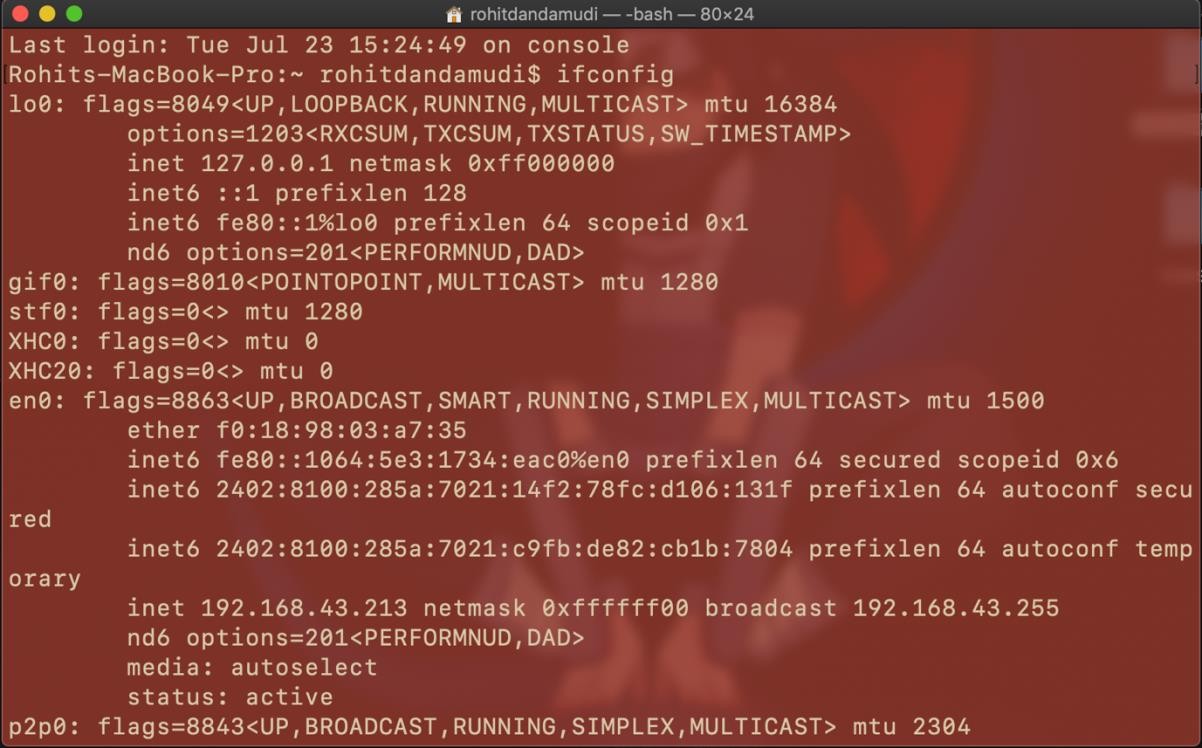
**EXPERIMENT-2:**

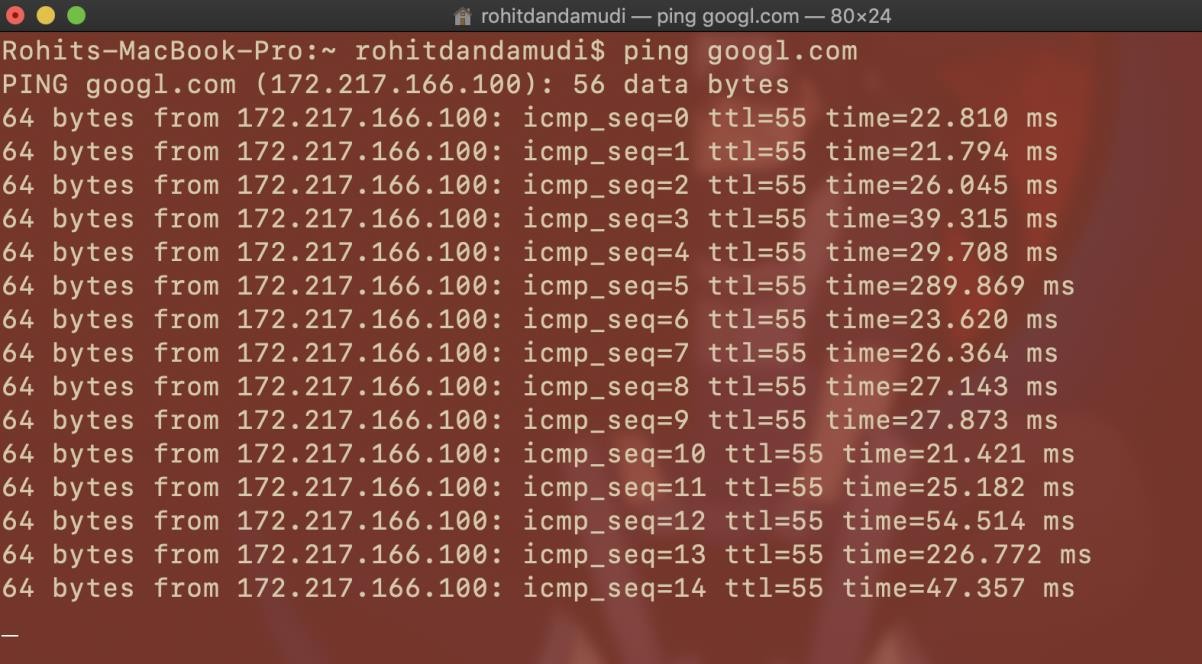
**Network commands and Configuration tools:**

1. Ifconfig(Interface configuration)

* Syntax: ifconfig
* ifconfig in short “interface configuration” utility for system/network administration in Unix/Linux operating systems to configure, manage and query network interface parameters via command line interface or in a system configuration scripts.
* The “ifconfig” command is used for displaying current network configuration information, setting up an ip address, netmask or broadcast address to an network interface, creating an alias for network interface, setting up hardware address and enable or disable network interface
* We can many options such as -a for all etc
* Enp1s0 tell ethernet port 1 and socket 0
* UP BROADCAST RUNNING MULTICAST etc are flags that describe the interfaces used



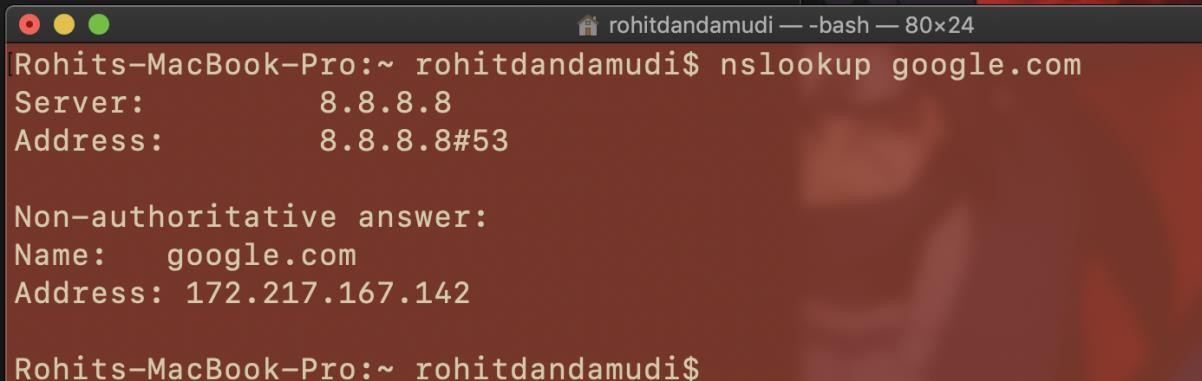
1. ping:

* Syntax: ping sitename
* The ping command is a command prompt command used to test the ability of the source computer to reach a specified destination computer. The ping command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.
* The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response. How many of those responses are returned, and how long it takes for them to return, are the two major pieces of information that the ping command provides.

1. Nslookup(name server lookup):

* Syntax: nslookup sitename

nslookup is a network administration command-line tool available in many computer operating systems for querying the Domain Name Server(DNS) to obtain domain name or IP address mapping, or other [DNS records](https://en.wikipedia.org/wiki/DNS_record). The name "nslookup" means "name server lookup".

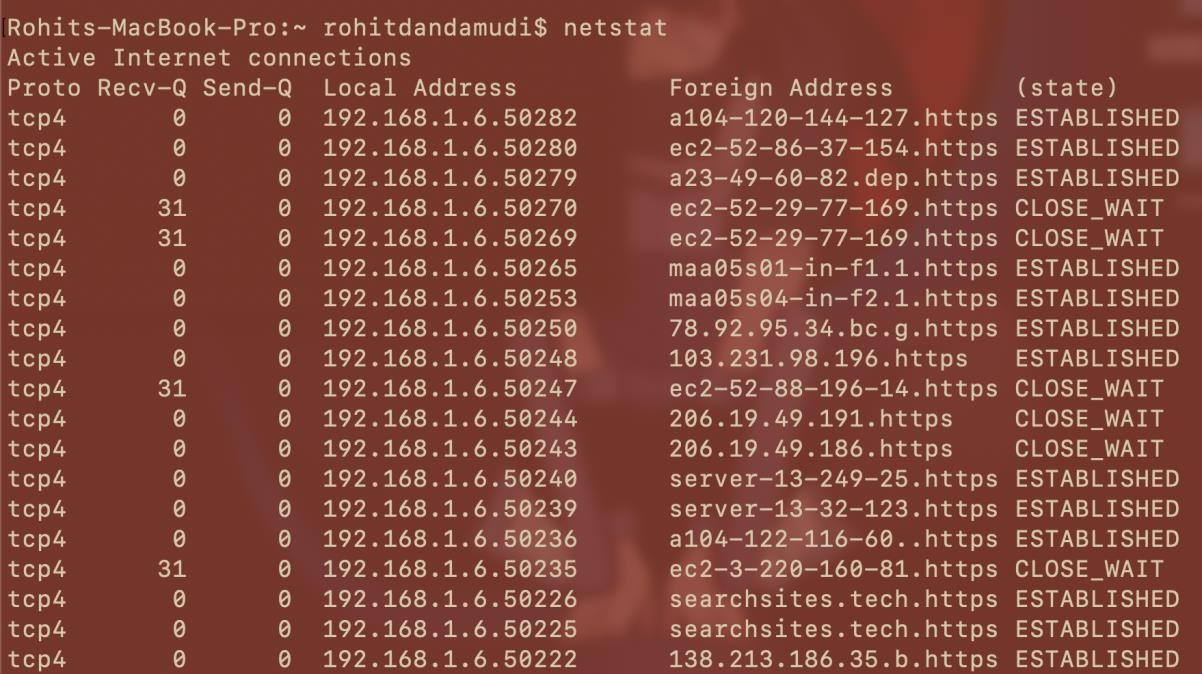


1. Netstat(network statistics):

Netstat is a common command line TCP/IP networking utility available in most other operating systems. Netstat provides information and statistics about protocols in use and current TCP/IP network connections. (The name derives from the

words *network* and *statistics*.)

NETSTAT -a -b -e -n -o -p proto -r -s -v interval



1. Nmap(Network Mapper):

* **Nmap** (*Network Mapper*) is a [free and open-source](https://en.wikipedia.org/wiki/Free_and_open-source_software) [network scanner](https://en.wikipedia.org/wiki/Network_scanner) created by Gordon Lyon (also known by his psuedonym *Fyodor Vaskovich*).[[3]](https://en.wikipedia.org/wiki/Nmap#cite_note-3)Nmap is used to

discover [hosts](https://en.wikipedia.org/wiki/Host_(network)) and [services](https://en.wikipedia.org/wiki/Web_service) on a [computer network](https://en.wikipedia.org/wiki/Computer_network) by sending [packets](https://en.wikipedia.org/wiki/Network_packet) and analyzing the responses.

* Nmap provides a number of features for probing computer networks, including host discovery and service and [operating system](https://en.wikipedia.org/wiki/Operating_system) detection. These features are extensible by [scripts](https://en.wikipedia.org/wiki/Scripting_language) that provide more advanced service detection,[[4]](https://en.wikipedia.org/wiki/Nmap#cite_note-Nmap_Scripting_Engine-4) vulnerability detection[,[4]](https://en.wikipedia.org/wiki/Nmap#cite_note-Nmap_Scripting_Engine-4) and other features. Nmap can adapt to network conditions

including [latency](https://en.wikipedia.org/wiki/Network_latency) and [congestion](https://en.wikipedia.org/wiki/Network_congestion) during a scan.

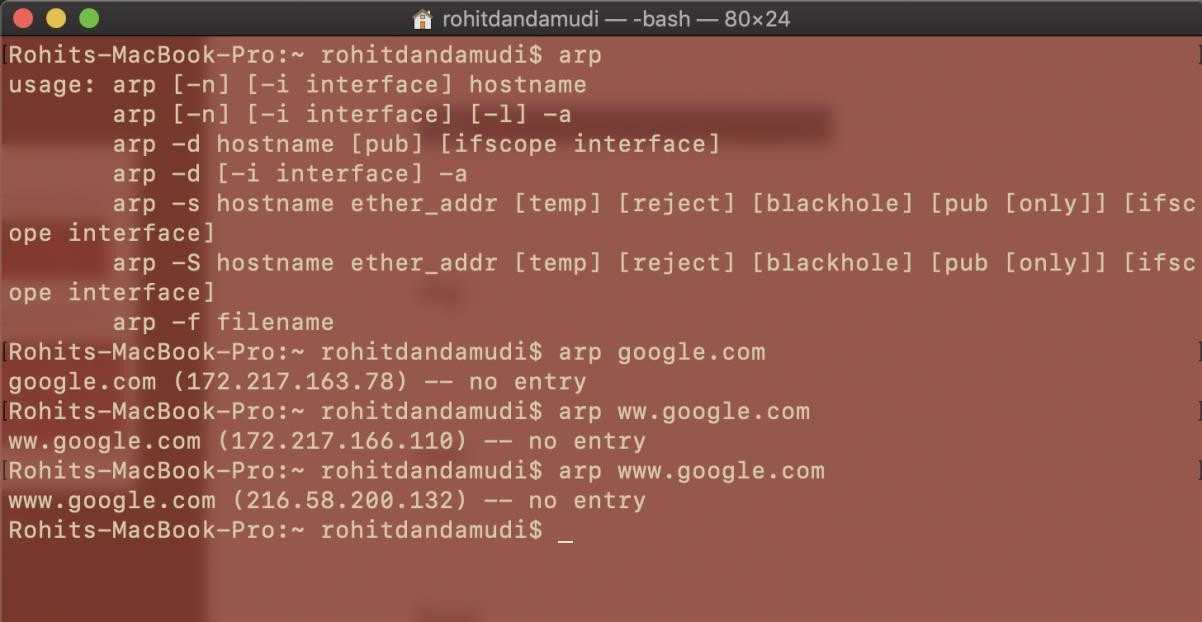
1. arp(Address Resolution Protocol):

* The address resolution protocol (arp) is a protocol used by the [Internet Protocol (IP)](https://erg.abdn.ac.uk/users/gorry/course/inet-pages/ip.html) [[RFC826],](https://erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html#Anchor-49575) specifically IPv4, to map [IP network addresses](https://erg.abdn.ac.uk/users/gorry/course/inet-pages/ip-address.html) to the hardware

addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer. It is used

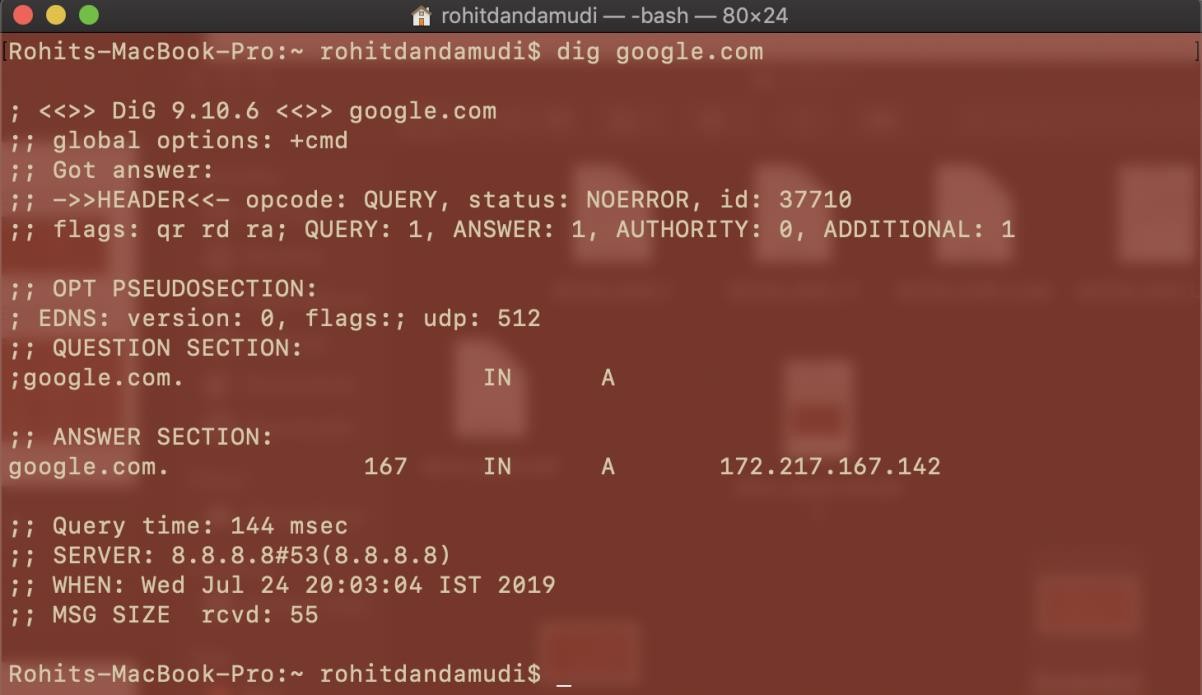
when [IPv4 is used over Ethernet.](https://erg.abdn.ac.uk/users/gorry/course/inet-pages/ip-enet.html)

* The term address resolution refers to the process of finding an address of a computer in a network. The address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address.



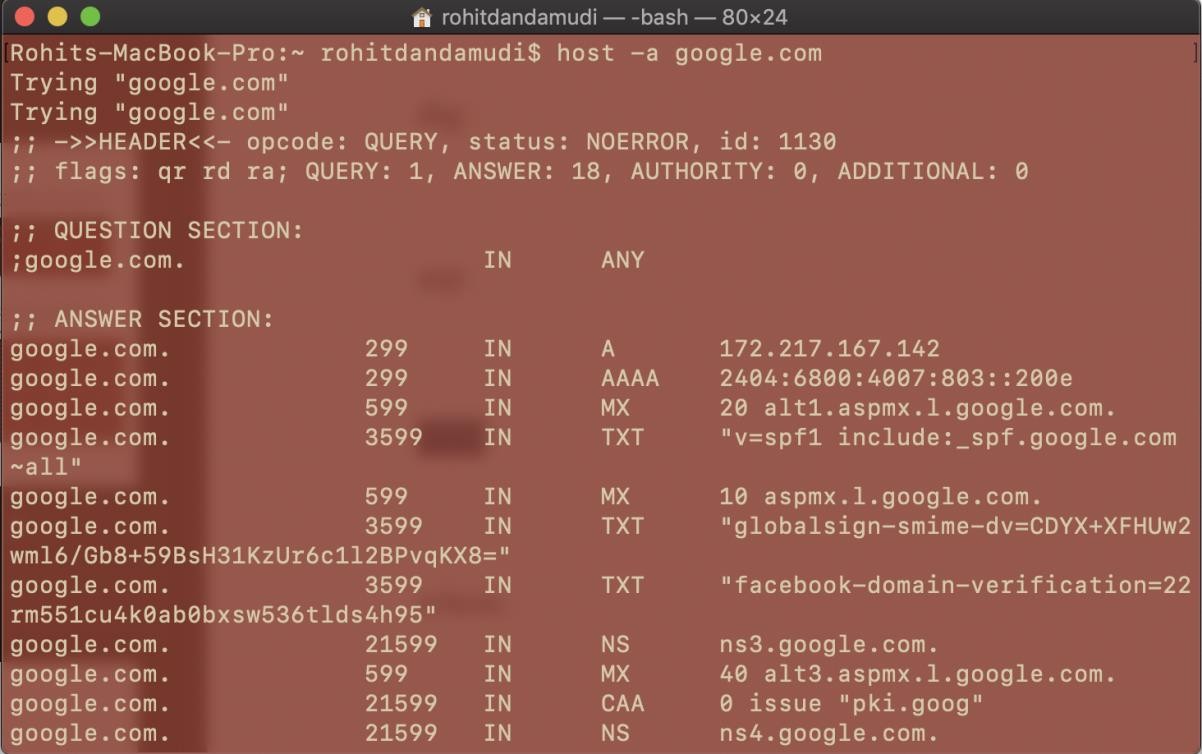
1. dig(domain information groper):

* Dig stands for (Domain Information Groper) is a network administration command- line tool for querying Domain Name System (DNS) name servers. It is useful for verifying and troubleshooting DNS problems and also to perform DNS lookups and displays the answers that are returned from the name server that were queried. dig is part of the BIND domain name server software suite. dig command replaces older tool such as nslookup and the host. dig tool is available in major Linux distributions.



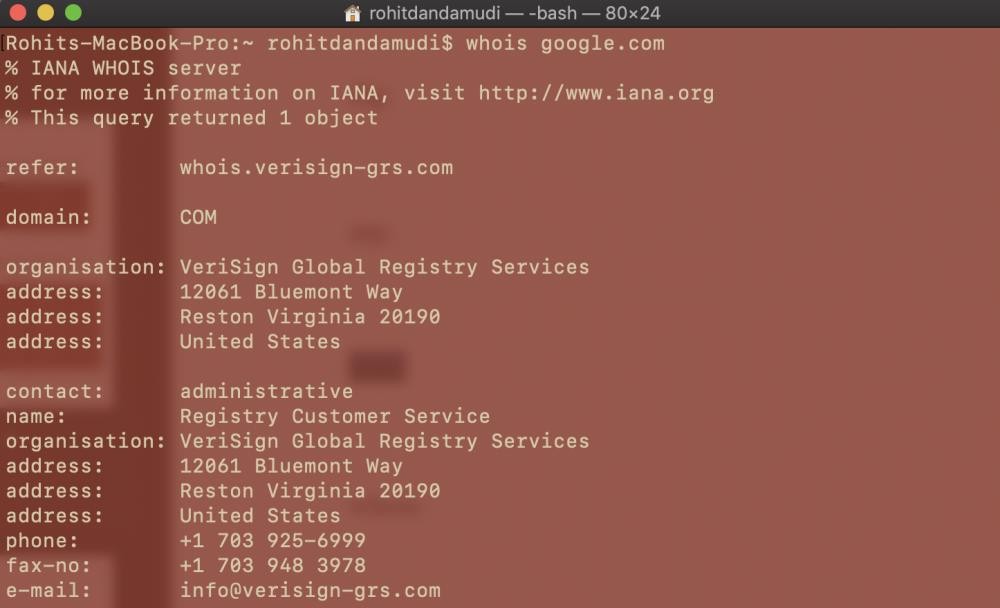
1. host:

* On unix-like operating systems, the **host** command is a DNSlookup utility, finding the IP address of a domain name. It also performs reverse lookups, finding the domain name associated with an IP address.
* host performs DNS lookups, converting domain names to IP addresses and vice versa. When no arguments or options are given, host prints a short summary of command line arguments and options.



1. whois:

* whois searches for an object in a WHOIS database. WHOIS is a [query](https://www.computerhope.com/jargon/q/query.htm)and response protocol that is widely used for querying [databases](https://www.computerhope.com/jargon/d/database.htm) that store the registered users of an Internet resource, such as a domain name or IP Address block, but is also used for a wider range of other information.



1. traceroute:

* A *traceroute* is a function which traces the path from one network to another. It allows us to diagnose the source of many problems.
* To be effective, the traceroute MUST be run during a time when you are experiencing the problem, from a computer that is experiencing the problem. A trace when you are able to connect, or one from another computer, is not helpful. Therefore, you should try to connect to your site again just before you run it. If the problem is no longer occurring, you will have to wait until the next time the problem occurs (if there is a next time) before running your traceroute.

