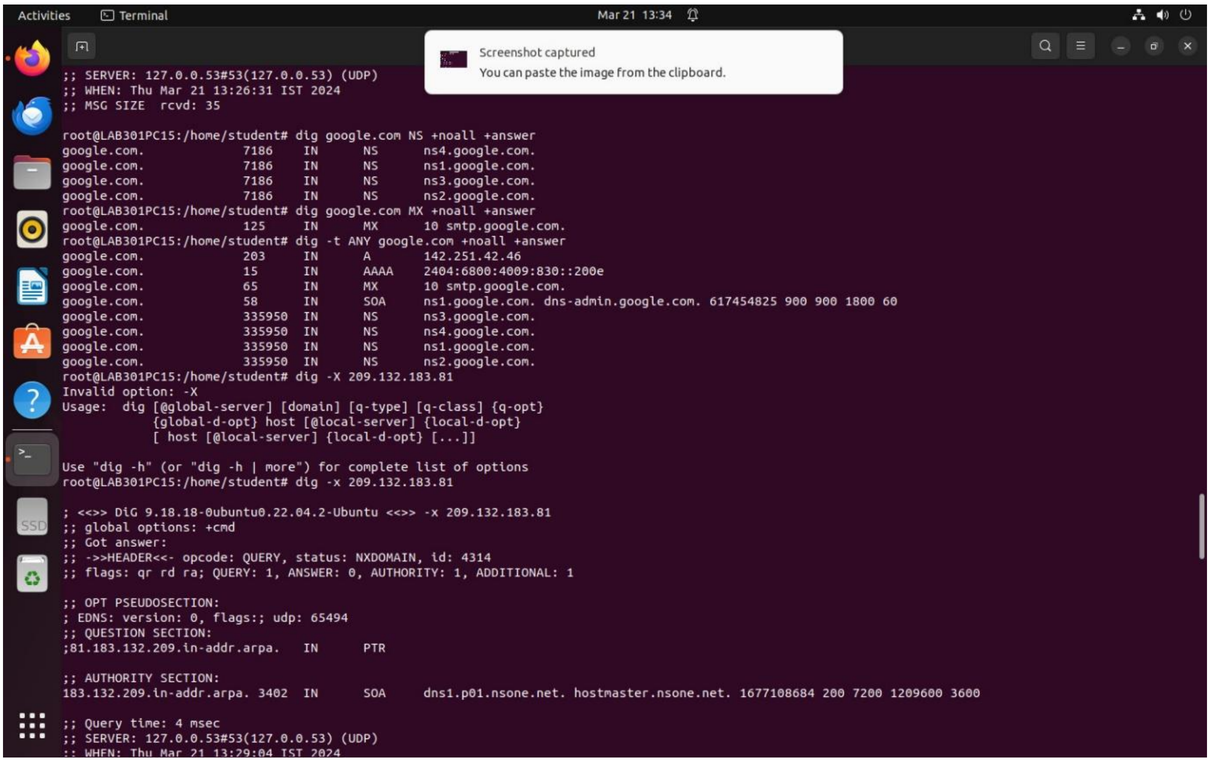
To view all the record types (A, MX, NS, etc.), use ANY as the record type as shown be low. student@lab:~ #dig t ANY google.com +noall +answer

6. View Short Output Using dig +short

To view just the ipaddress of a web site (i.e the A record), use the short form option as shown below. student@lab:~ #dig google.com +short

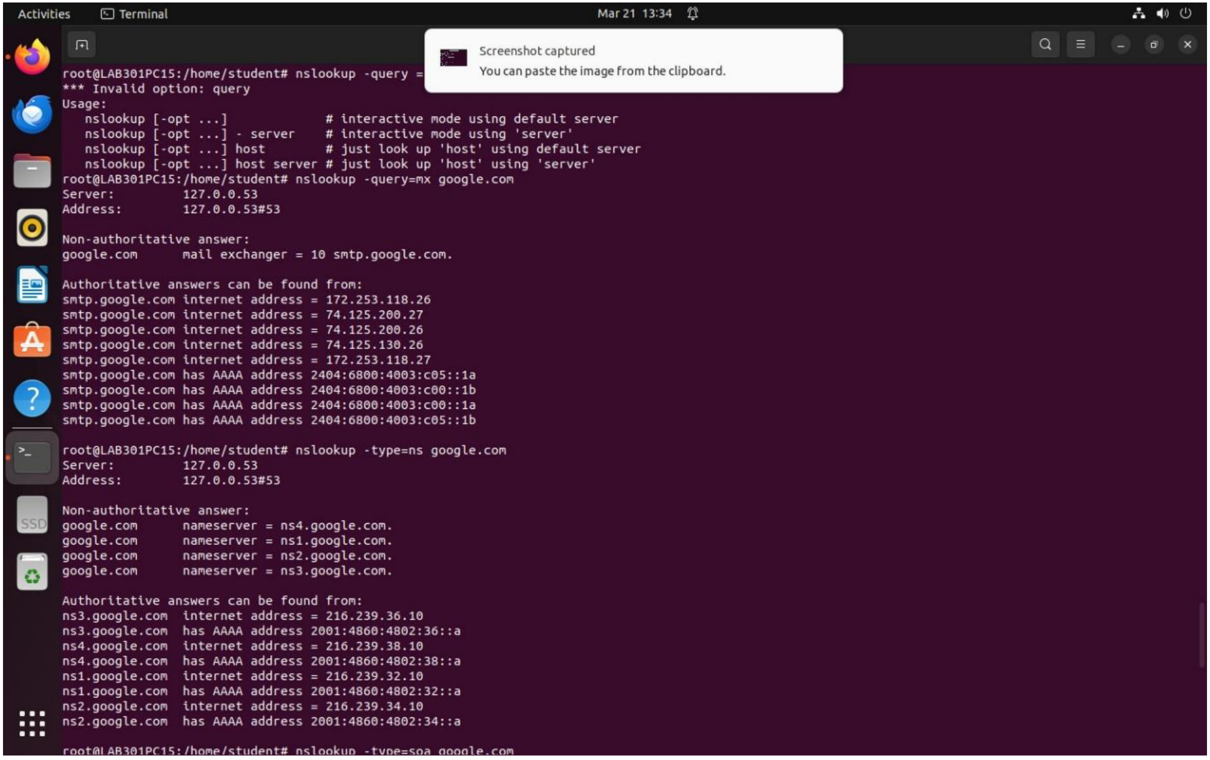
7. DNS Reverse Lookup Using dig –x

To perform a DNS reverse look up using the ip address using dig x as shown below student@lab:~ #dig x 209.132.183.81



Screenshot captured
You can paste the image from the clipboard.

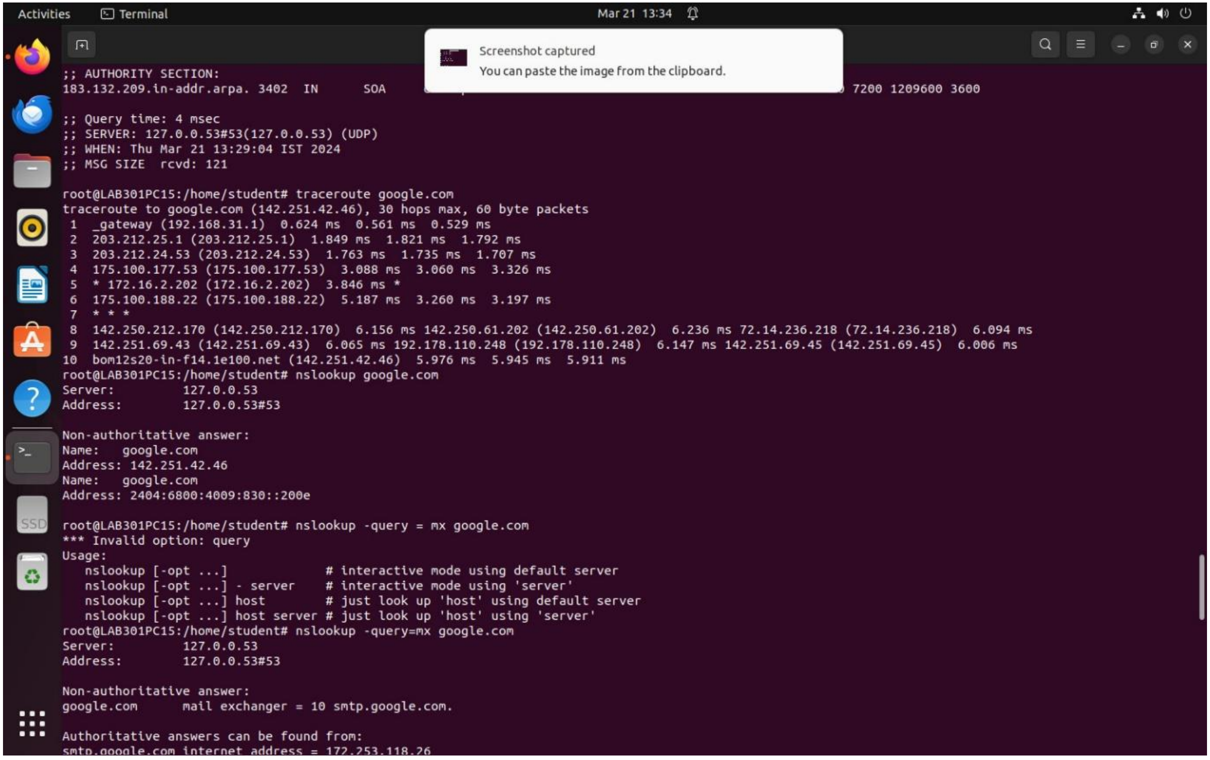
```
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 21 13:26:31 IST 2024
;; MSG SIZE  rcvd: 35

root@LAB301PC15:/home/student# dig google.com NS +noall +answer
google.com.             7186    IN      NS      ns4.google.com.
google.com.             7186    IN      NS      ns1.google.com.
google.com.             7186    IN      NS      ns3.google.com.
google.com.             7186    IN      NS      ns2.google.com.
root@LAB301PC15:/home/student# dig google.com MX +noall +answer
google.com.             125     IN      MX      10 smtp.google.com.
root@LAB301PC15:/home/student# dig -t ANY google.com +noall +answer
google.com.             203     IN      A       142.251.42.46
google.com.             15      IN      AAAA    2404:6800:4009:830::200e
google.com.             65      IN      MX      10 smtp.google.com.
google.com.             58      IN      SOA     ns1.google.com. dns-admin.google.com. 617454825 900 900 1800 60
google.com.             335950  IN      NS      ns3.google.com.
google.com.             335950  IN      NS      ns4.google.com.
google.com.             335950  IN      NS      ns1.google.com.
google.com.             335950  IN      NS      ns2.google.com.
root@LAB301PC15:/home/student# dig -X 209.132.183.81
Invalid option: -X
Usage:  dig [@global-server] [domain] [q-type] [q-class] {q-opt}
            {global-d-opt} host [@local-server] {local-d-opt}
            [ host [@local-server] {local-d-opt} [...]]

Use "dig -h" (or "dig -h | more") for complete list of options
root@LAB301PC15:/home/student# dig -x 209.132.183.81

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> -x 209.132.183.81
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 4314
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;81.183.132.209.in-addr.arpa.   IN      PTR

;; AUTHORITY SECTION:
183.132.209.in-addr.arpa. 3402  IN      SOA     dns1.p01.nsone.net. hostmaster.nsone.net. 1677108684 200 7200 1209600 3600

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 21 13:29:04 IST 2024
```



Screenshot captured
You can paste the image from the clipboard.

```
root@LAB301PC15:/home/student# nslookup -query =
*** Invalid option: query
Usage:
   nslookup [-opt ...]             # interactive mode using default server
   nslookup [-opt ...] - server    # interactive mode using 'server'
   nslookup [-opt ...] host        # just look up 'host' using default server
   nslookup [-opt ...] host server # just look up 'host' using 'server'
root@LAB301PC15:/home/student# nslookup -query=mx google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:
smtp.google.com internet address = 172.253.118.26
smtp.google.com internet address = 74.125.200.27
smtp.google.com internet address = 74.125.200.26
smtp.google.com internet address = 74.125.130.26
smtp.google.com internet address = 172.253.118.27
smtp.google.com has AAAA address 2404:6800:4003:c05::1a
smtp.google.com has AAAA address 2404:6800:4003:c00::1b
smtp.google.com has AAAA address 2404:6800:4003:c00::1a
smtp.google.com has AAAA address 2404:6800:4003:c05::1b

root@LAB301PC15:/home/student# nslookup -type=ns google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns3.google.com.

Authoritative answers can be found from:
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a

root@LAB301PC15:/home/student# nslookup -type=soa google.com
```

Traceroute - Traceroute prints the route that packets take to a network host. Traceroute utility uses the TTL field in the IP header to achieve its operation. TTL field describes how much hops a particular packet will take while traveling on network. So, this effectively outlines the lifetime of the packet on network. This field is usually set to 32 or 64. Each time the packet is held on an intermediate router, it decreases the TTL value by 1. When a router finds the TTL value of 1 in a received packet then that packet is not forwarded but instead discarded. After discarding the packet, router sends an ICMP error message of ―Time exceeded back to the source from where ‖ packet generated. The ICMP packet that is sent back contains the IP address of the router. So now it can be easily understood that traceroute operates by sending packets with TTL value starting from 1 and then incrementing by one each time. Each time a router receives the packet, it checks the TTL field, if TTL field is 1 then it discards the packet and sends the ICMP error packet containing its IP address and this is what traceroute requires. So traceroute incrementally fetches the IP of all the routers between the source and the destination. Command: student@lab:~ #traceroute google.com



Screenshot captured
You can paste the image from the clipboard.

```
;; AUTHORITY SECTION:
183.132.209.in-addr.arpa. 3402  IN      SOA                                                       7200 1209600 3600

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 21 13:29:04 IST 2024
;; MSG SIZE  rcvd: 121

root@LAB301PC15:/home/student# traceroute google.com
traceroute to google.com (142.251.42.46), 30 hops max, 60 byte packets
 1  _gateway (192.168.31.1)  0.624 ms  0.561 ms  0.529 ms
 2  203.212.25.1 (203.212.25.1)  1.849 ms  1.821 ms  1.792 ms
 3  203.212.24.53 (203.212.24.53)  1.763 ms  1.735 ms  1.707 ms
 4  175.100.177.53 (175.100.177.53)  3.088 ms  3.060 ms  3.326 ms
 5  * 172.16.2.202 (172.16.2.202)  3.846 ms *
 6  175.100.188.22 (175.100.188.22)  5.187 ms  3.260 ms  3.197 ms
 7  * * *
 8  142.250.212.170 (142.250.212.170)  6.156 ms 142.250.61.202 (142.250.61.202)  6.236 ms 72.14.236.218 (72.14.236.218)  6.094 ms
 9  142.251.69.43 (142.251.69.43)  6.065 ms 192.178.110.248 (192.178.110.248)  6.147 ms 142.251.69.45 (142.251.69.45)  6.006 ms
10  bom12s20-in-f14.1e100.net (142.251.42.46)  5.976 ms  5.945 ms  5.911 ms
root@LAB301PC15:/home/student# nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.42.46
Name:   google.com
Address: 2404:6800:4009:830::200e

root@LAB301PC15:/home/student# nslookup -query = mx google.com
*** Invalid option: query
Usage:
   nslookup [-opt ...]             # interactive mode using default server
   nslookup [-opt ...] - server    # interactive mode using 'server'
   nslookup [-opt ...] host        # just look up 'host' using default server
   nslookup [-opt ...] host server # just look up 'host' using 'server'
root@LAB301PC15:/home/student# nslookup -query=mx google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:
smtp.google.com internet address = 172.253.118.26
```

Nslookup - The nslookup command is used to query internet name servers interactively for information. Nslookup, which stands for "name server lookup”. It is a useful tool for finding out information about a named domain. By default, nslookup will translate a domain name to an IP address (or vice versa).

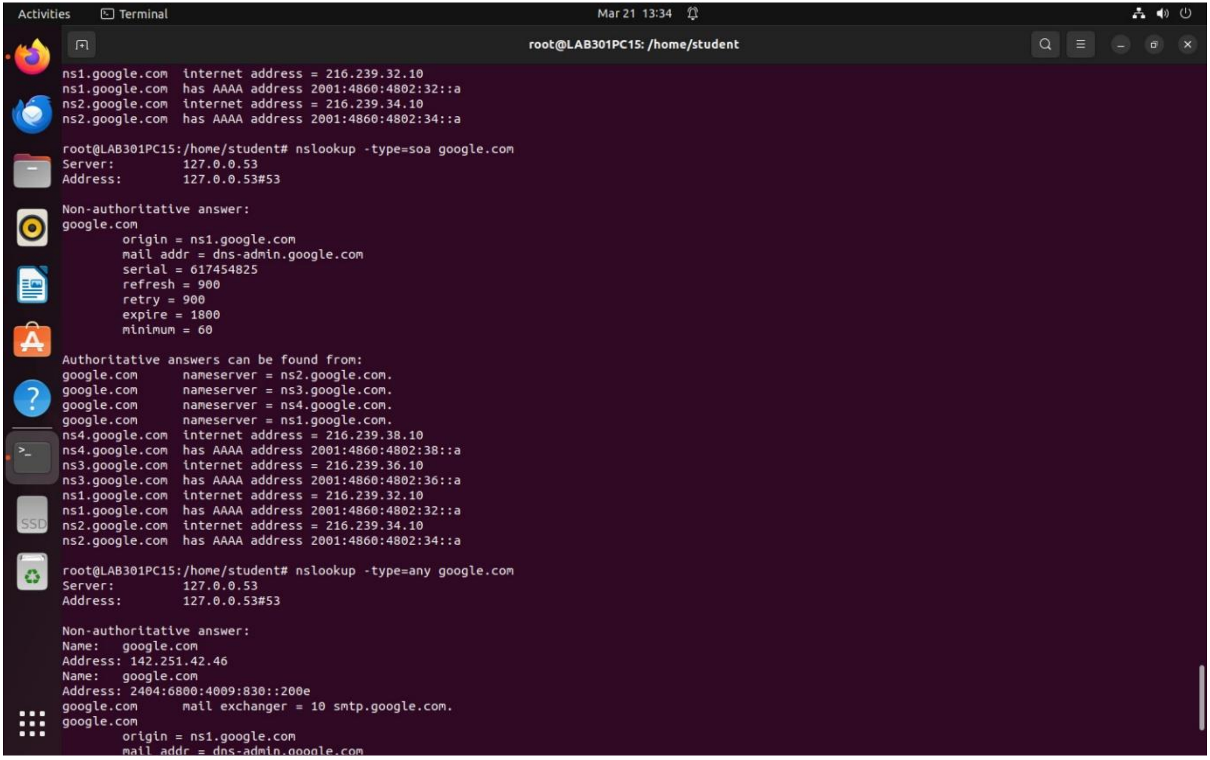
Nslookup has two modes: interactive and noninteractive.

Interactive mode allows the user to query name servers for information about variou shosts and domains or to print a list of hosts in a domain. Noninteractive mode is us ed to print just the name and requested information for a host or domain.

1. Simple nslookup command student@lab:~ #nslookup google.com

2. Query the MX Record using query=mx student@lab:~
#nslookup query = mx google.com
MX (Mail Exchange) record maps a domain name to a list of mail exchange servers for that domain

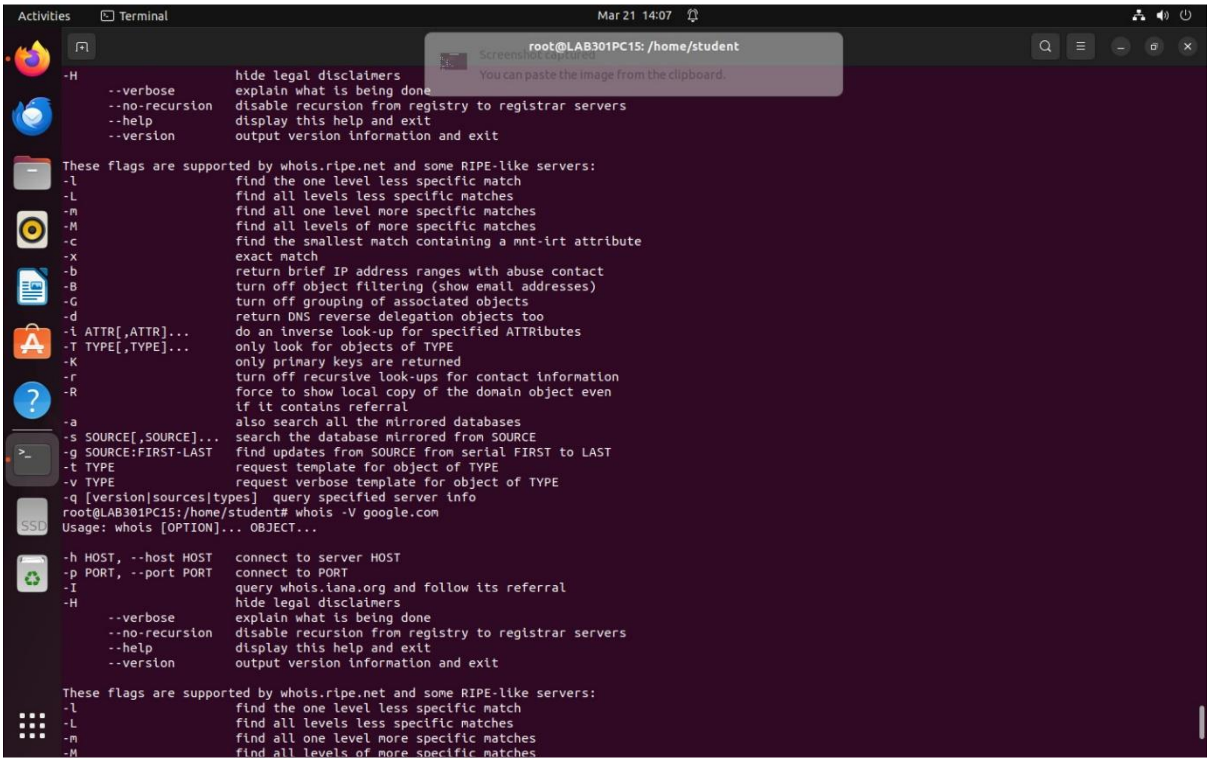
3. Query the NS Record using type=ns
student@lab: ~ #nslookup type = ns google.com
NS (Name Server) record maps a domain name to a list of DNS servers authoritative for that domain. 4. Query the SOA Record using type=soa
student@lab: ~ #nslookup type = soa google.com SOA record (start of authority) provides the authoritative information about the domain,
the email address of the domain admin, the domain serial number, etc
5. View available DNS records using query=any
student@lab: ~ #nslookup type = any google.com



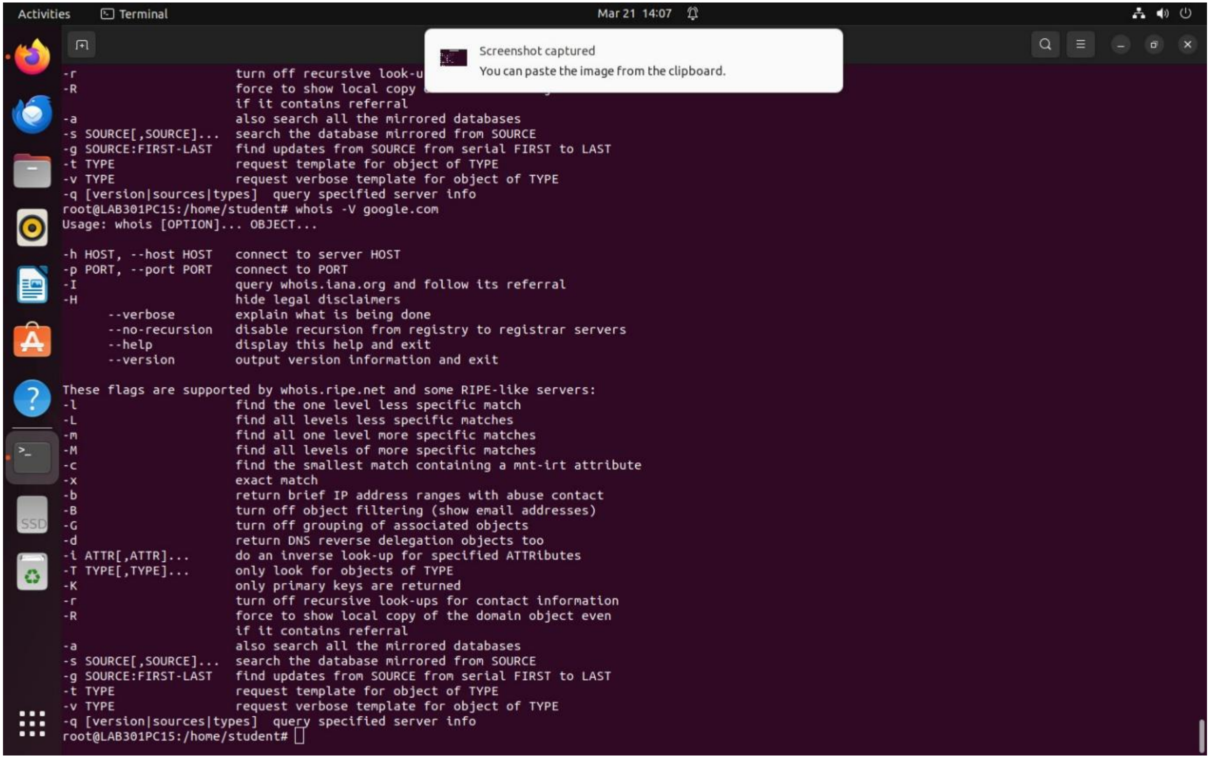
```
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a

root@LAB301PC15:/home/student# nslookup -type=soa google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 617454825
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60

Authoritative answers can be found from:
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns1.google.com.
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a

root@LAB301PC15:/home/student# nslookup -type=any google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.42.46
Name:   google.com
Address: 2404:6800:4009:830::200e
google.com      mail exchanger = 10 smtp.google.com.
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
```

EXTRA:

whois -V google.com: Verbose output

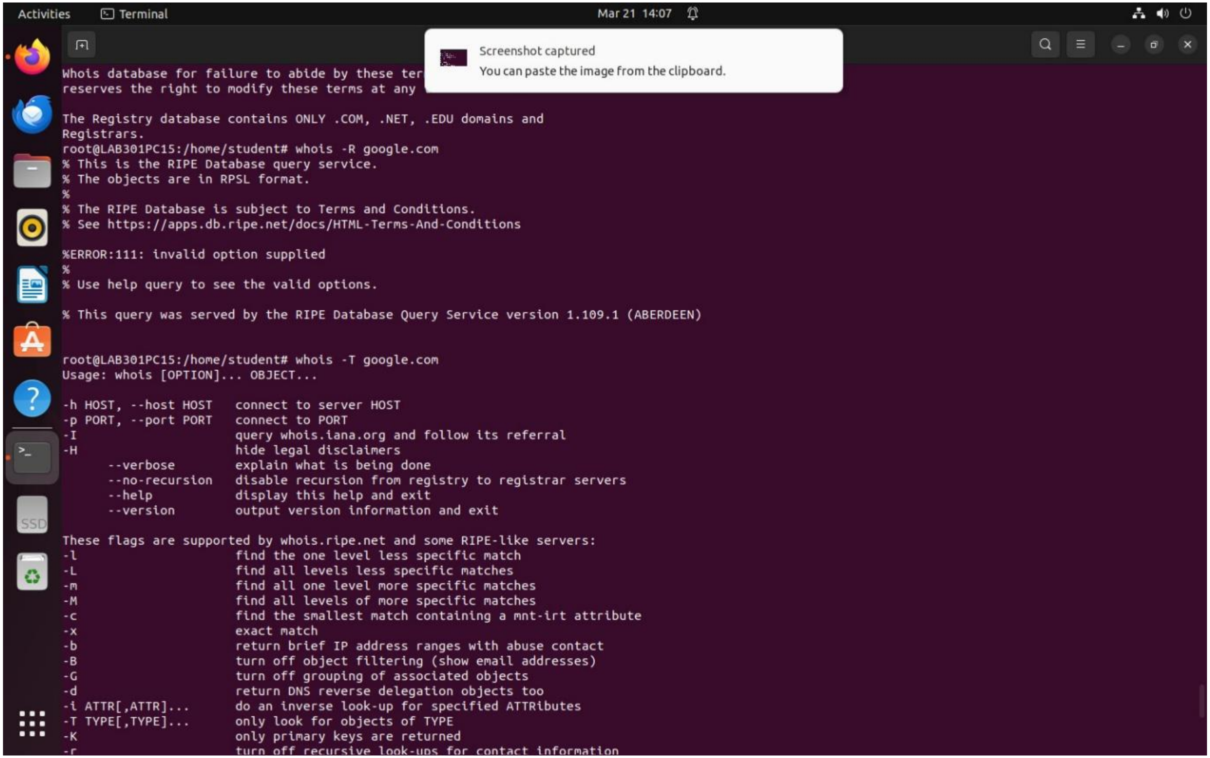

Activities
Terminal
Mar 21 14:07
root@LAB301PC15: /home/student
Screenshot captured
You can paste the image from the clipboard.

```
-H                      hide legal disclaimers
      --verbose         explain what is being done
      --no-recursion    disable recursion from registry to registrar servers
      --help            display this help and exit
      --version         output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                      find the one level less specific match
-L                      find all levels less specific matches
-m                      find all one level more specific matches
-M                      find all levels of more specific matches
-c                      find the smallest match containing a mnt-irt attribute
-x                      exact match
-b                      return brief IP address ranges with abuse contact
-B                      turn off object filtering (show email addresses)
-G                      turn off grouping of associated objects
-d                      return DNS reverse delegation objects too
-i ATTR[,ATTR]...       do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...       only look for objects of TYPE
-K                      only primary keys are returned
-r                      turn off recursive look-ups for contact information
-R                      force to show local copy of the domain object even
                        if it contains referral
-a                      also search all the mirrored databases
-s SOURCE[,SOURCE]...   search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST    find updates from SOURCE from serial FIRST to LAST
-t TYPE                 request template for object of TYPE
-v TYPE                 request verbose template for object of TYPE
-q [version|sources|types]  query specified server info
root@LAB301PC15:/home/student# whois -V google.com
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST    connect to server HOST
-p PORT, --port PORT    connect to PORT
-I                      query whois.iana.org and follow its referral
-H                      hide legal disclaimers
      --verbose         explain what is being done
      --no-recursion    disable recursion from registry to registrar servers
      --help            display this help and exit
      --version         output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                      find the one level less specific match
-L                      find all levels less specific matches
-m                      find all one level more specific matches
-M                      find all levels of more specific matches
```



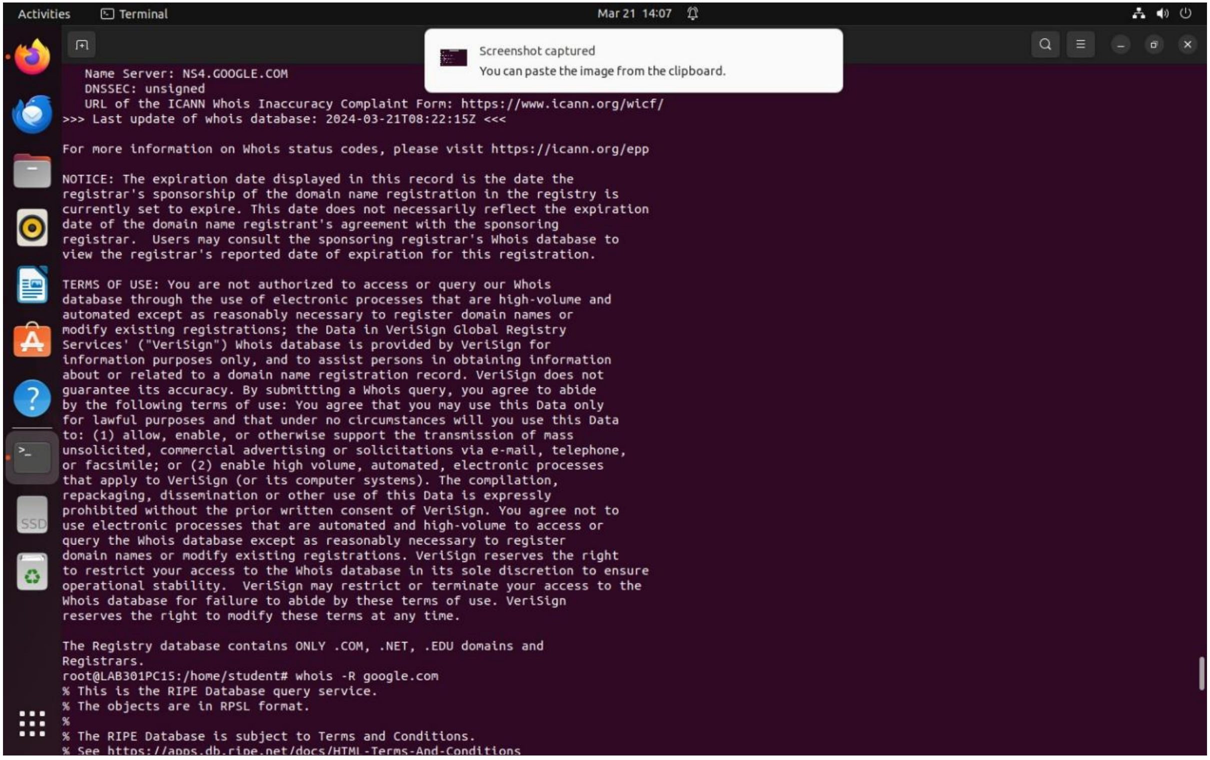
```
-r                      turn off recursive look-u
-R                      force to show local copy
                        if it contains referral
-a                      also search all the mirrored databases
-s SOURCE[,SOURCE]...   search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST    find updates from SOURCE from serial FIRST to LAST
-t TYPE                 request template for object of TYPE
-v TYPE                 request verbose template for object of TYPE
-q [version|sources|types]  query specified server info
root@LAB301PC15:/home/student# whois -V google.com
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST    connect to server HOST
-p PORT, --port PORT    connect to PORT
-I                      query whois.iana.org and follow its referral
-H                      hide legal disclaimers
      --verbose         explain what is being done
      --no-recursion    disable recursion from registry to registrar servers
      --help            display this help and exit
      --version         output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                      find the one level less specific match
-L                      find all levels less specific matches
-m                      find all one level more specific matches
-M                      find all levels of more specific matches
-c                      find the smallest match containing a mnt-irt attribute
-x                      exact match
-b                      return brief IP address ranges with abuse contact
-B                      turn off object filtering (show email addresses)
-G                      turn off grouping of associated objects
-d                      return DNS reverse delegation objects too
-i ATTR[,ATTR]...       do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...       only look for objects of TYPE
-K                      only primary keys are returned
-r                      turn off recursive look-ups for contact information
-R                      force to show local copy of the domain object even
                        if it contains referral
-a                      also search all the mirrored databases
-s SOURCE[,SOURCE]...   search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST    find updates from SOURCE from serial FIRST to LAST
-t TYPE                 request template for object of TYPE
-v TYPE                 request verbose template for object of TYPE
-q [version|sources|types]  query specified server info
root@LAB301PC15:/home/student# 
```

whois -T google.com: Specify query types.



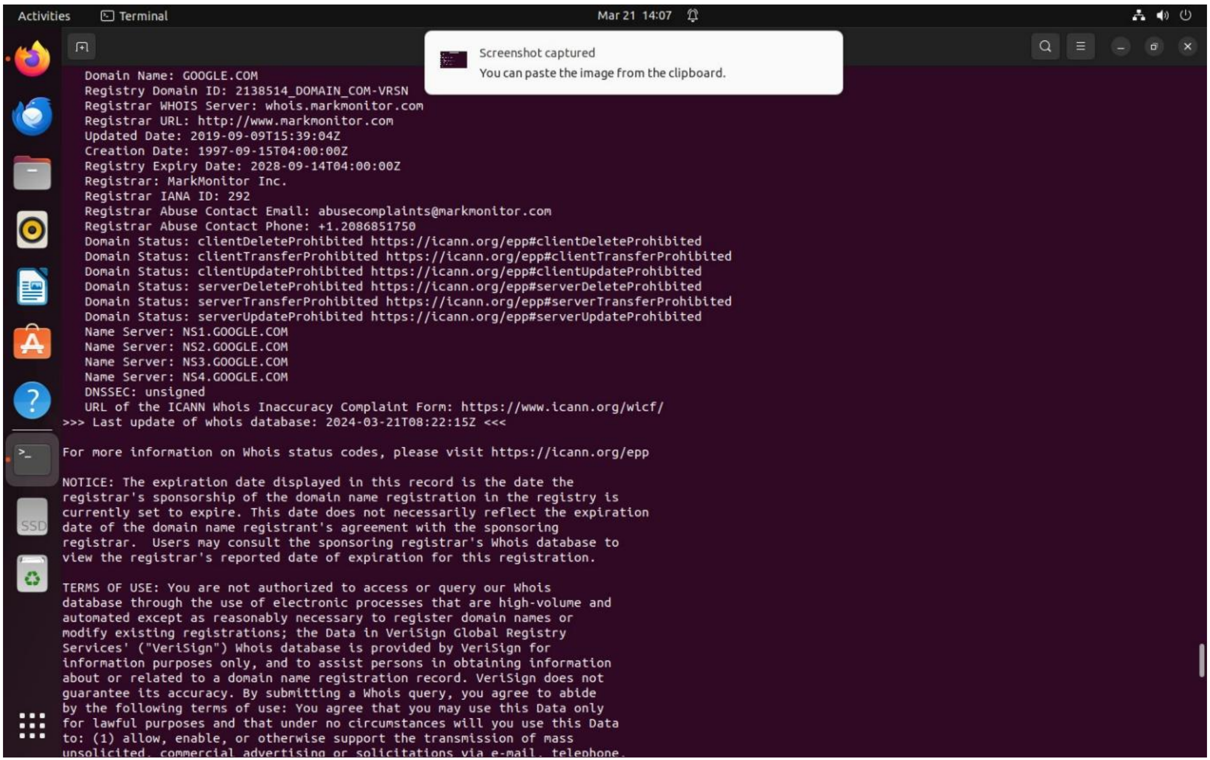
Screenshot captured
You can paste the image from the clipboard.

```
Whois database for failure to abide by these ter
reserves the right to modify these terms at any

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
root@LAB301PC15:/home/student# 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

%ERROR:111: invalid option supplied
%
% Use help query to see the valid options.

% This query was served by the RIPE Database Query Service version 1.109.1 (ABERDEEN)


root@LAB301PC15:/home/student# whois -T google.com
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST   connect to server HOST
-p PORT, --port PORT   connect to PORT
-I                     query whois.iana.org and follow its referral
-H                     hide legal disclaimers
      --verbose        explain what is being done
      --no-recursion   disable recursion from registry to registrar servers
      --help           display this help and exit
      --version        output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                     find the one level less specific match
-L                     find all levels less specific matches
-m                     find all one level more specific matches
-M                     find all levels of more specific matches
-c                     find the smallest match containing a mnt-irt attribute
-x                     exact match
-b                     return brief IP address ranges with abuse contact
-B                     turn off object filtering (show email addresses)
-G                     turn off grouping of associated objects
-d                     return DNS reverse delegation objects too
-i ATTR[,ATTR]...      do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]...      only look for objects of TYPE
-K                     only primary keys are returned
-r                     turn off recursive look-ups for contact information
```



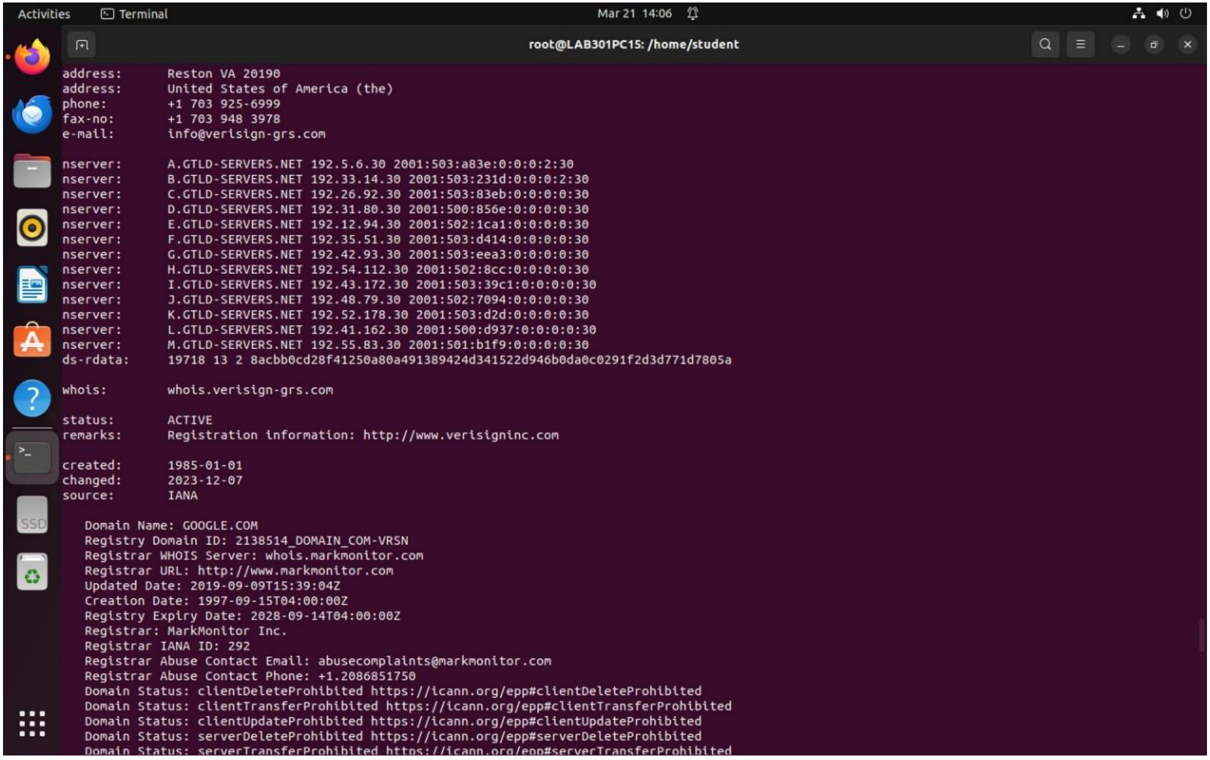
Screenshot captured
You can paste the image from the clipboard.

```
   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: 2024-03-21T08:22:15Z <<<

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
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
root@LAB301PC15:/home/student# 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
```



Screenshot captured
You can paste the image from the clipboard.

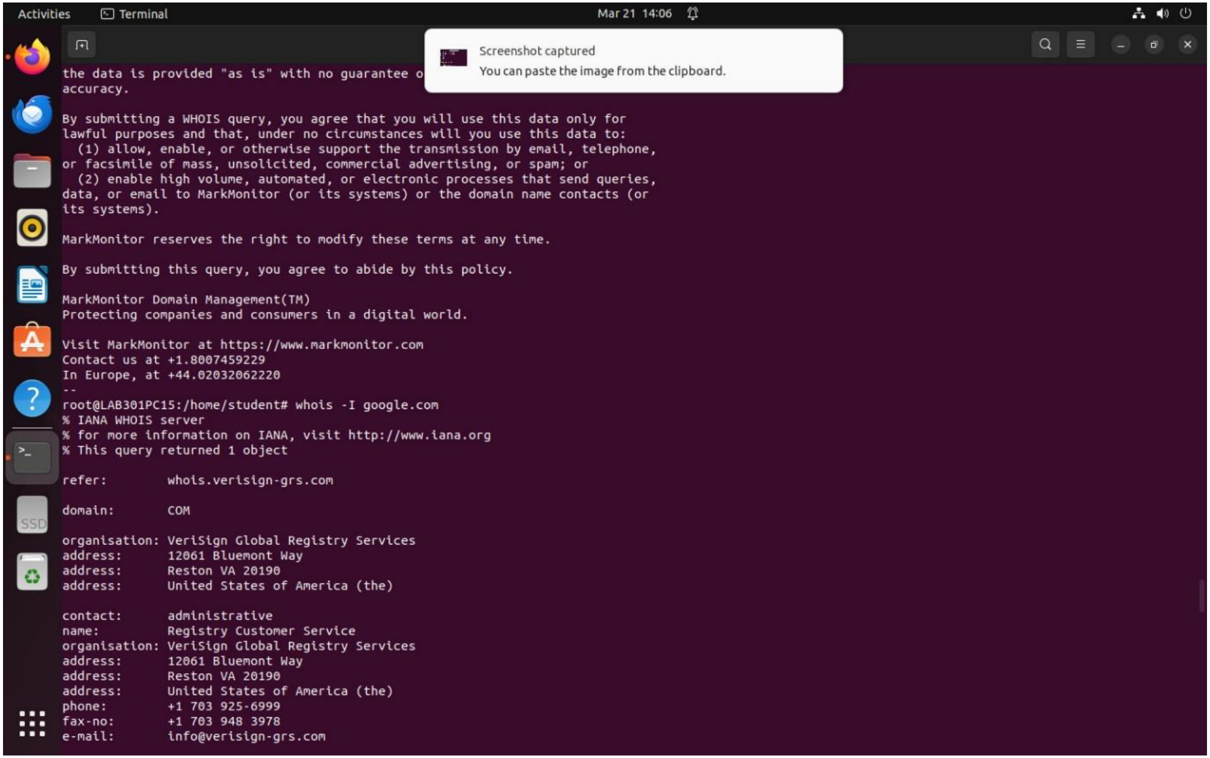
```
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: 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: 2024-03-21T08:22:15Z <<<

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
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
```



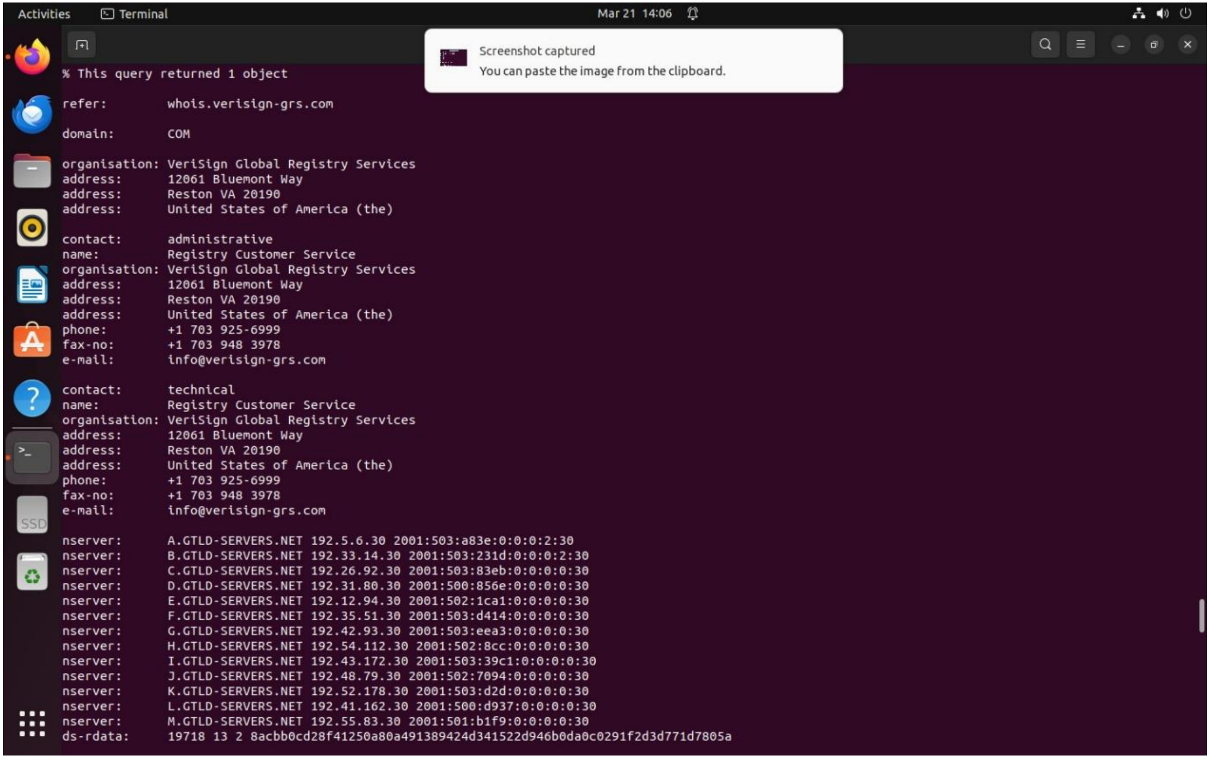
root@LAB301PC15: /home/student

```
address:      Reston VA 20190
address:      United States of America (the)
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

nserver:      A.GTLD-SERVERS.NET 192.5.6.30 2001:503:a83e:0:0:0:2:30
nserver:      B.GTLD-SERVERS.NET 192.33.14.30 2001:503:231d:0:0:0:2:30
nserver:      C.GTLD-SERVERS.NET 192.26.92.30 2001:503:83eb:0:0:0:0:30
nserver:      D.GTLD-SERVERS.NET 192.31.80.30 2001:500:856e:0:0:0:0:30
nserver:      E.GTLD-SERVERS.NET 192.12.94.30 2001:502:1ca1:0:0:0:0:30
nserver:      F.GTLD-SERVERS.NET 192.35.51.30 2001:503:d414:0:0:0:0:30
nserver:      G.GTLD-SERVERS.NET 192.42.93.30 2001:503:eea3:0:0:0:0:30
nserver:      H.GTLD-SERVERS.NET 192.54.112.30 2001:502:8cc:0:0:0:0:30
nserver:      I.GTLD-SERVERS.NET 192.43.172.30 2001:503:39c1:0:0:0:0:30
nserver:      J.GTLD-SERVERS.NET 192.48.79.30 2001:502:7094:0:0:0:0:30
nserver:      K.GTLD-SERVERS.NET 192.52.178.30 2001:503:d2d:0:0:0:0:30
nserver:      L.GTLD-SERVERS.NET 192.41.162.30 2001:500:d937:0:0:0:0:30
nserver:      M.GTLD-SERVERS.NET 192.55.83.30 2001:501:b1f9:0:0:0:0:30
ds-rdata:     19718 13 2 8acbb0cd28f41250a80a491389424d341522d946b0da0c0291f2d3d771d7805a

whois:        whois.verisign-grs.com

status:       ACTIVE
remarks:      Registration information: http://www.verisigninc.com

created:      1985-01-01
changed:      2023-12-07
source:       IANA

   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
```

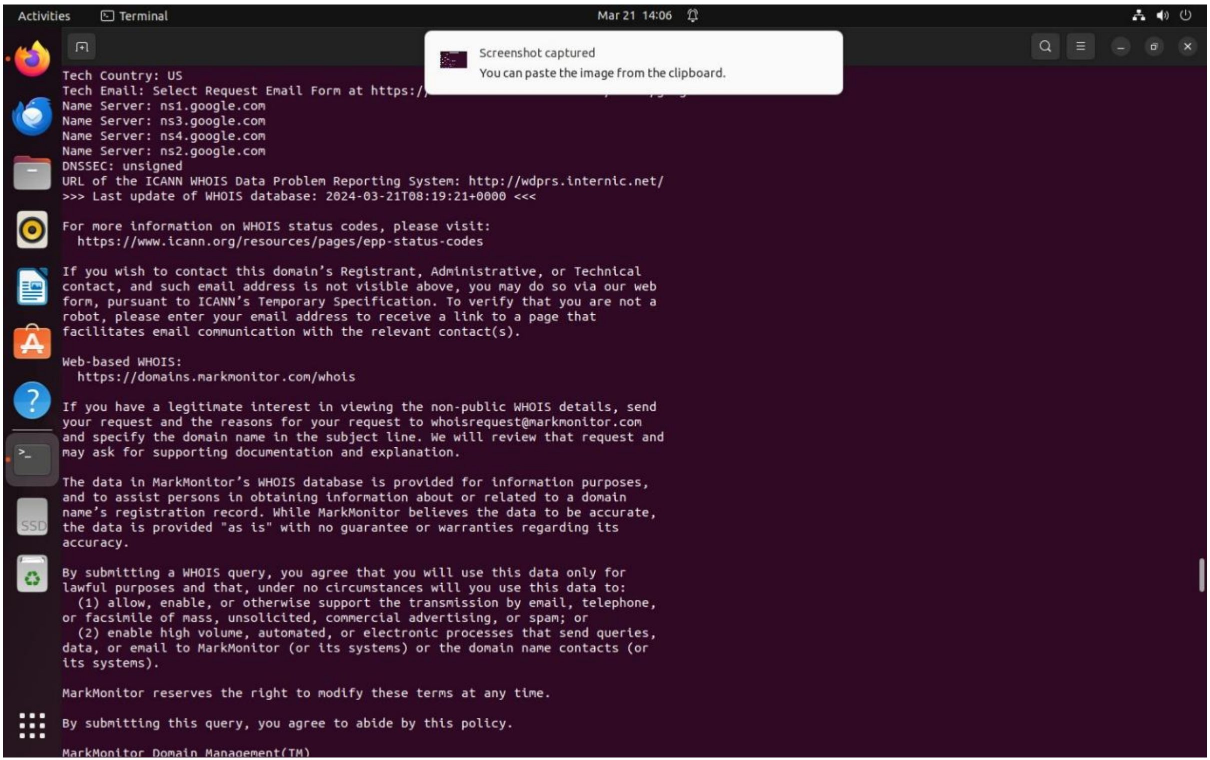
whois -I google.com: Enable case-insensitive lookups.



```
the data is provided "as is" with no guarantee o
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
  (1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
  (2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220
--
root@LAB301PC15:/home/student# whois -I google.com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.verisign-grs.com

domain:       COM

organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)

contact:      administrative
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com
```

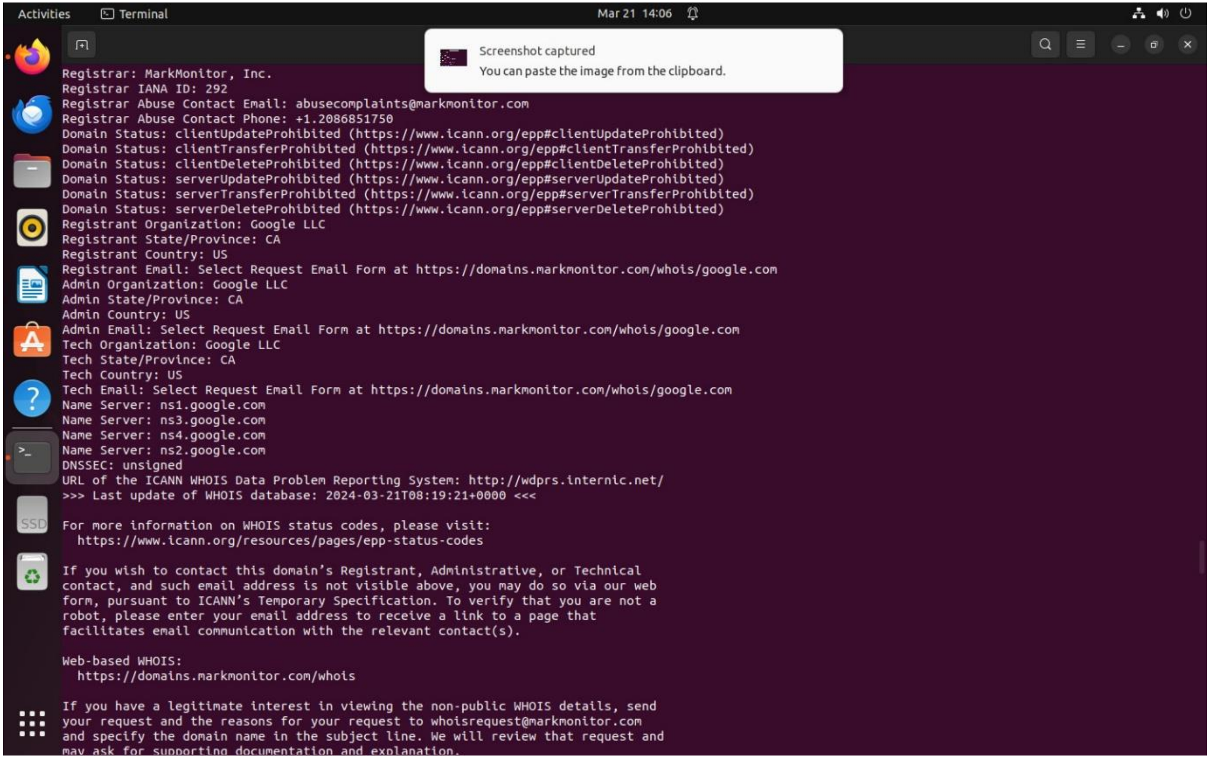


```
% This query returned 1 object

refer:        whois.verisign-grs.com

domain:       COM

organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)

contact:      administrative
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

contact:      technical
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

nserver:      A.GTLD-SERVERS.NET 192.5.6.30 2001:503:a83e:0:0:0:2:30
nserver:      B.GTLD-SERVERS.NET 192.33.14.30 2001:503:231d:0:0:0:2:30
nserver:      C.GTLD-SERVERS.NET 192.26.92.30 2001:503:83eb:0:0:0:0:30
nserver:      D.GTLD-SERVERS.NET 192.31.80.30 2001:500:856e:0:0:0:0:30
nserver:      E.GTLD-SERVERS.NET 192.12.94.30 2001:502:1ca1:0:0:0:0:30
nserver:      F.GTLD-SERVERS.NET 192.35.51.30 2001:503:d414:0:0:0:0:30
nserver:      G.GTLD-SERVERS.NET 192.42.93.30 2001:503:eea3:0:0:0:0:30
nserver:      H.GTLD-SERVERS.NET 192.54.112.30 2001:502:8cc:0:0:0:0:30
nserver:      I.GTLD-SERVERS.NET 192.43.172.30 2001:503:39c1:0:0:0:0:30
nserver:      J.GTLD-SERVERS.NET 192.48.79.30 2001:502:7094:0:0:0:0:30
nserver:      K.GTLD-SERVERS.NET 192.52.178.30 2001:503:d2d:0:0:0:0:30
nserver:      L.GTLD-SERVERS.NET 192.41.162.30 2001:500:d937:0:0:0:0:30
nserver:      M.GTLD-SERVERS.NET 192.55.83.30 2001:501:b1f9:0:0:0:0:30
ds-rdata:     19718 13 2 8acbb0cd28f41250a80a491389424d341522d946b0da0c0291f2d3d771d7805a
```



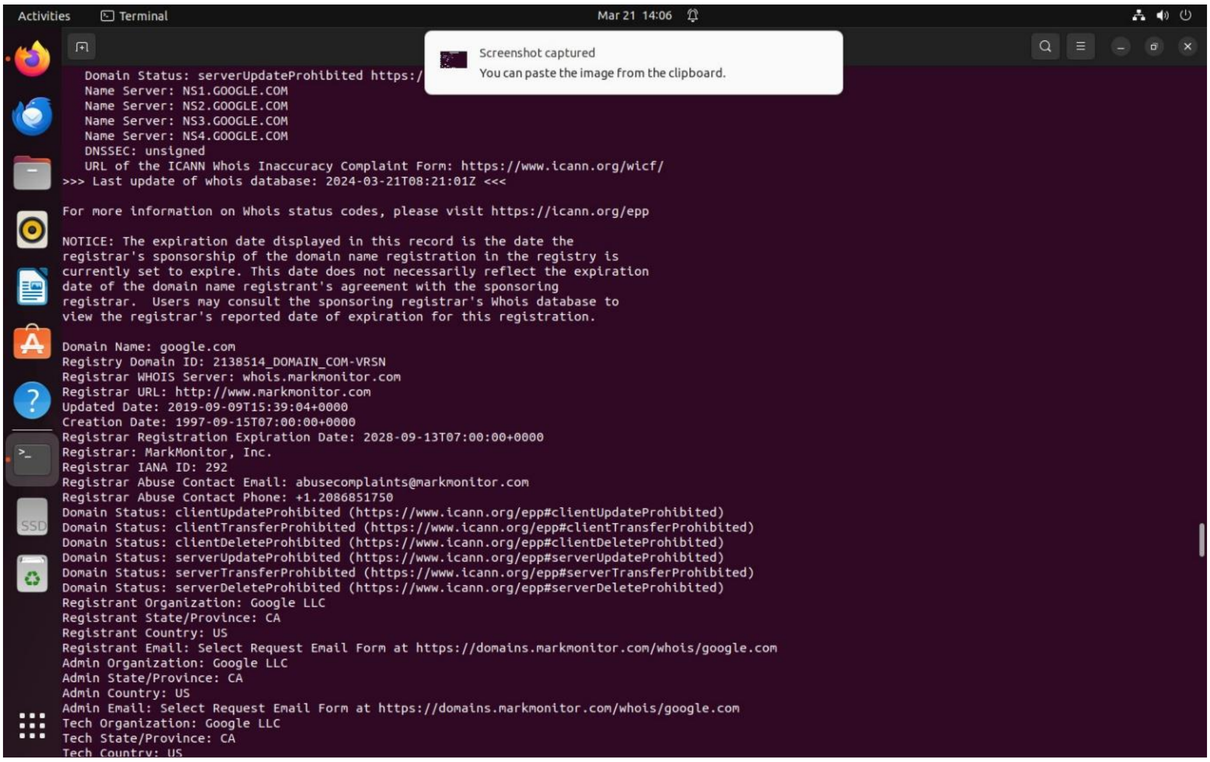
Screenshot captured
You can paste the image from the clipboard.

```
Tech Country: US
Tech Email: Select Request Email Form at https:/
Name Server: ns1.google.com
Name Server: ns3.google.com
Name Server: ns4.google.com
Name Server: ns2.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-03-21T08:19:21+0000 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
  (1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
  (2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)
```



Screenshot captured
You can paste the image from the clipboard.

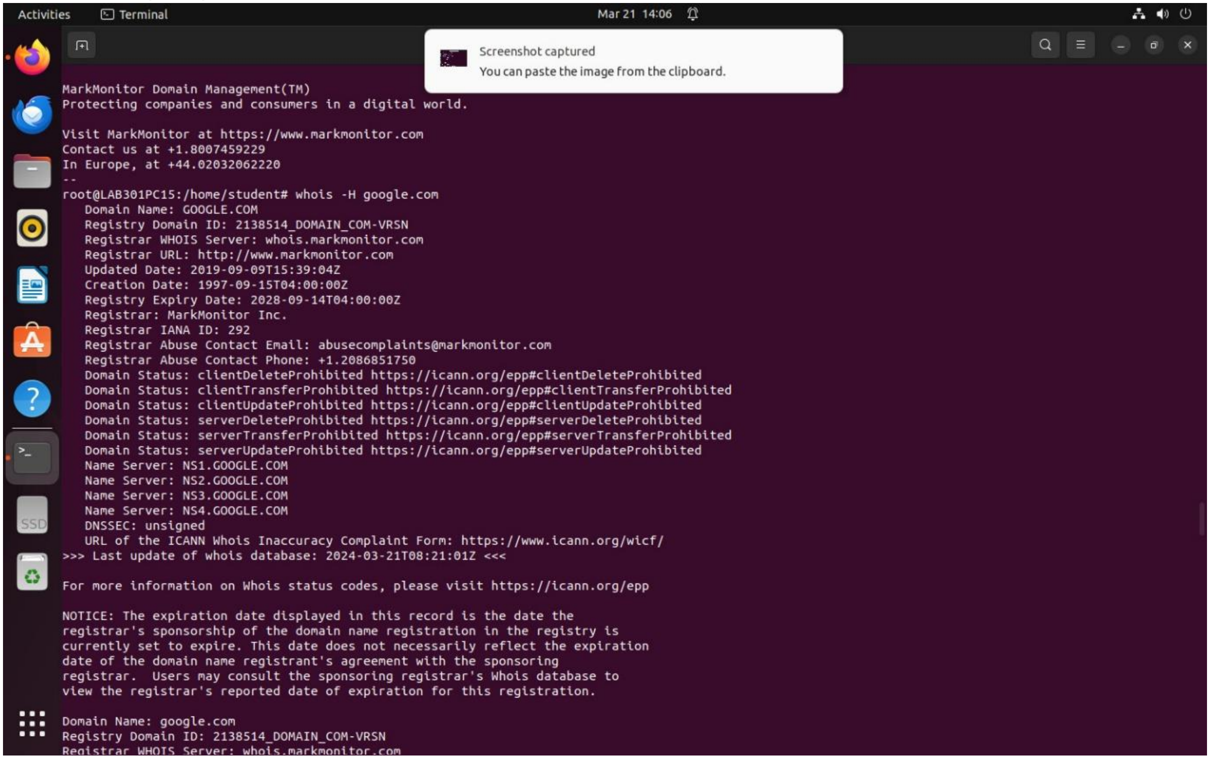
```
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
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
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns1.google.com
Name Server: ns3.google.com
Name Server: ns4.google.com
Name Server: ns2.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-03-21T08:19:21+0000 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.
```



Screenshot captured
You can paste the image from the clipboard.

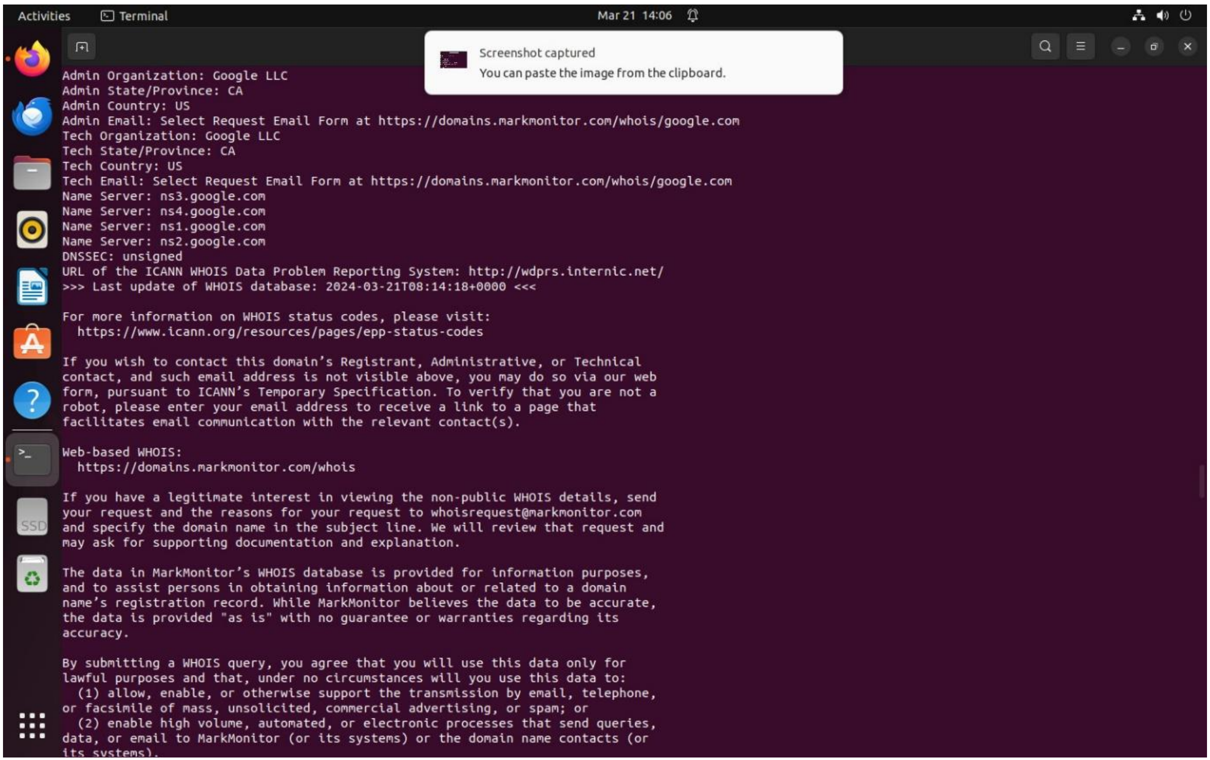
```
   Domain Status: serverUpdateProhibited https:/
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-03-21T08:21:01Z <<<

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
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
```

whois -H google.com: Hide legal disclaimers.



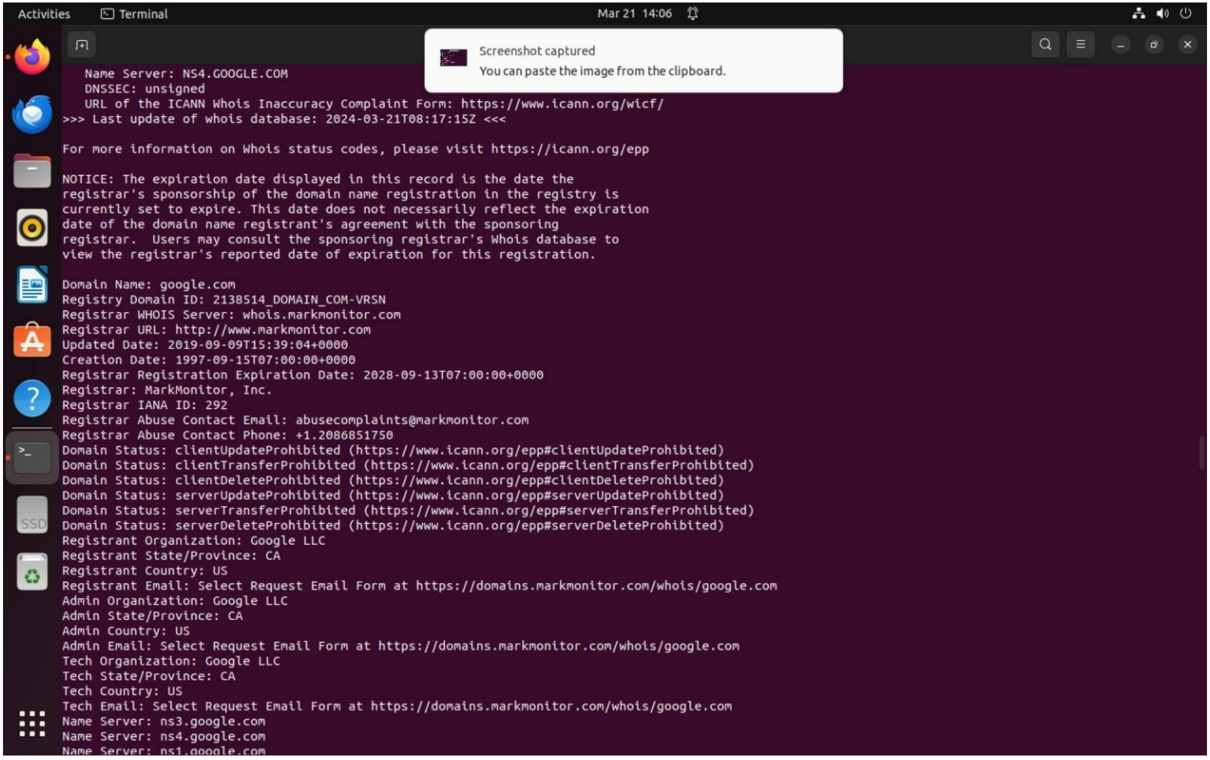
Screenshot captured
You can paste the image from the clipboard.

```
MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220
--
root@LAB301PC15:/home/student# 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: 2024-03-21T08:21:01Z <<<

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
```



Screenshot captured
You can paste the image from the clipboard.

```
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns3.google.com
Name Server: ns4.google.com
Name Server: ns1.google.com
Name Server: ns2.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-03-21T08:14:18+0000 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain’s Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN’s Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor’s WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name’s registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
  (1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
  (2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).
```



Screenshot captured
You can paste the image from the clipboard.

```
   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: 2024-03-21T08:17:15Z <<<

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
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns3.google.com
Name Server: ns4.google.com
Name Server: ns1.google.com
```