NAME : KHUSHBOO
ROLL NO -16 D15 IT

EXPERIMENT - 6

COMMANDS :

1. dig :

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 This is your input. Since we said 'dig redhat.com', and the default type dig command uses is A record, it indicates in this section that we asked for the A record of the redhat.com website
- ANSWER SECTION: This displays the answer it receives from the DNS. i.e This is your output. This displays the A record of redhat.com
- AUTHORITY SECTION: This displays the DNS name server that has the authority to respond to this query. Basically this displays available name servers of redhat.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 including how much time it took to execute this query

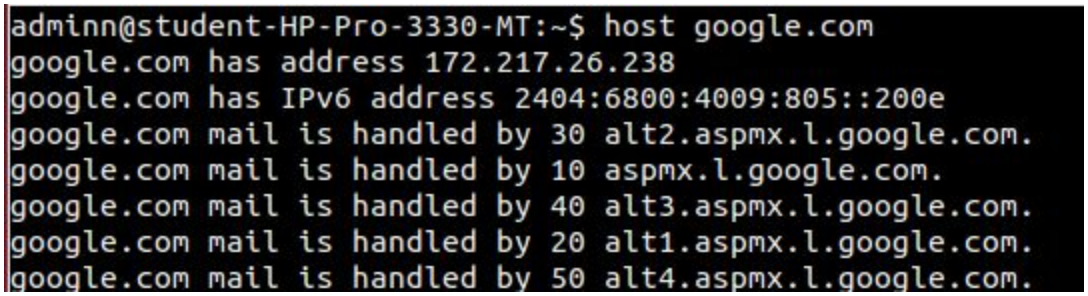
```
adminn@student-HP-Pro-3330-MT:~$ dig certifiedhacker.com

; <<>> DiG 9.9.5-3ubuntu0.17-Ubuntu <<>> certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5797
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;certifiedhacker.com.           IN      A

;; ANSWER SECTION:
certifiedhacker.com.    14399   IN      A       162.241.216.11

;; Query time: 268 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sat Aug 25 09:48:09 IST 2018
;; MSG SIZE  rcvd: 64
```

```
adminn@student-HP-Pro-3330-MT:~$ dig google.com

; <<>> DiG 9.9.5-3ubuntu0.17-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48727
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             76      IN      A       172.217.26.238

;; AUTHORITY SECTION:
google.com.             19004   IN      NS      ns4.google.com.
google.com.             19004   IN      NS      ns2.google.com.
google.com.             19004   IN      NS      ns1.google.com.
google.com.             19004   IN      NS      ns3.google.com.

;; ADDITIONAL SECTION:
ns4.google.com.         21350   IN      A       216.239.38.10
ns4.google.com.         21350   IN      AAAA    2001:4860:4802:38::a
ns1.google.com.         21350   IN      A       216.239.32.10
ns1.google.com.         21350   IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         21350   IN      A       216.239.34.10
ns2.google.com.         21350   IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         21350   IN      A       216.239.36.10
ns3.google.com.         21350   IN      AAAA    2001:4860:4802:36::a

;; Query time: 7 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sat Aug 25 09:48:35 IST 2018
;; MSG SIZE  rcvd: 303
```

2 . host :

host is a simple utility for performing DNS lookups. It is normally used to convert names to IP addresses and vice versa. When no arguments or options are given, **host** prints a short summary of its **command** line arguments and options. name is the domain name that is to be looked up.

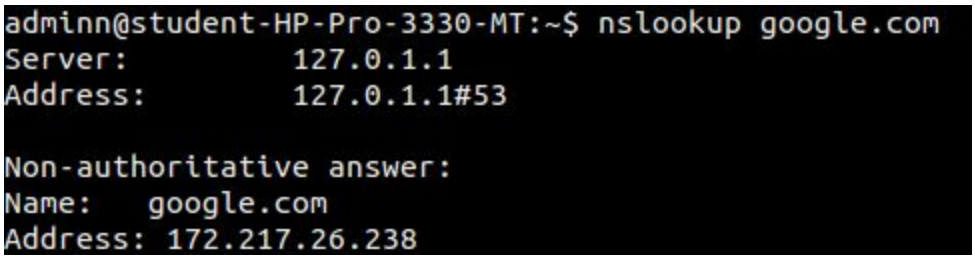
```
adminn@student-HP-Pro-3330-MT:~$ host certifiedhacker.com
certifiedhacker.com has address 162.241.216.11
certifiedhacker.com mail is handled by 0 mail.certifiedhacker.com.
```



3 . nslookup :

nslookup (name server lookup) is a tool used to perform DNS lookups in Linux. It is used to display DNS details, such as the IP address of a particular computer, the MX records for a domain or the NSservers of a domain.

nslookup can operate in two modes: interactive and non-interactive. The interactive mode allows you to query name servers for information about various hosts and domains or to print a list of hosts in a domain. The non-interactive mode allows you to print just the name and requested information for a host or domain.



4 . traceroute :

The traceroute command is used in Linux to map the journey that a packet of information undertakes from its source to its destination. One use for traceroute is to locate when data loss occurs throughout a network, which could signify a node that's down.

Because each hop in the record reflects a new server or router between the originating PC and the intended target, reviewing the results of a traceroute scan also lets you identify slow points that may adversely affect your network traffic.

```
adminn@student-HP-Pro-3330-MT:~$ traceroute certifiedhacker.com
traceroute to certifiedhacker.com (162.241.216.11), 64 hops max
  1   192.168.32.1  0.230ms  0.250ms  0.217ms
  2   103.197.221.161  0.522ms  0.341ms  0.325ms
  3   103.197.223.17  2.088ms  0.731ms  0.509ms
  4   *  *  *
  5   *  103.42.160.13  3.007ms  4.130ms
  6   182.79.245.26  69.270ms  56.949ms  57.305ms
  7   116.51.27.225  56.796ms  56.756ms  56.445ms
  8   129.250.3.146  66.236ms  67.608ms  66.371ms
  9   129.250.3.48  243.561ms  242.781ms  243.231ms
 10   129.250.2.183  242.907ms  239.456ms  269.982ms
 11   129.250.4.155  272.518ms  272.381ms  273.108ms
 12   129.250.5.4  291.873ms  322.495ms  303.358ms
 13   129.250.4.178  292.597ms  292.522ms  294.645ms
 14   131.103.117.102  286.055ms  285.579ms  285.869ms
 15   216.117.50.138  288.153ms  299.359ms  288.018ms
 16   108.167.150.98  262.780ms  262.432ms  262.233ms
 17   108.167.150.114  261.346ms  261.038ms  50.682ms
 18   162.241.216.11  283.903ms  282.044ms  281.672ms
```

5 . whois :

whois is a client for the WHOIS directory service.
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.comfor NIC handles or whois.arin.net for IPv4 addresses and network names.

```
adminn@student-HP-Pro-3330-MT:~$ whois certifiedhacker.com
   Domain Name: CERTIFIEDHACKER.COM
   Registry Domain ID: 88849376_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.networksolutions.com
   Registrar URL: http://networksolutions.com
   Updated Date: 2016-03-16T12:38:41Z
   Creation Date: 2002-07-30T00:32:00Z
   Registry Expiry Date: 2021-07-30T00:32:00Z
   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: NS1.BLUEHOST.COM
   Name Server: NS2.BLUEHOST.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2018-08-25T04:17:23Z <<<

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