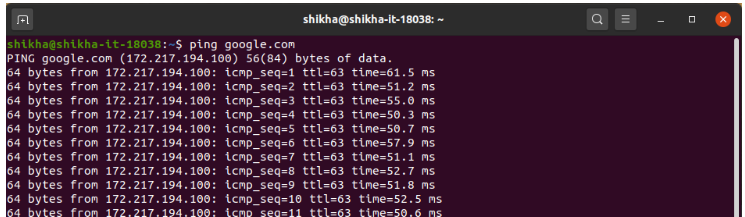
**Name:Farhana Afrin Shikha**

**ID:IT-18038**

**Linux Network Tools**

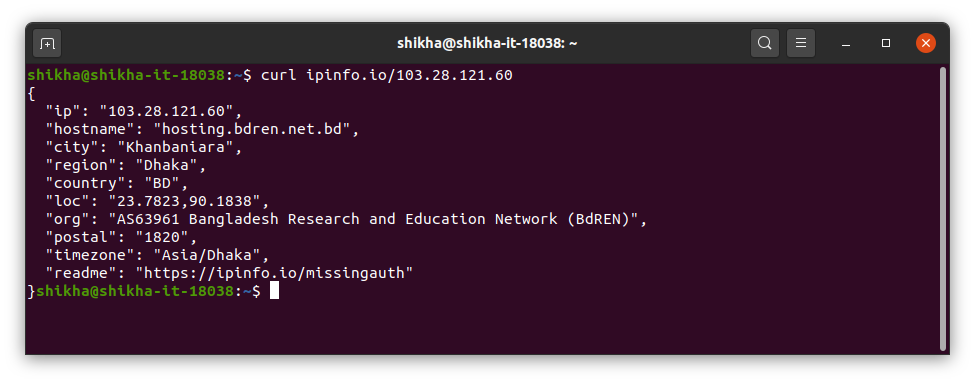
**ping :**

ping is a [computer network](https://en.wikipedia.org/wiki/Computer_network) administration [software utility](https://en.wikipedia.org/wiki/Utility_software) used to test the reachability of a [host](https://en.wikipedia.org/wiki/Host_(network)) on an [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP) network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software.Ping measures the [round-trip time](https://en.wikipedia.org/wiki/Round-trip_time) for messages sent from the originating host to a destination computer that are echoed back to the source. The name comes from [active sonar](https://en.wikipedia.org/wiki/Active_sonar) terminology that sends a [pulse](https://en.wikipedia.org/wiki/Pulse_(signal_processing)) of sound and listens for the echo to detect objects under water.



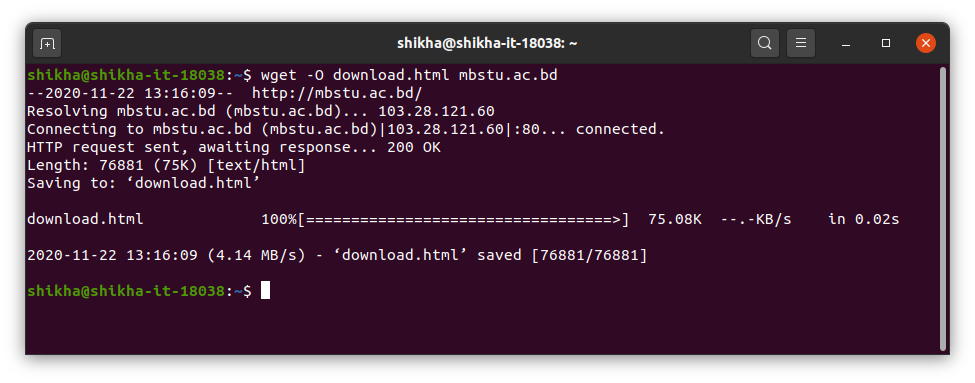
**curl**:

curl is an awesome tool that lets you create network requests from the command line. Published Oct 06, 2018. curl is a a command line tool that allows to transfer data across the network. It supports lots of protocols out of the box, including HTTP, HTTPS, FTP, FTPS, SFTP, IMAP, SMTP, POP3, and many more.



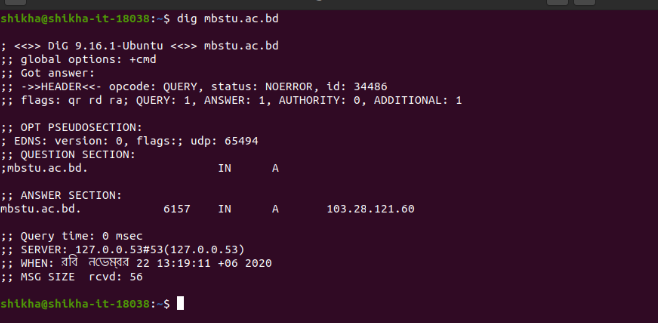
**wget:**

wget is the non-interactive network downloader which is used to download files from the server even when the user has not logged on to the system and it can work in the background without hindering the current process. ... wget is non-interactive, meaning that it can work in the background, while the user is not logged on.



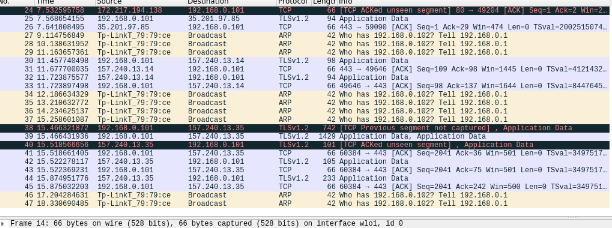
**dig:**

**dig** is a **network** administration command-line tool for querying the Domain Name System (DNS). **dig** is useful for **network** troubleshooting and for educational purposes. ... **dig** supports Internationalized domain name (IDN) queries. **dig** is a component of the domain name server software suite BIND.



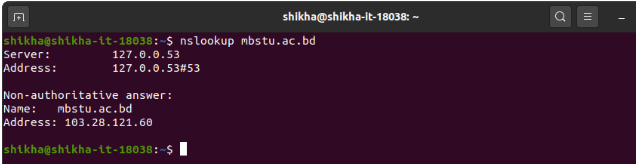
**wireShark:**

**Wireshark** is a free and open-source packet analyzer. ... **Wireshark** is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on **Linux**, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.

****

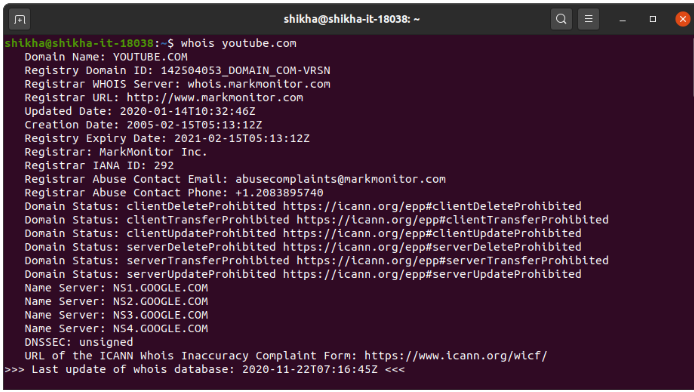
**nslookup**:

**nslookup** (from name server lookup) is a **network** administration command-line tool available in many **computer** operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping, or other DNS records.



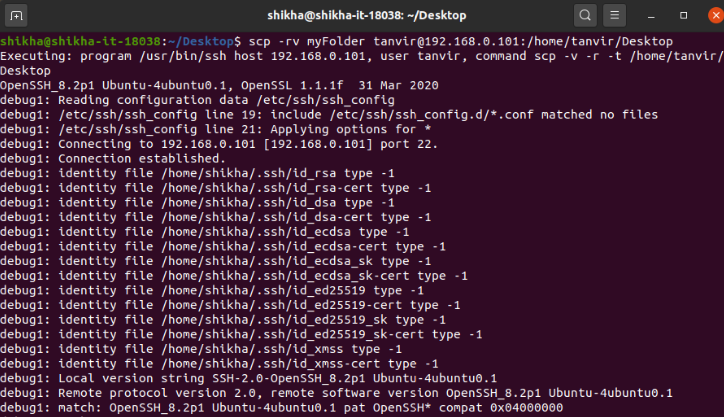
**whois:**

**whois** is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them. The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership.



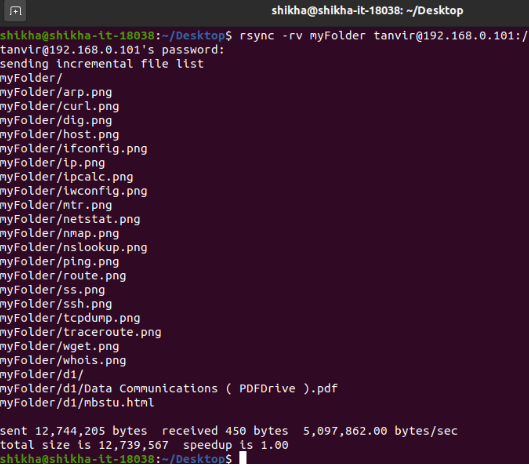
**scp:**

Secure copy protocol (**SCP**) is a means of securely transferring **computer** files between a local host and a remote host or between two remote hosts. It is based on the Secure Shell(SSH) protocol. "**SCP**" commonly refers to both the Secure Copy Protocol and the program itself.



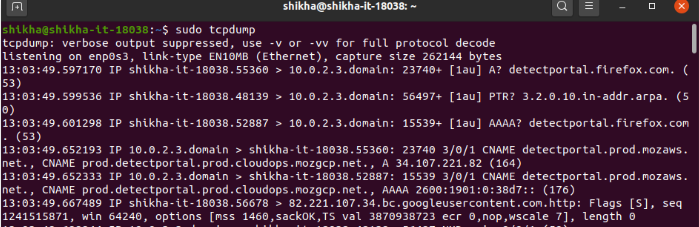
**rsync:**

**rsync** is a software tool used to either copy files locally, from one path/directory to another, or transfer them between a local **computer** and a remote one, through a **network** such as LAN (Local Area **Network**) or the Internet.



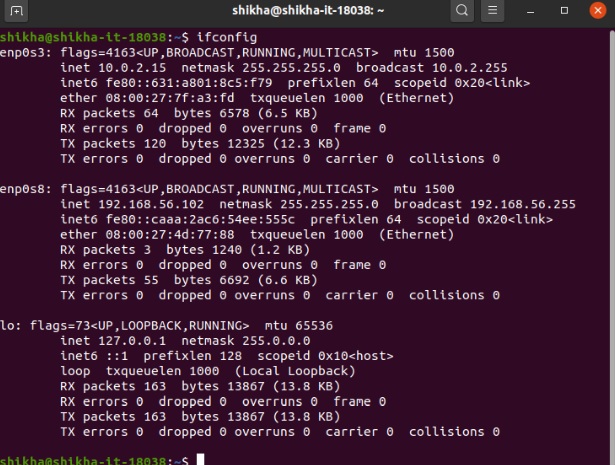
**tcpdump:**

**tcpdump** is a data-**network** packet analyzer **computer** program that runs under a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a **network** to which the **computer** is attached.



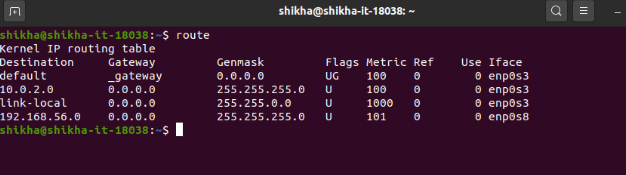
**ifconfig:**

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** interfaces



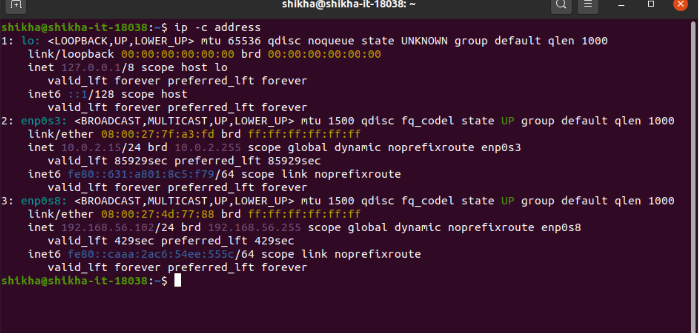
**route:**

**Routing** is the process of selecting a **path** for traffic in a **network** or between or across multiple **networks**. ... Packet forwarding is the transit of **network** packets from one **network** interface to another. Intermediate nodes are typically **network** hardware devices such as routers, gateways, firewalls, or switches.



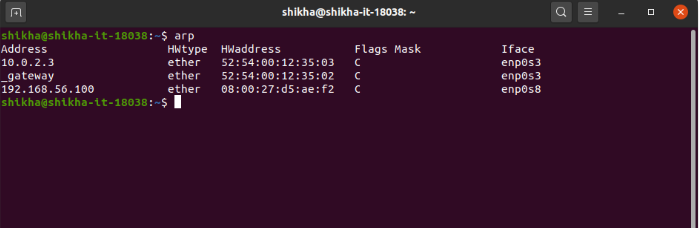
**ip:**

**IP** address stands for internet protocol address; it is an identifying number that is associated with a specific **computer** or **computer network**. When connected to the internet, the **IP** address allows the **computers** to send and receive information.



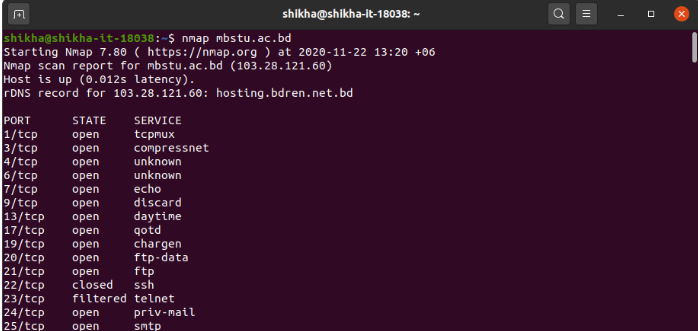
**arp**:

The Address Resolution Protocol (**ARP**) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite.



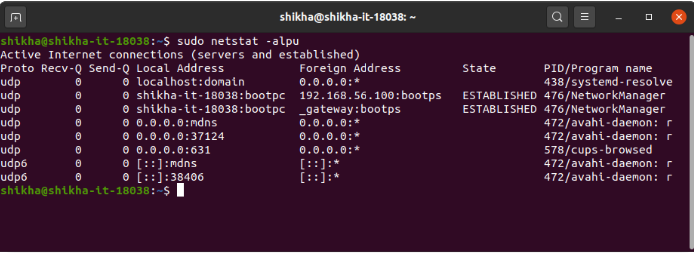
**nmap:**

**Nmap**, short for **Network** Mapper, is a free, open-source tool for vulnerability scanning and **network** discovery. **Network** administrators use **Nmap** to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.



**netstat**:

In **computing**, **netstat** (**network** statistics) is a command-line **network** utility that displays **network** connections for Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of **network** interface (**network** interface controller or software-defined **network** interface) and **network** protocol ...

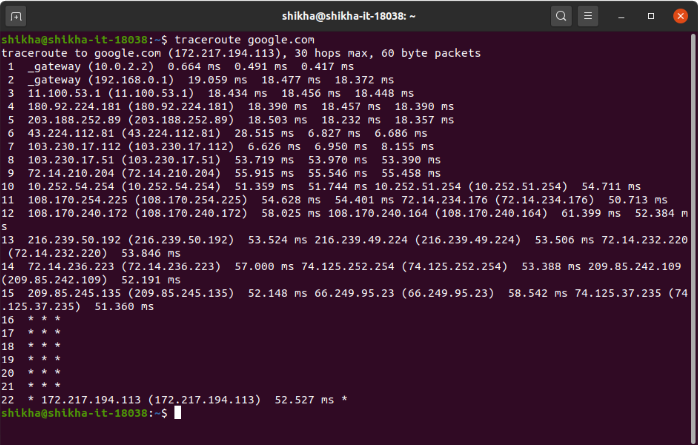


**ss:**

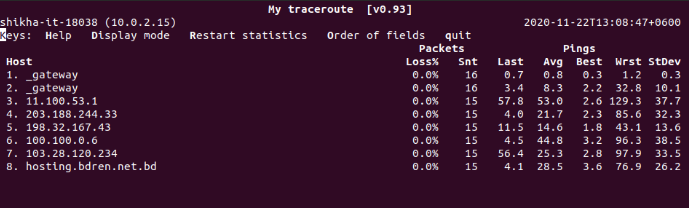


**traceroute:**

**Traceroute** is a **network** diagnostic tool used to track in real-time the pathway taken by a packet on an IP **network** from source to destination, reporting the IP addresses of all the routers it pinged in between. **Traceroute** also records the time taken for each hop the packet makes during its route to the destination.

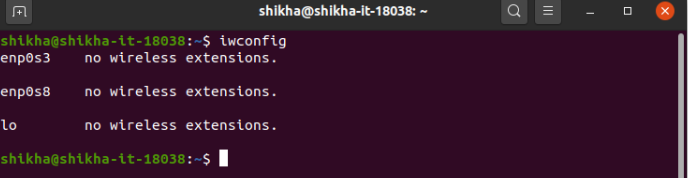


**mtr:**

My traceroute, originally named Matt's traceroute (**MTR**), is a **computer** program which combines the functions of the traceroute and ping programs in one **network** diagnostic tool. **MTR** probes routers on the route path by limiting the number of hops individual packets may traverse, and listening to responses of their expiry.

**iwconfig:**

**Iwconfig** is similar to ifconfig(8), but is dedicated to the wireless interfaces. It is used to set the parameters of the **network** interface which are specific to the wireless operation (for example : the frequency).



**ipcalc**:

**ipcalc** provides a simple way to calculate IP information for a host. The various options specify what information **ipcalc** should display on standard out. Multiple options may be specified. An IP address to operate on must always be specified. Most operations also require a netmask or a CIDR prefix as well.

