Experiment 07

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

Roll No.	19
Name	Manav Jawrani
Class	D15-A
Subject	Security Lab
LO Mapped	LO3: Explore the different network reconnaissance tools to gather information about networks

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

Theory:

1. Whois: -

whois searches for an object in a WHOIS database. WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block, but is also used for a wider range of other information.
Most modern versions of whois try to guess the right server to ask for the specified object. If no guess can be made, whois will connect to whois.networksolutions.com for NIC handles or whois.arin.net for IPv4 addresses and network names.

Syntax:
whois [-h HOST] [-p PORT] [-aCFHlLMmrRSVx] [-g SOURCE:FIRST-LAST]
[-i ATTR] [-S SOURCE] [-T TYPE] object

Options:
-h HOST Connect to WHOIS database host HOST.
-H Suppress the display of legal disclaimers.
-p PORT When connecting, connect to network port PORT.
--verbose Operate verbosely.
--help Display a help message, and exit.

2. Dig Command: -

dig command stands for Domain Information Groper. It is used for retrieving information about DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups. Dig command replaces older tools such as nslookup and the host.
Installing dig command:-

In case of Debian/Ubuntu
$sudo apt-get install dnsutils

Working with dig command:

1. To query domain "A" record
dig google.com
This command causes dig to look up the “A” record for the domain name “geeksforgeeks.org”.

2. To query domain "A" record with +short
dig google.com +short
By default dig is verbose and by using “+short” option we can reduce the output drastically
as shown.

3. To remove comment lines.
dig google.com +nocomments
This command makes a request and excludes the comment lines.

4. To set or clear all display flags.
dig google.com +noall

5. To query detailed answers.
dig google.com +noall +answer
If we want to view the answers section information in detail, we first stop the display of all section using "+noall" option and then query the answers section only by using "+answer" option with the dig command.

3. Traceroute command: -

traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes. Below image depicts how traceroute command is used to reach the Google(172.217.26.206) hosts from the local machine and it also prints details about all the hops that it visits in between.The first column corresponds to the hop count. The second column represents the address of that hop and after that, you see three space-separated time in milliseconds. traceroute command sends three packets to the hop and each of the time refers to the time taken by the packet to reach the hop.

Syntax:
traceroute host_Address
eg. traceroute google.com

4. nslookup command: -
nslookup (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems.

Syntax:
nslookup [option]
e.g.
nslookup google.com :
nslookup followed by the domain name will display the "A Record" (IP Address) of the domain. Use this command to find the address record for a domain. It queries to domain name servers and get the details.

nslookup -type=ns google.com : Lookup for an ns record
NS (Name Server) record maps a domain name to a list of DNS servers authoritative for that domain. It will output the name services which are associated with the given domain.

nslookup 192.168.0.10 : Reverse DNS lookup
You can also do the reverse DNS look-up by providing the IP Address as argument to nslookup.

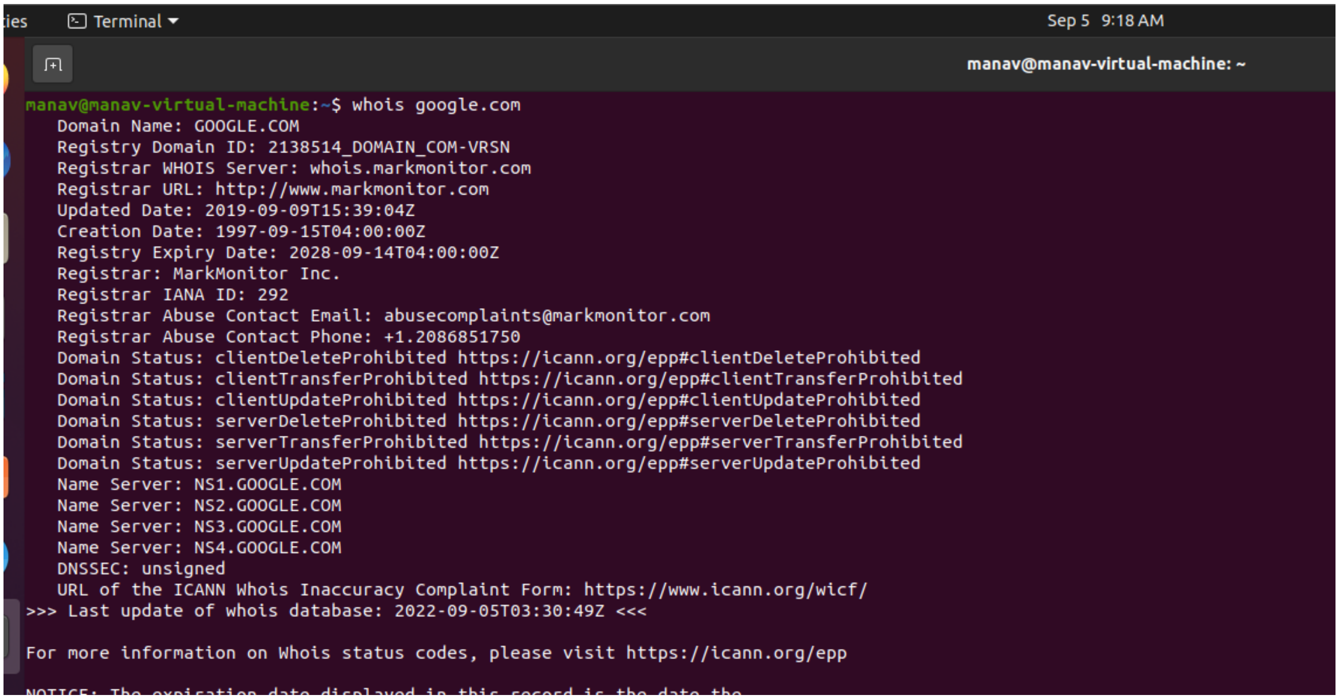
5. ping
PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. To stop pinging we should use ctrl+c otherwise it will keep on sending packets.

6. netstat

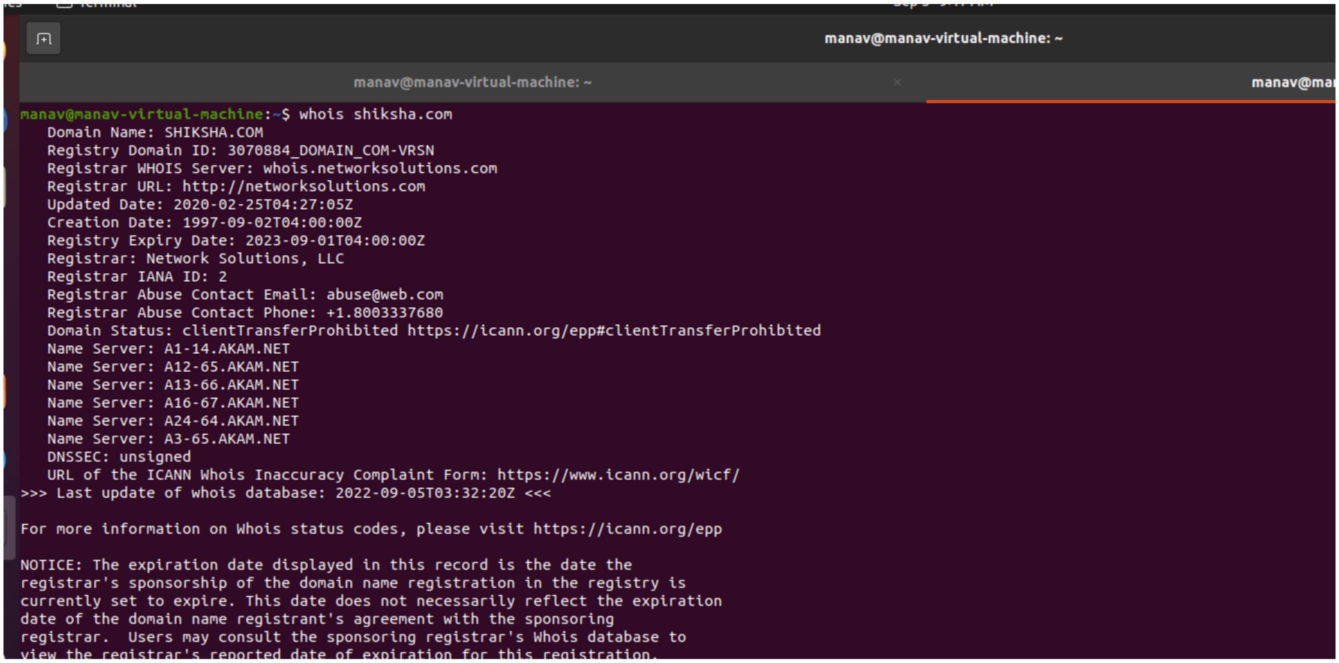
Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.

Results:

1. whois command

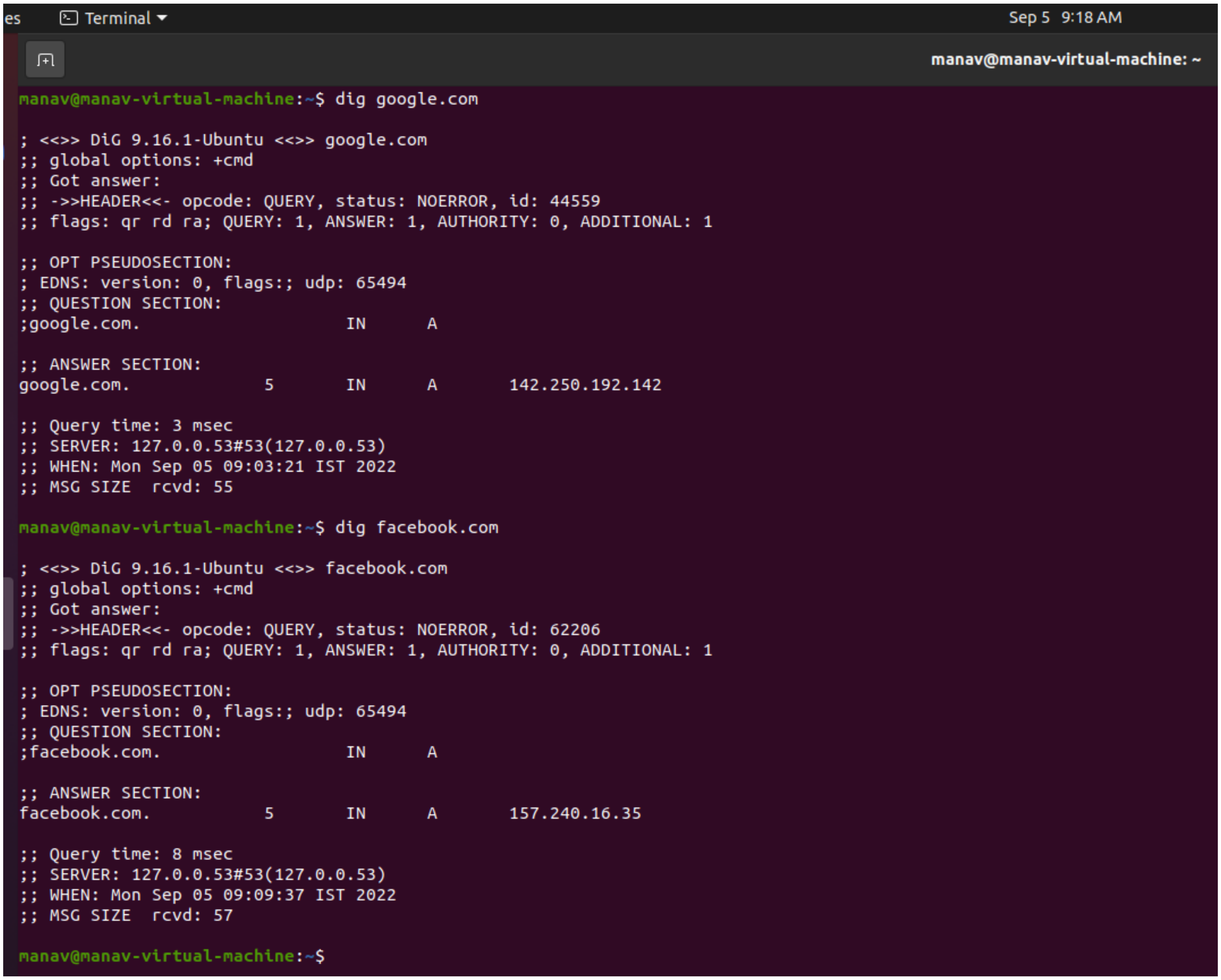


```
manav@manav-virtual-machine:~$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry 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: 2022-09-05T03:30:49Z <<<

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
```


manav@manav-virtual-machine: ~
manav@manav-virtual-machine: ~
manav@ma

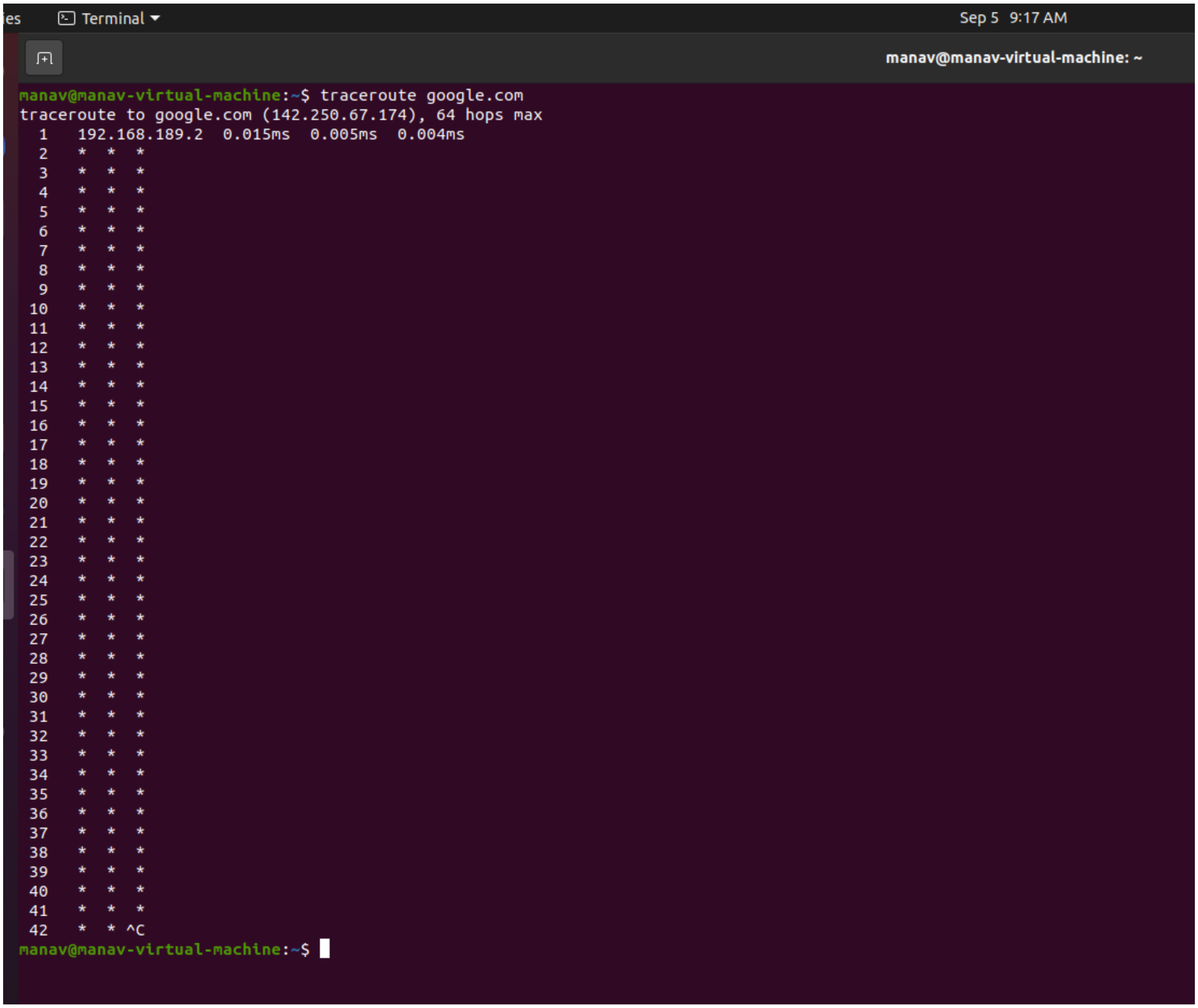
```
manav@manav-virtual-machine:~$ whois shiksha.com
   Domain Name: SHIKSHA.COM
   Registry Domain ID: 3070884_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.networksolutions.com
   Registrar URL: http://networksolutions.com
   Updated Date: 2020-02-25T04:27:05Z
   Creation Date: 1997-09-02T04:00:00Z
   Registry Expiry Date: 2023-09-01T04:00:00Z
   Registrar: Network Solutions, LLC
   Registrar IANA ID: 2
   Registrar Abuse Contact Email: abuse@web.com
   Registrar Abuse Contact Phone: +1.8003337680
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: A1-14.AKAM.NET
   Name Server: A12-65.AKAM.NET
   Name Server: A13-66.AKAM.NET
   Name Server: A16-67.AKAM.NET
   Name Server: A24-64.AKAM.NET
   Name Server: A3-65.AKAM.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-09-05T03:32:20Z <<<

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.
```

2. dig command



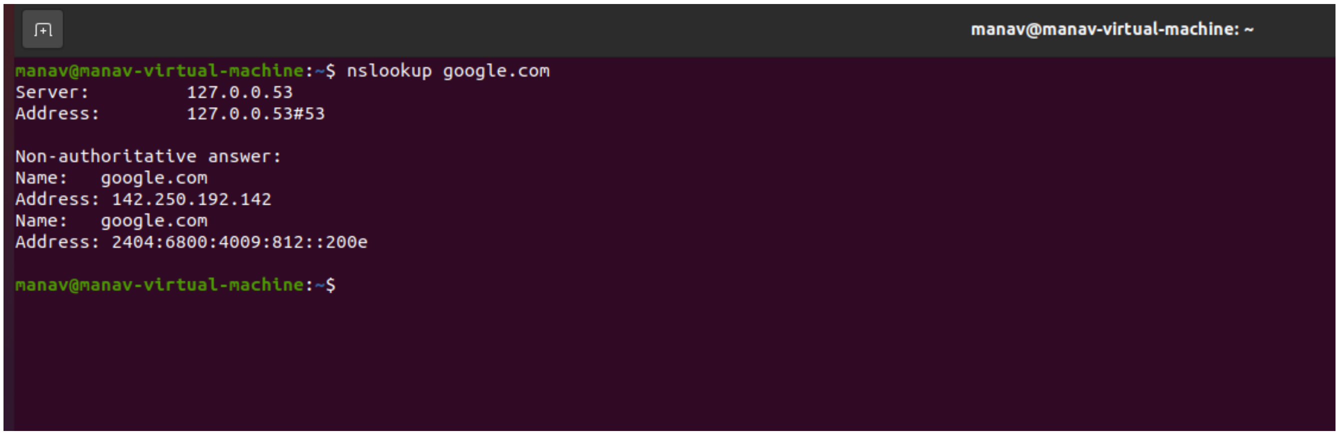
```
manav@manav-virtual-machine:~$ dig google.com

; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44559
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
google.com.             5       IN      A       142.250.192.142

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Sep 05 09:03:21 IST 2022
;; MSG SIZE  rcvd: 55

manav@manav-virtual-machine:~$ dig facebook.com

; <<>> DiG 9.16.1-Ubuntu <<>> facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62206
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
facebook.com.           5       IN      A       157.240.16.35

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Sep 05 09:09:37 IST 2022
;; MSG SIZE  rcvd: 57

manav@manav-virtual-machine:~$
```

3. traceroute command



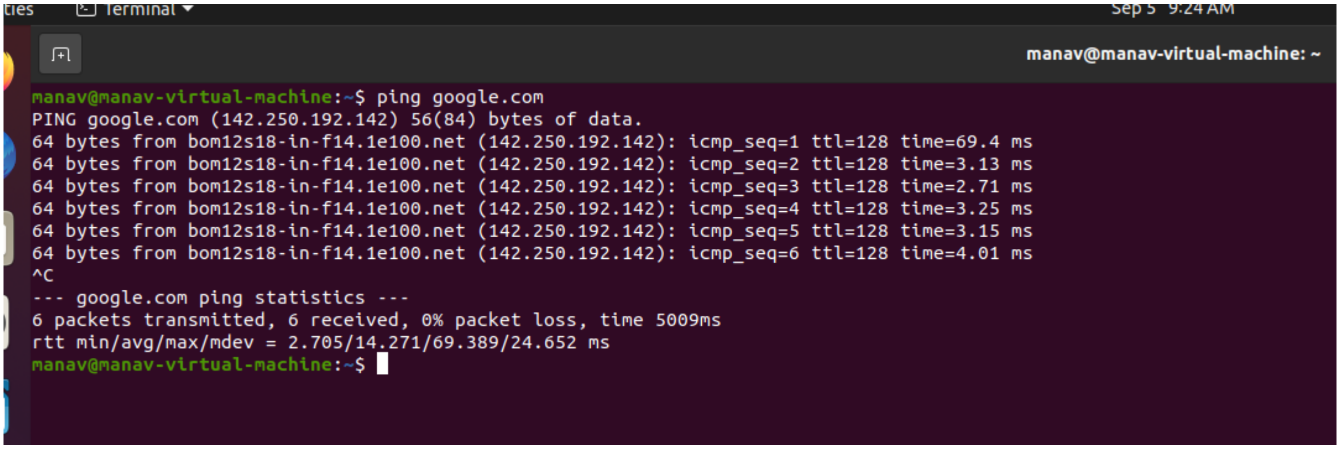
```
manav@manav-virtual-machine:~$ traceroute google.com
traceroute to google.com (142.250.67.174), 64 hops max
  1   192.168.189.2  0.015ms  0.005ms  0.004ms
  2   *  *  *
  3   *  *  *
  4   *  *  *
  5   *  *  *
  6   *  *  *
  7   *  *  *
  8   *  *  *
  9   *  *  *
 10   *  *  *
 11   *  *  *
 12   *  *  *
 13   *  *  *
 14   *  *  *
 15   *  *  *
 16   *  *  *
 17   *  *  *
 18   *  *  *
 19   *  *  *
 20   *  *  *
 21   *  *  *
 22   *  *  *
 23   *  *  *
 24   *  *  *
 25   *  *  *
 26   *  *  *
 27   *  *  *
 28   *  *  *
 29   *  *  *
 30   *  *  *
 31   *  *  *
 32   *  *  *
 33   *  *  *
 34   *  *  *
 35   *  *  *
 36   *  *  *
 37   *  *  *
 38   *  *  *
 39   *  *  *
 40   *  *  *
 41   *  *  *
 42   *  * ^C
manav@manav-virtual-machine:~$ 
```

4. nslookup



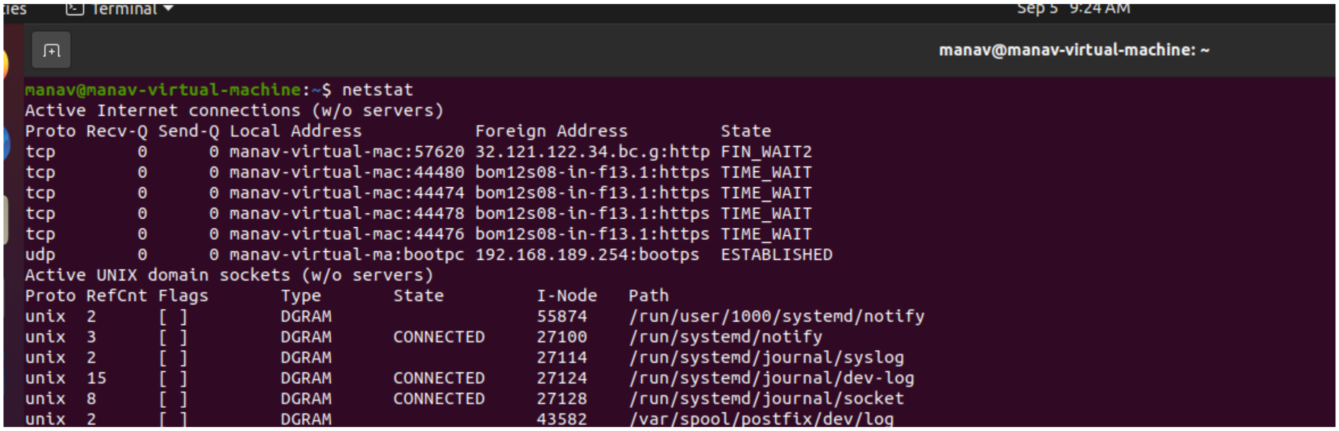
```
manav@manav-virtual-machine:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.192.142
Name:   google.com
Address: 2404:6800:4009:812::200e

manav@manav-virtual-machine:~$
```

5. ping



```
manav@manav-virtual-machine:~$ ping google.com
PING google.com (142.250.192.142) 56(84) bytes of data.
64 bytes from bom12s18-in-f14.1e100.net (142.250.192.142): icmp_seq=1 ttl=128 time=69.4 ms
64 bytes from bom12s18-in-f14.1e100.net (142.250.192.142): icmp_seq=2 ttl=128 time=3.13 ms
64 bytes from bom12s18-in-f14.1e100.net (142.250.192.142): icmp_seq=3 ttl=128 time=2.71 ms
64 bytes from bom12s18-in-f14.1e100.net (142.250.192.142): icmp_seq=4 ttl=128 time=3.25 ms
64 bytes from bom12s18-in-f14.1e100.net (142.250.192.142): icmp_seq=5 ttl=128 time=3.15 ms
64 bytes from bom12s18-in-f14.1e100.net (142.250.192.142): icmp_seq=6 ttl=128 time=4.01 ms
^C
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 2.705/14.271/69.389/24.652 ms
manav@manav-virtual-machine:~$ 
```

6. netstat



```
manav@manav-virtual-machine:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 manav-virtual-mac:57620 32.121.122.34.bc.g:http FIN_WAIT2
tcp        0      0 manav-virtual-mac:44480 bom12s08-in-f13.1:https TIME_WAIT
tcp        0      0 manav-virtual-mac:44474 bom12s08-in-f13.1:https TIME_WAIT
tcp        0      0 manav-virtual-mac:44478 bom12s08-in-f13.1:https TIME_WAIT
tcp        0      0 manav-virtual-mac:44476 bom12s08-in-f13.1:https TIME_WAIT
udp        0      0 manav-virtual-ma:bootpc 192.168.189.254:bootps  ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    55874    /run/user/1000/systemd/notify
unix  3      [ ]         DGRAM      CONNECTED     27100    /run/systemd/notify
unix  2      [ ]         DGRAM                    27114    /run/systemd/journal/syslog
unix  15     [ ]         DGRAM      CONNECTED     27124    /run/systemd/journal/dev-log
unix  8      [ ]         DGRAM      CONNECTED     27128    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    43582    /var/spool/postfix/dev/log
```

<u>Conclusion</u>:

Thus, we have studied the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.