Terna Engineering College

Computer Engineering Department

Class: TE **Sem.: VI**

Course: System Security Lab

PART A

(PART A: TO BE REFERRED BY STUDENTS)

Experiment No.04

A.1 Aim:

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

A.2 Prerequisite:

Basic Knowledge of IP addresses, DNS.

A.3 Outcome:

After the successful completion of this experiment, students will be able to apply basic network commands to gather basic network information.

A.4 Theory:

Network Reconnaissance:

- Act of reconnoitring ---explore to find something(especially to gain information about enemy)
- In the world of hacking, reconnaissance begins with “Footprinting”
- i.e accumulating data about the target’s environment, and finding vulnerabilities.
- The attacker gathers information in two phases viz: passive attacks and active attacks

Passive attacks:

- Gathering information about a target without his/her knowledge….Eavesdropping
- Yahoo or google search
- Surfing online community groups
- Gathering information from websites of organisations. e.g. contact details, email address etc.
- Blogs, newsgroups, press releases etc.
- Going through job posting in particular job profiles

Reconnaissance Tools:

- WHOIS, dig, traceroute, nslookup
- 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 domain's 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 Facebook.com

ssc@ssc-OptiPlex-380:~$ whois facebook.com
For more information on Whois status codes, please visit https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en.

- Domain Name: facebook.com
- Registry Domain ID: 2320948_DOMAIN_COM-VRSN
- Registrar WHOIS Server: whois.markmonitor.com Registrar URL: http://www.markmonitor.com
- Updated Date: 2014-10-28T12:38:28-0700
- Creation Date: 1997-03-28T21:00:00-0800
- Registrar Registration Expiration Date: 2020-03-29T21:00:00-0700 Registrar: MarkMonitor, Inc.
- Registrar IANA ID: 292
- Registrar Abuse Contact Email: abusecomplaints@markmonitor.com Registrar Abuse Contact Phone: +1.2083895740
- 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)
- Registry Registrant ID:
- Registrant Name: Domain Administrator Registrant Organization: Facebook, Inc.
- Registrant Street: 1601 Willow Road, Registrant City: Menlo Park
- Registrant State/Province: CA Registrant Postal Code: 94025

- Registrant Country: US
- Registrant Phone: +1.6505434800
- Registrant PhoneExt:
- Registrant Fax: +1.6505434800
- Registrant Fax Ext:
- Registrant Email: domain@fb.com Registry Admin ID:
- Admin Name: Domain Administrator Admin Organization: Facebook, Inc.
- Admin Street: 1601 Willow Road, Admin City: Menlo Park
- Admin State/Province: CA
- Admin Postal Code: 94025
- Admin Country: US
- Admin Phone: +1.6505434800
- Admin Phone Ext:
- Admin Fax: +1.6505434800
- Admin Fax Ext:
- Admin Email: domain@fb.com Registry Tech ID:
- Tech Name: Domain Administrator
- Tech Organization: Facebook, Inc. Tech Street: 1601 Willow Road, Tech City: Menlo Park
- Tech State/Province: CA
- Tech Postal Code: 94025
- Tech Country: US
- Tech Phone: +1.6505434800
- Tech Phone Ext:
- Tech Fax: +1.6505434800
- Tech Fax Ext:
- Tech Email: domain@fb.com
- Name Server: b.ns.facebook.com
- Name Server: a.ns.facebook.com
- DNSSEC: unsigned
- URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
  >>> Last update of WHOIS database: 2015-07-16T21:08:30-0700 <<<

The Data in Mark Monitor.com's WHOIS database is provided by MarkMonitor.com for information purposes, and to assist persons in obtaining information about or related to a domain name registration record. MarkMonitor.com does not guarantee 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:

- allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail (spam); or
- Enable high volume, automated, electronic processes that apply to MarkMonitor.com (or its systems).

MarkMonitor.com reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this policy.

MarkMonitor is the Global Leader in Online Brand Protection. MarkMonitor Domain Management(TM)

MarkMonitor Brand Protection(TM) MarkMonitorAntiPiracy(TM) MarkMonitorAntiFraud(TM) Professional and Managed Services

Visit MarkMonitor at http://www.markmonitor.com Contact us at +1.8007459229 In Europe, at +44.02032062220 ssc@ssc-OptiPlex-380:~$

- **Dig -** Dig is a networking tool that can query DNS servers for information. It can be beneficial for diagnosing problems with domain pointing and is a good way to verify that your configuration is working. The most basic way to use dig is to specify the domain we wish to query:

Example:

```
$ dig duckduckgo.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. For users who are new to the TTL field, this field describes how much hops a particular packet will take while travelling on the network. So, this effectively outlines the lifetime of the packet on the 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, the router sends an ICMP error message of ― Time exceeded‖ back to the source from where the 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 the TTL field is 1 then it discards the packet and sends the ICMP error packet containing its IP address and this is what the traceroute requires. So traceroute incrementally fetches the IP of all the routers between the source and the destination.

Example:

```
$traceroute example.com
```

PART B

(PART B: TO BE COMPLETED BY STUDENTS)

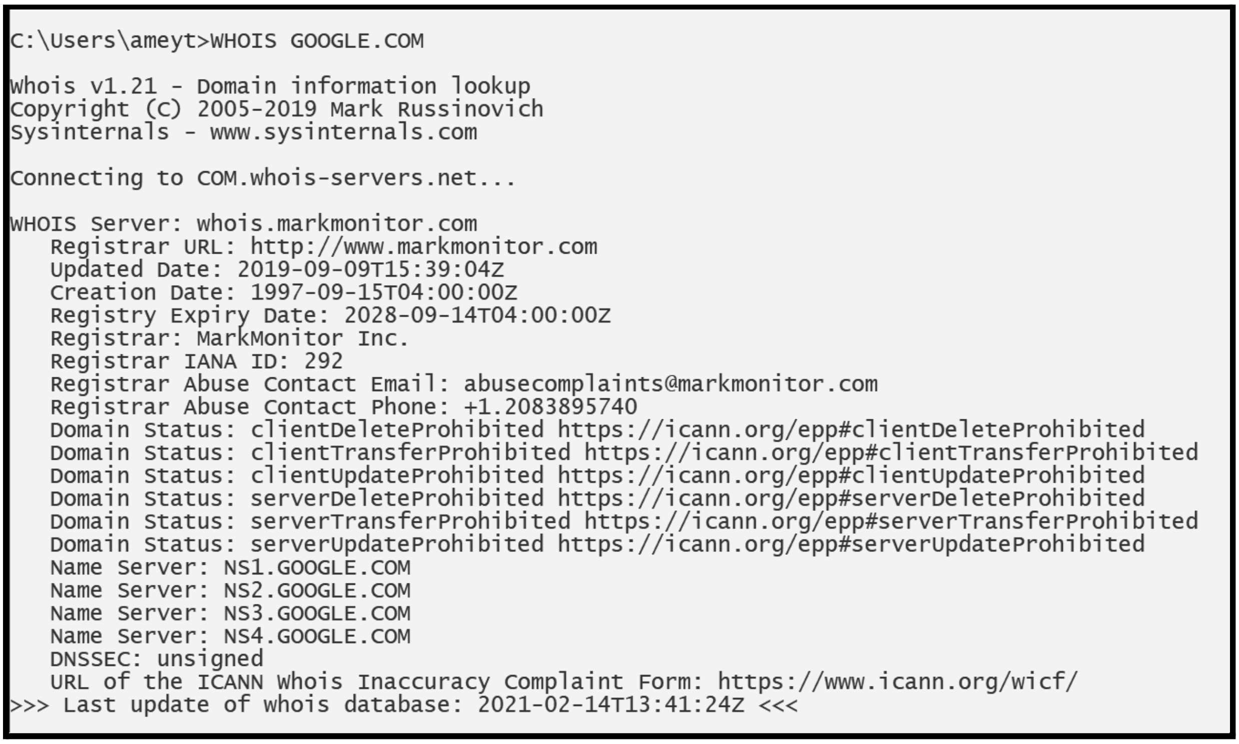
(Students must submit the soft copy as per the following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case there is no Blackboard access available)

Roll No. 50	**Name:** AMEY THAKUR
Class: Comps TE B	**Batch:** B3
Date of Experiment: 09/03/2021	**Date of Submission:** 09/03/2021
Grade:	

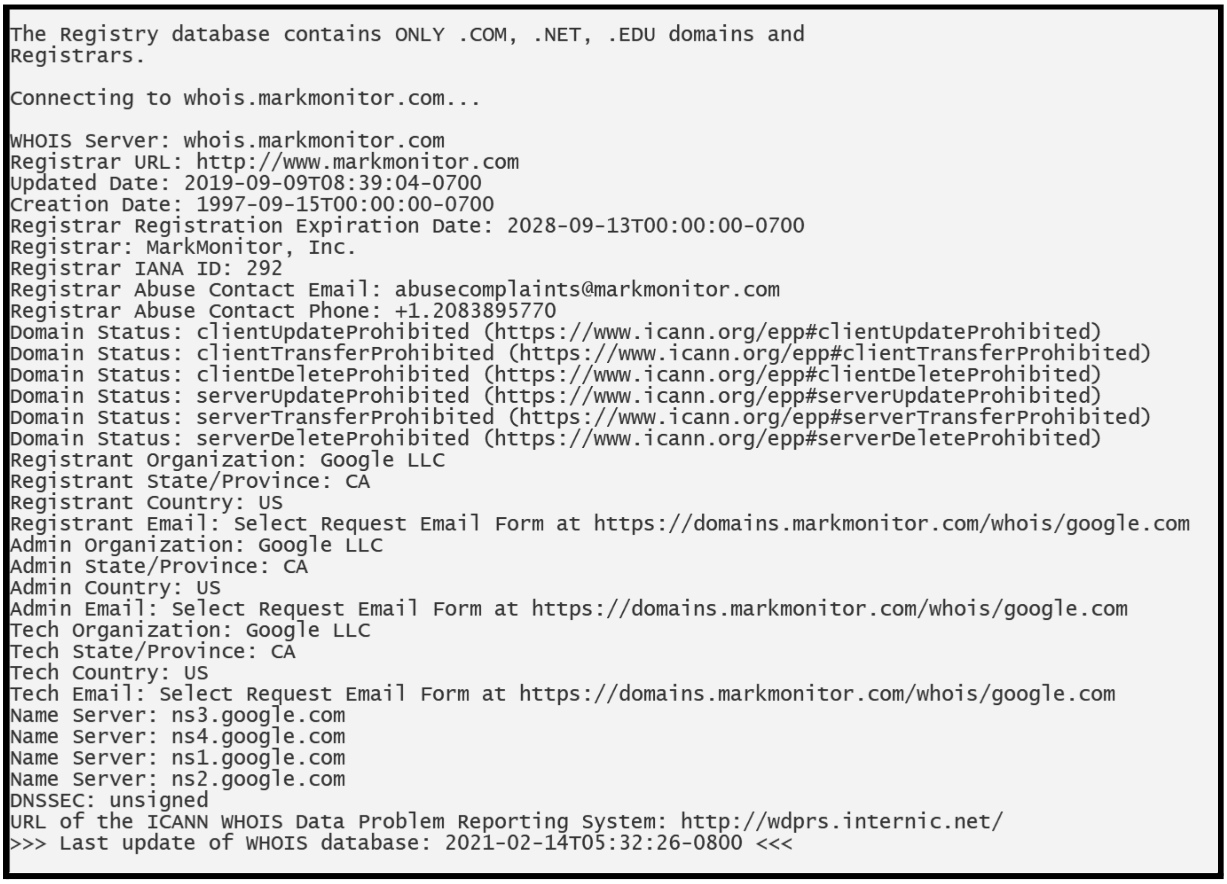
B.1 Output of Reconnaissance Tools

(add a snapshot of the output of Reconnaissance Tools)

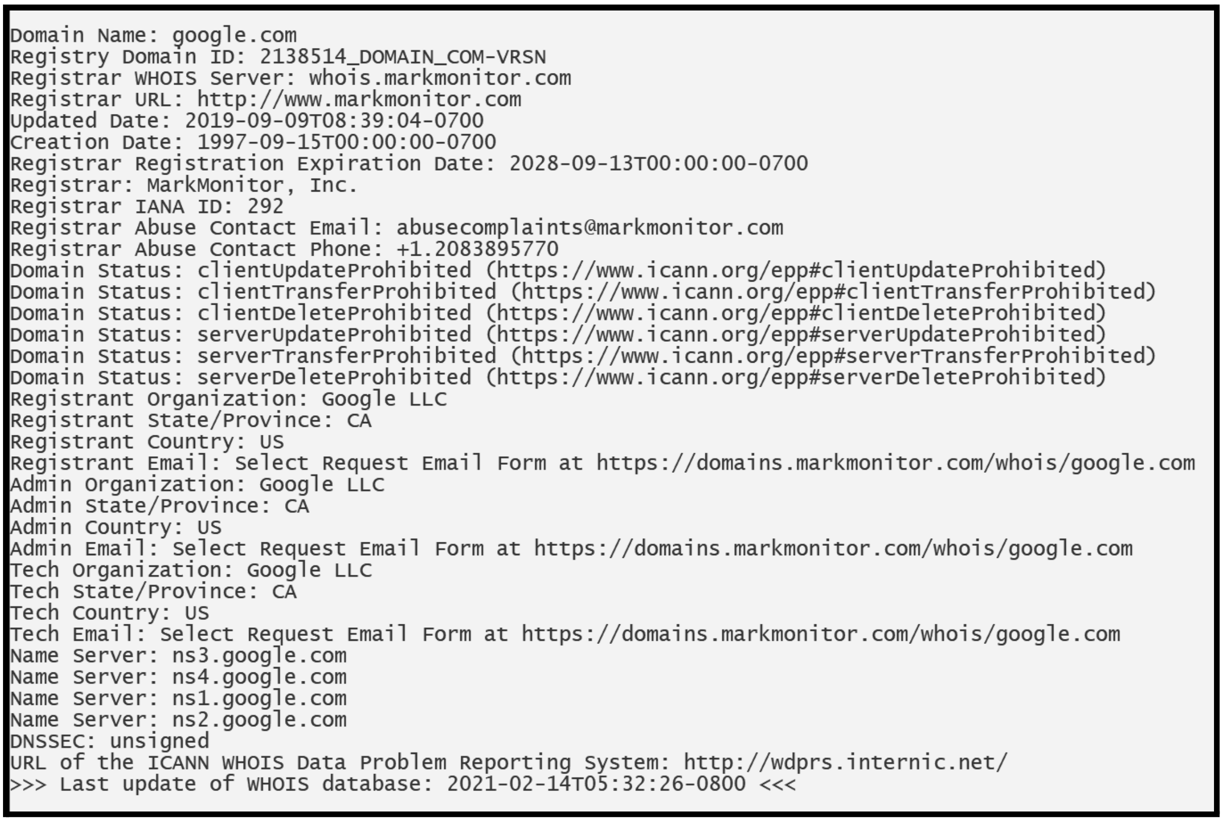
- **WHOIS (GOOGLE.COM)**



```
C:\Users\ameyt>WHOIS GOOGLE.COM

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...

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: +1.2083895740
   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: 2021-02-14T13:41:24Z <<<
```

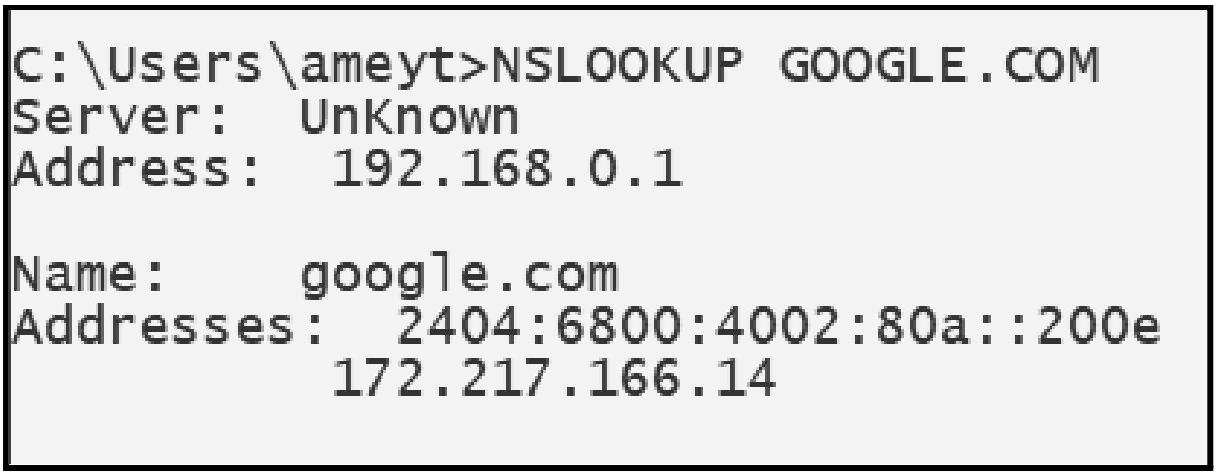


```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

Connecting to whois.markmonitor.com...

WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T08:39:04-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2028-09-13T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
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
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: 2021-02-14T05:32:26-0800 <<<
```



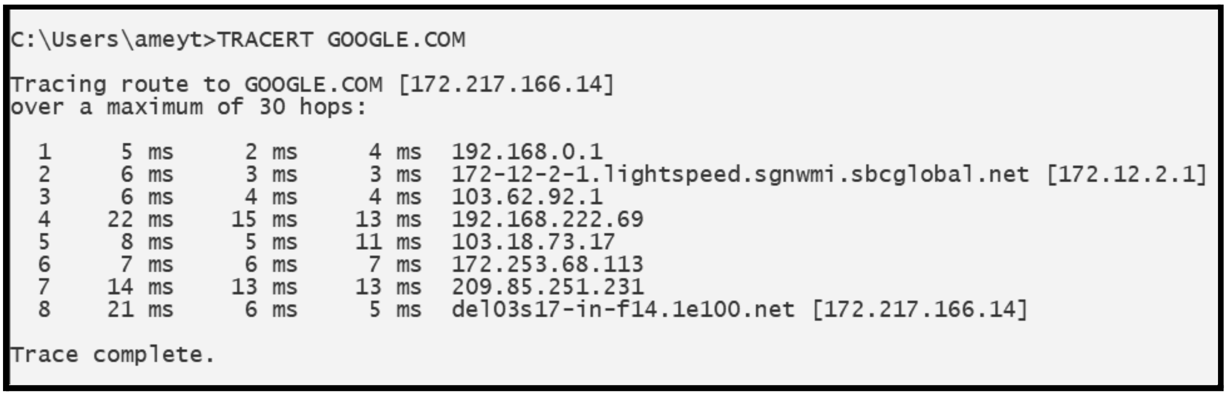
```
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T08:39:04-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2028-09-13T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
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
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: 2021-02-14T05:32:26-0800 <<<
```

- **NSLOOKUP (GOOGLE.COM)**



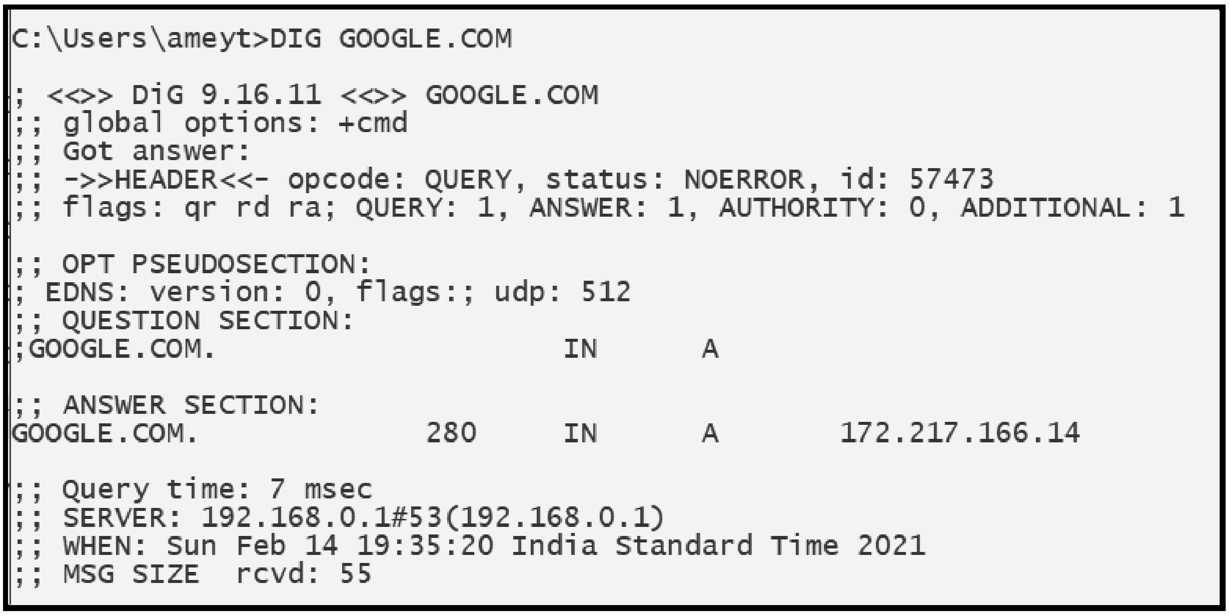
```
C:\Users\ameyt>NSLOOKUP GOOGLE.COM
Server:  UnKnown
Address:  192.168.0.1

Name:    google.com
Addresses:  2404:6800:4002:80a::200e
          172.217.166.14
```

- **TRACERT (GOOGLE.COM)**



```
C:\Users\ameyt>TRACERT GOOGLE.COM

Tracing route to GOOGLE.COM [172.217.166.14]
over a maximum of 30 hops:

  1     5 ms     2 ms     4 ms  192.168.0.1
  2     6 ms     3 ms     3 ms  172-12-2-1.lightspeed.sgnwmi.sbcglobal.net [172.12.2.1]
  3     6 ms     4 ms     4 ms  103.62.92.1
  4    22 ms    15 ms    13 ms  192.168.222.69
  5     8 ms     5 ms    11 ms  103.18.73.17
  6     7 ms     6 ms     7 ms  172.253.68.113
  7    14 ms    13 ms    13 ms  209.85.251.231
  8    21 ms     6 ms     5 ms  del03s17-in-f14.1e100.net [172.217.166.14]

Trace complete.
```

- **DIG (GOOGLE.COM)**



```
C:\Users\ameyt>DIG GOOGLE.COM

; <<>> DiG 9.16.11 <<>> GOOGLE.COM
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57473
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
GOOGLE.COM.             280     IN      A       172.217.166.14

;; Query time: 7 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sun Feb 14 19:35:20 India Standard Time 2021
;; MSG SIZE  rcvd: 55
```

B.2 Commands/tools used with the syntax:

1. **WHOIS** : GOOGLE.COM
2. **NSLOOKUP** : GOOGLE.COM
3. **TRACERT** : GOOGLE.COM
4. **DIG** : GOOGLE.COM

B.3 Question of Curiosity:

1. What information is grabbed from Whois?

Ans:

- When you register a domain name, ICANN requires that you provide personal details that include your name, address, phone number, etc. All of this information is automatically added to a publicly-available database that catalogues the owners of every domain name that is registered. This massive database of information is called Whois.
- A Whois record contains all of the contact information associated with the person, group, or company that registers a particular domain name. Typically, each Whois record will contain information such as the name and contact information of the Registrant (who owns the domain), the name and contact information of the registrar Registrar (the organization or commercial entity that registered the domain name), the registration dates, the name servers, the most recent update, and the expiration date. Whois records may also provide the administrative and technical contact information (which is often, but not always, the registrant).
- WHOIS information includes standard details such as your email address, telephone number, address, city and country. It also includes your registration, update, expiration date and name servers.

2. What information is grabbed from traceroute?

Ans:

- Traceroute is a command which can show you the path of a packet of information taken from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes.
- With Traceroute, we can
    1. Get the complete path that a packet uses to reach its destination.
    2. Discover the names and identity of routers and devices within the path.
    3. Find the time it took to send and receive data to each device on the path.

- ➔ Traceroute gives you complete information about the path that your data will take to reach its destination, without actually sending data (other than ICMP).
- ➔ For example, if the source of the path (your computer) is in Boston, Massachusetts and the destination in San Jose, California (a Server), Traceroute will identify the complete path, each hop (the computers, routers, or any devices that come in between the source and the destination) on the path, and the time it takes to go and come back.

3. What information is grabbed from a dig?

Ans:

- ➔ A command dig is a tool for querying DNS nameservers for information about host addresses, mail exchanges, nameservers, and related information. This tool can be used from any Linux (Unix) or Macintosh OS X operating system. The most typical use of dig is to simply query a single host.
- ➔ dig (domain information groper) is a network administration command-line tool for querying the Domain Name System (DNS).
- ➔ dig is useful for network troubleshooting and educational purposes. It can operate based on command-line option and flag arguments, or in batch mode by reading requests from an operating system file. When a specific name server is not specified in the command invocation, it uses the operating system's default resolver, it queries the DNS root zone.
- ➔ dig supports Internationalized domain name (IDN) queries.

4. After using traceroute how the attacker can use the information, based on the same what kind of attacks can be applied?

Ans:

- ➔ Help you find out where a communication breakdown has occurred.
- ➔ Tracing Anonymous Packets to Their Approximate Source.
- ➔ Without getting into vendor specifics, disable IP-directed broadcasts to all of your routers to keep your network healthy. Letting traceroute, ping, or any of the other ICMP messages into and through your network from the Internet is an invitation for network mapping, and it could lead to an attack.

B.4 Conclusion:

(Write an appropriate conclusion.)

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