**Name - Gaurang A Raorane Roll No - 49**

**Class - D15A Batch - C**

**CA EXPERIMENT 2**

**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

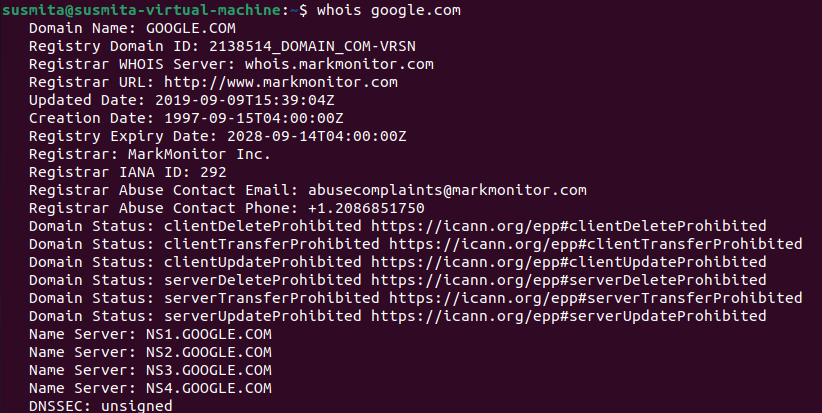
registered users of an Internet resource, such as a domain name or an IP address

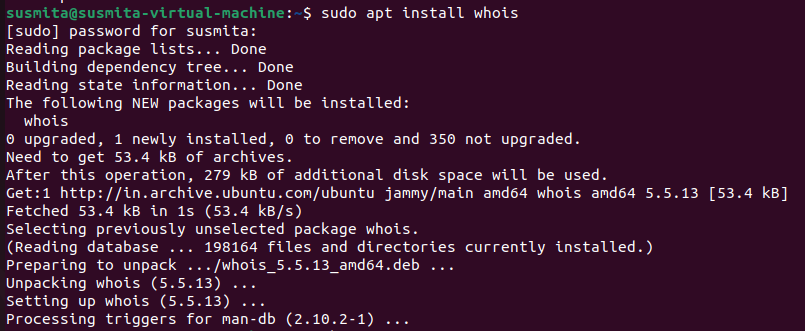
block, but is also used for a wider range of other information. Most modern

versions of whois try to guess the right server to ask for the specified object.

Examples:

* Obtaining the domain WHOIS record for computersolutions.com
* WHOIS record by IP querying
* Querying WHOIS in google search engine





2. **Dig (Domain Information Groper):**

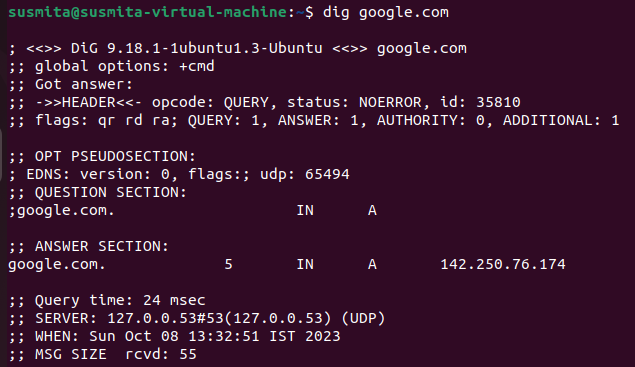
Dig is a networking tool that can query DNS servers for information. It

can be very helpful 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:

dig example.com



3. **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 TTL field, this field describes how much hops a particular

packet will take while traveling 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

when 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 the packet was generated. The ICMP packet that is sent back contains the IP

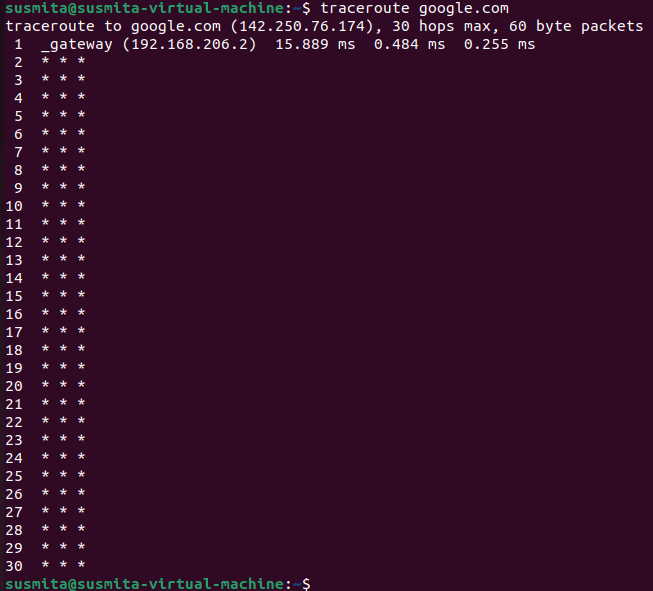
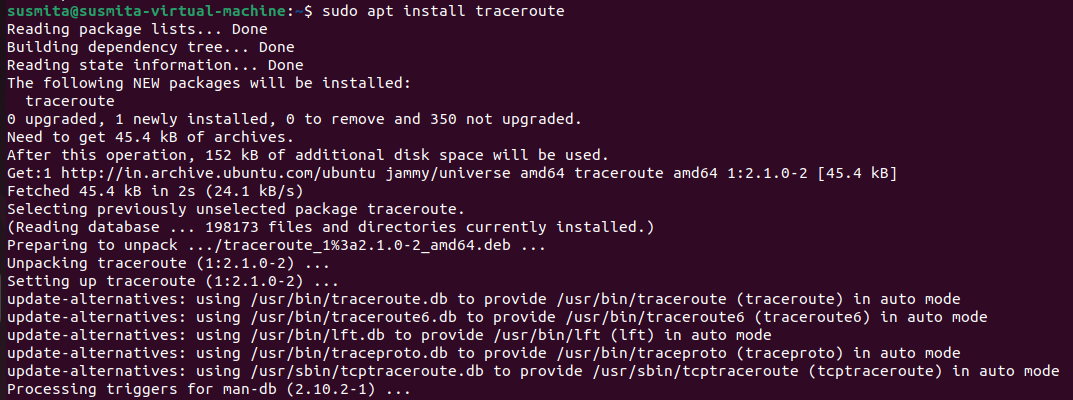
address of the router. So now it can be easily understood that traceroute operates

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.

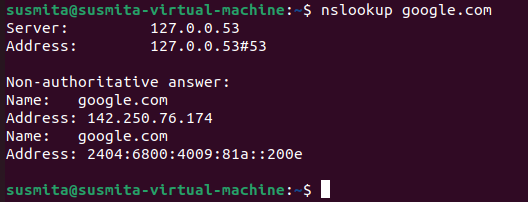
Example: traceroute example.com

4. **Nslookup (Name Server Lookup):**

The nslookup command is used to query internet name servers interactively for information. nslookup, which stands for "name server lookup", 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). For instance, to find out what the IP address of microsoft.com is, you could run the command:

nslookup microsoft.com

****

**Conclusion:**

Successfully studied the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks.