www.techiya.in
IGNOU BCA Solved Assignment 2020-21

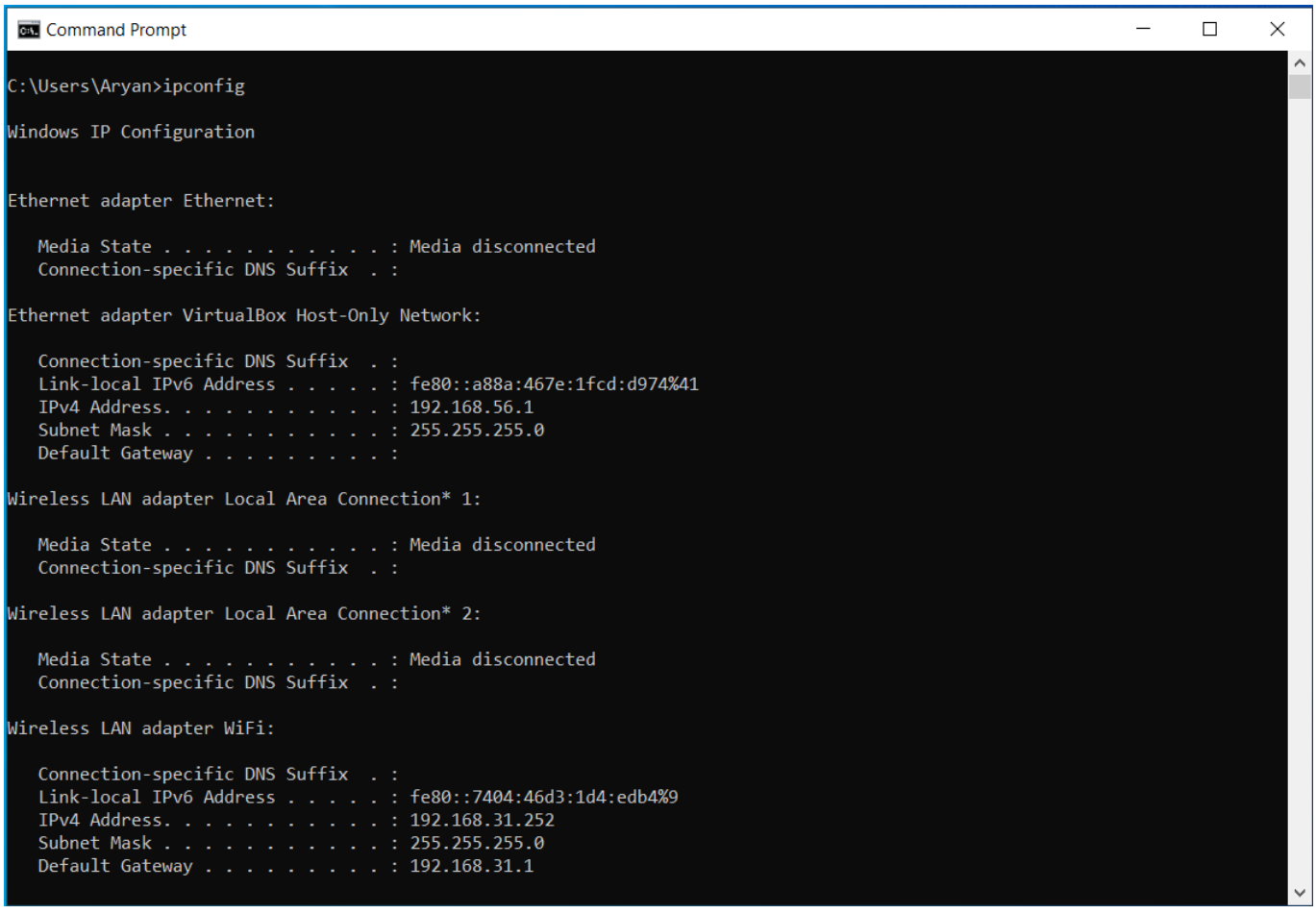
Course Code : BCSL-063

Course Title : Operating System Networking Management Lab

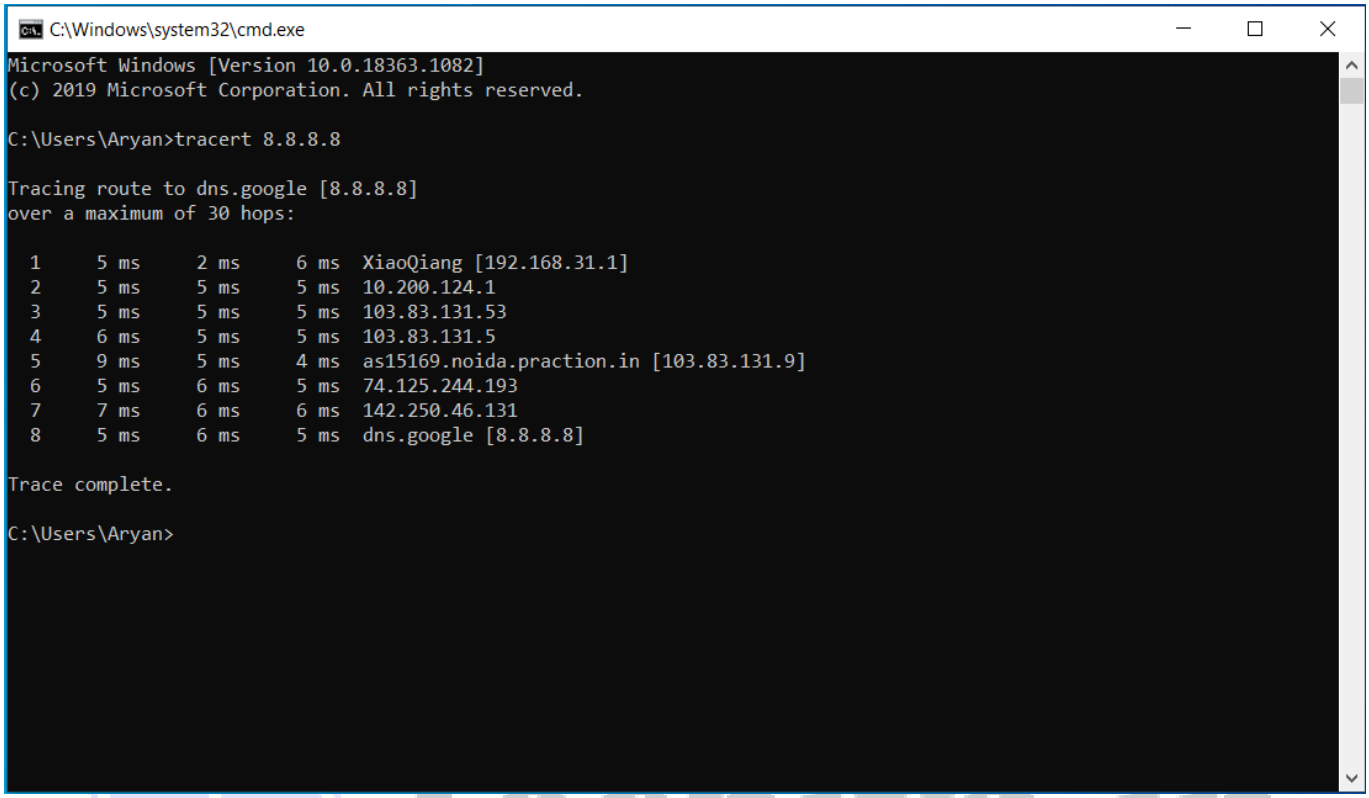
Assignment Number: BCA(6)/L-063/Assignment/2020-21

Q1. (a) Run the following commands and write/show output:

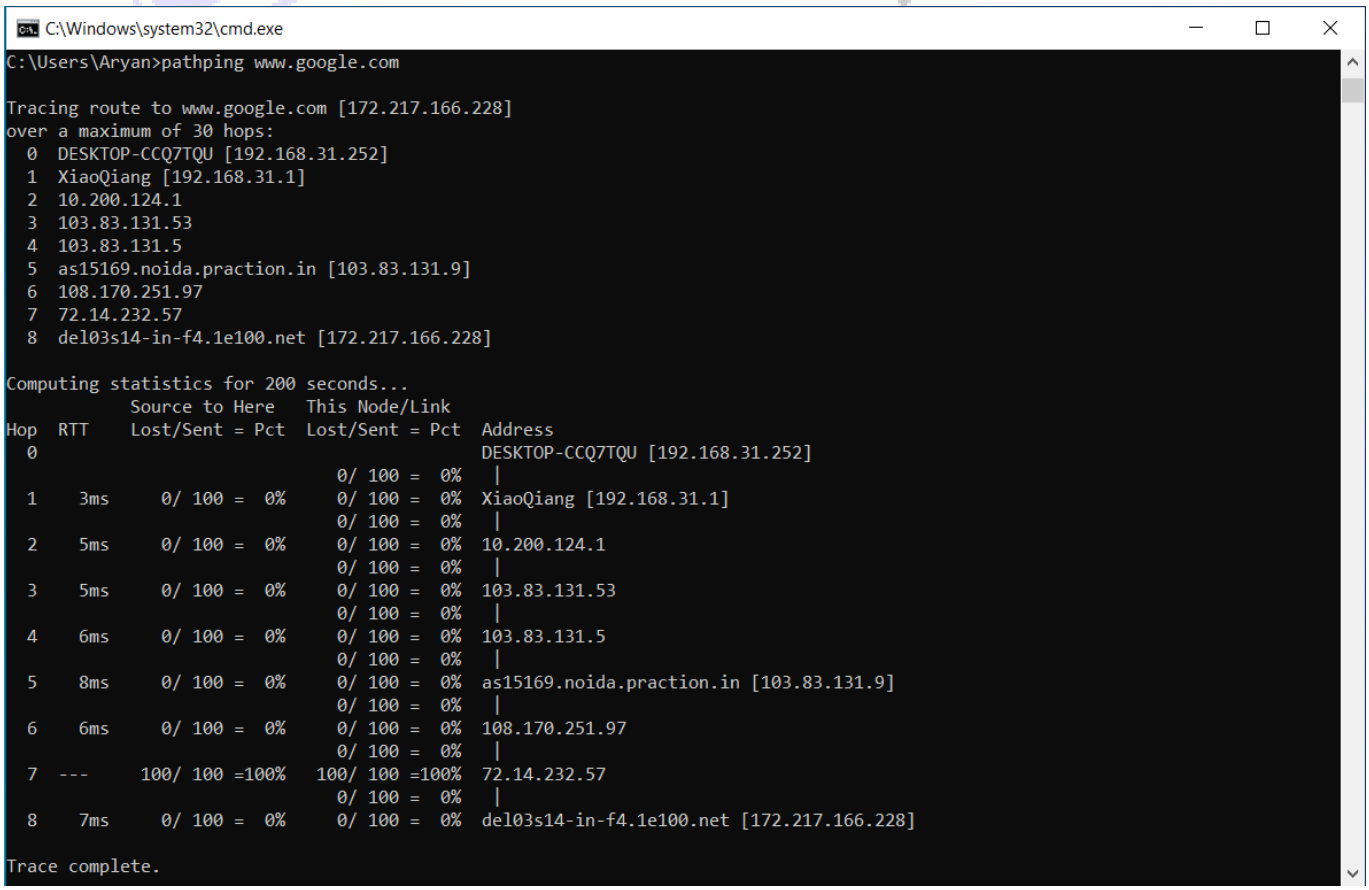
- **IPConfig**



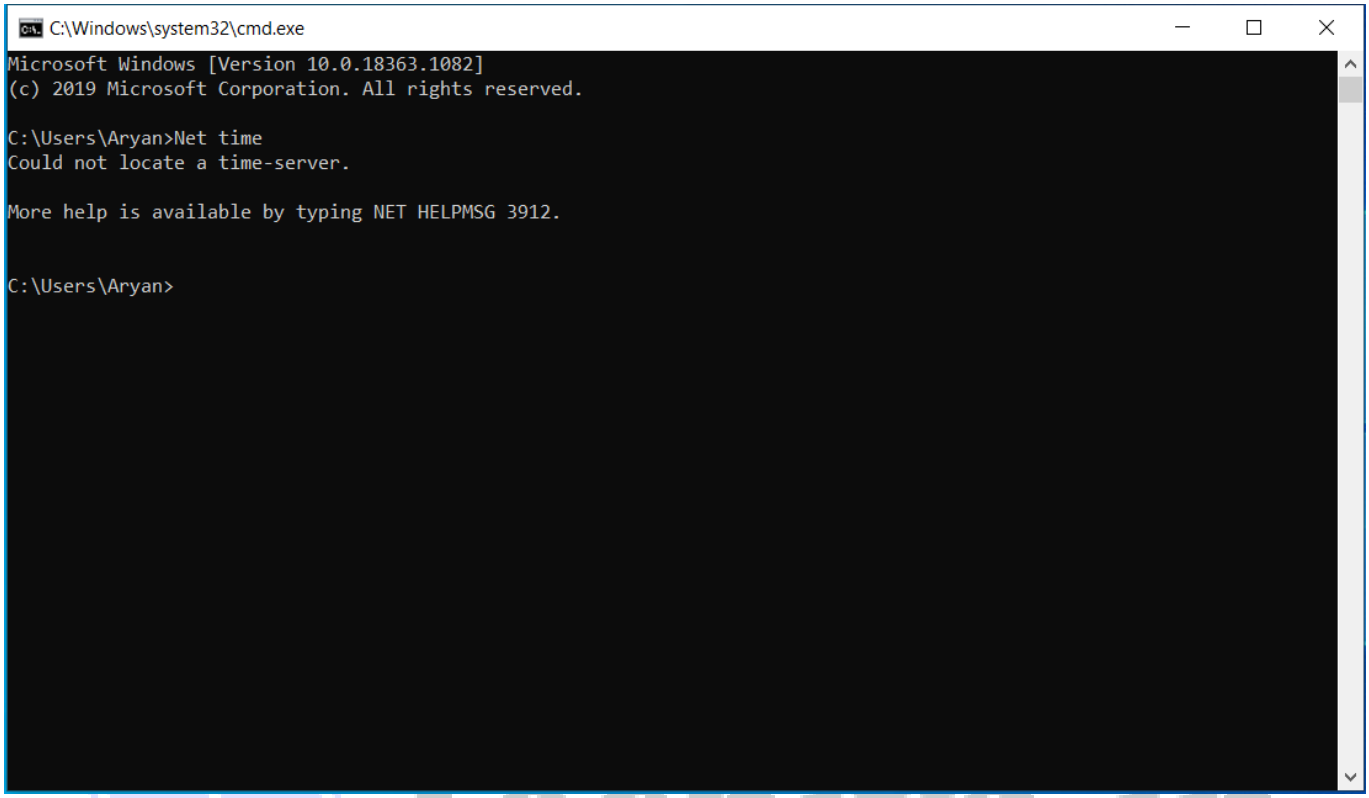
- **tracert**



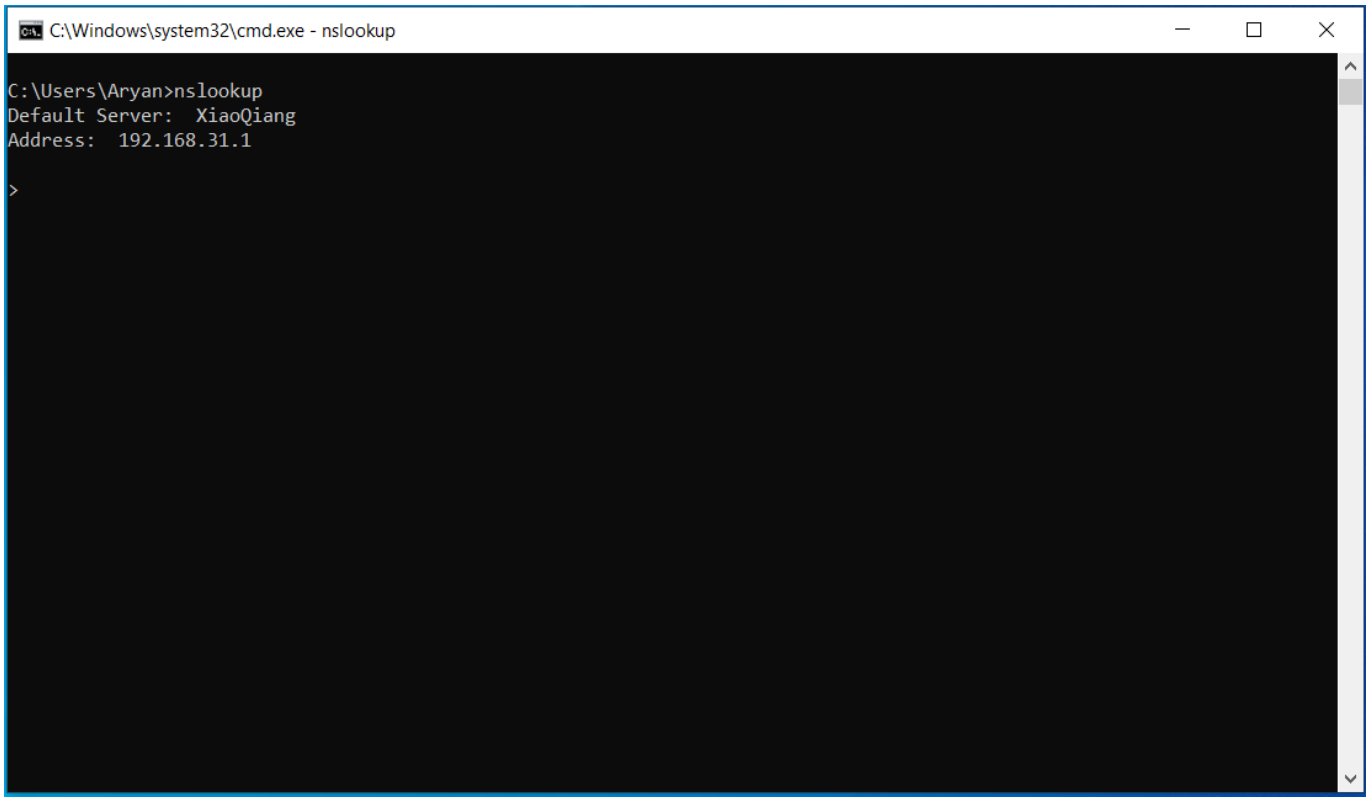
- **pathping**



- **nettime**



- **nslookup**



Q1. (b) Answer the following questions related to the above commands:

- **How is tracert command different from pathping in terms of the output information they produce? Explain**

Ans: The main difference between tracert and pathping is that tracert helps to find the actual path from the source to the destination device while pathping is a command that provides information about network latency and network loss at intermediate hops between the source and the destination devices.

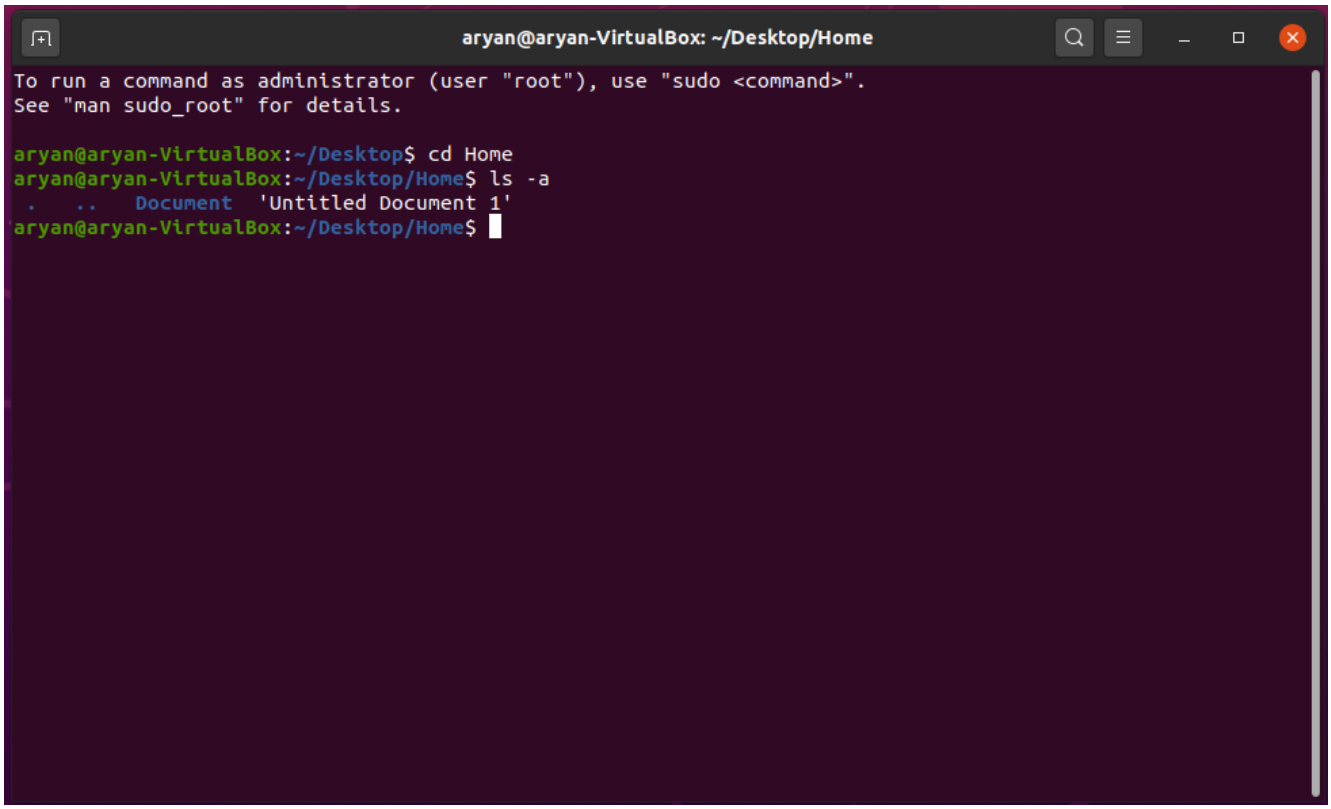
When there are issues in the network, they solve them by troubleshooting. In this, tracert and pathping are two utilities or commands to troubleshoot a network. Overall, pathping is a combination of the commands tracert and ping.

- **What is the output of Nslookup command? Explain**

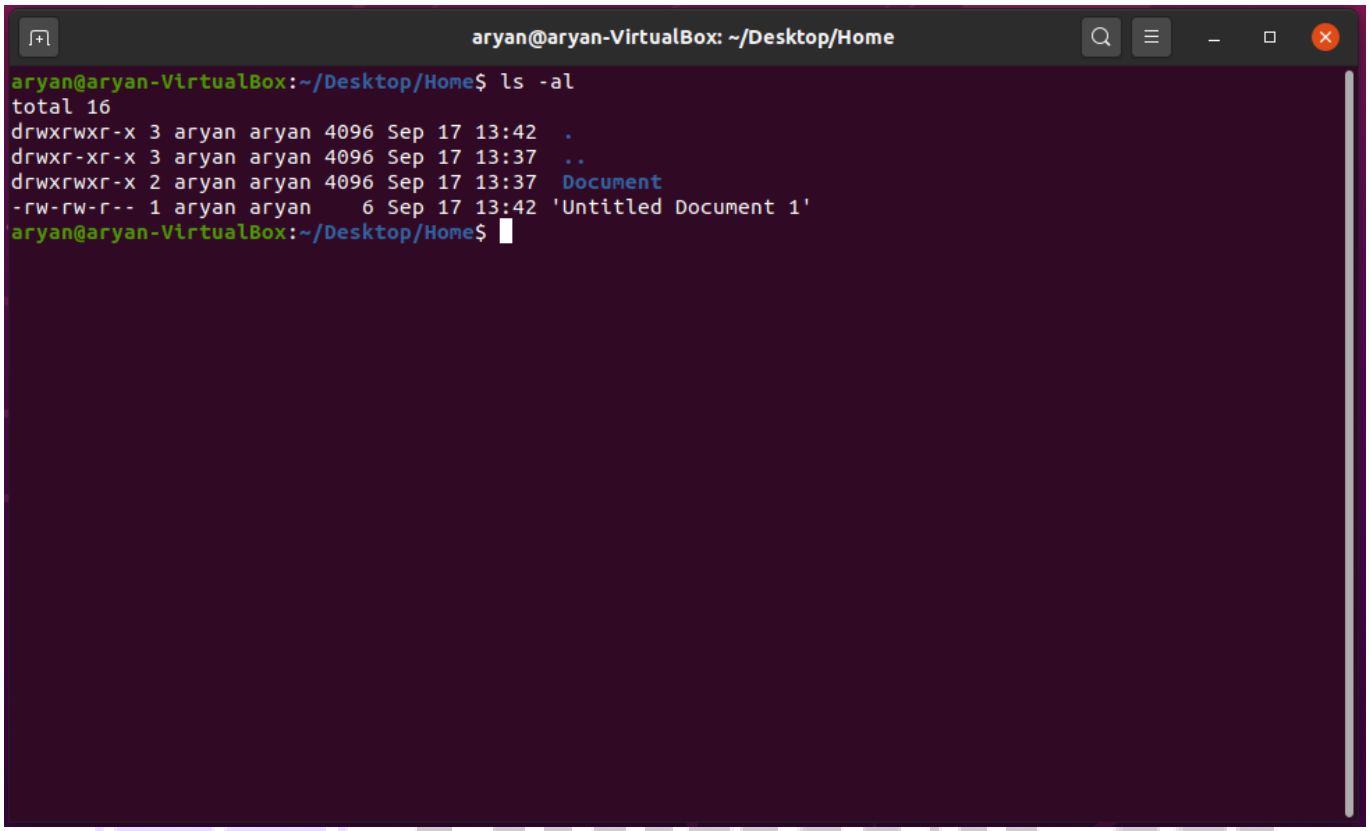
Ans: nslookup is a simple but very practical command-line tool, which is principally used to find the IP address that corresponds to a host, or the domain name that corresponds to an IP address (a process called “Reverse DNS Lookup”). nslookup allows itself to be used in the command-line of the operating system in question; Windows users start the service via the command prompt, and Unix users via the terminal window. Additionally, there are now a number of services that make it possible to use nslookup online.

Q1. (c) Answer the following questions:

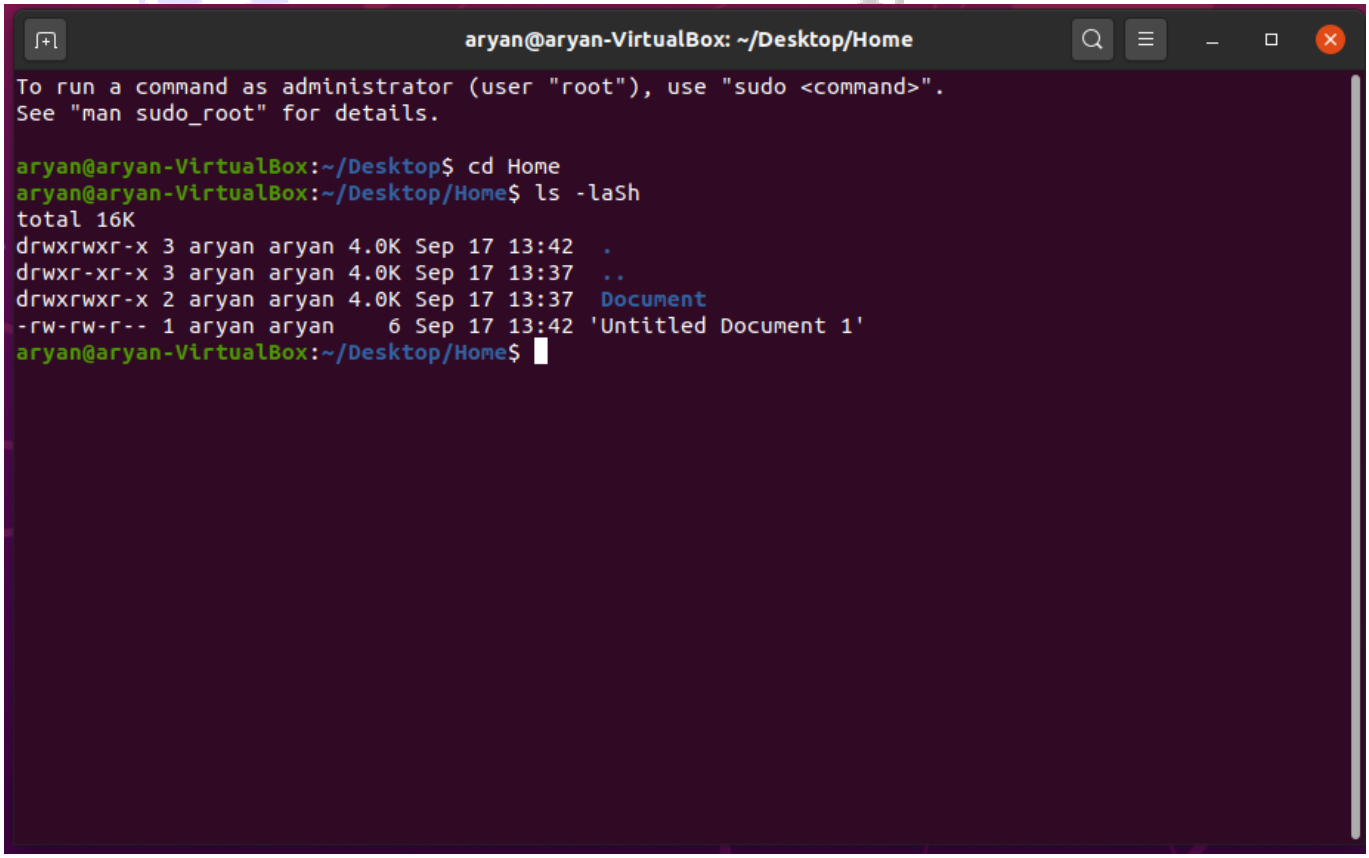
- **List all the files within a directory including hidden files**



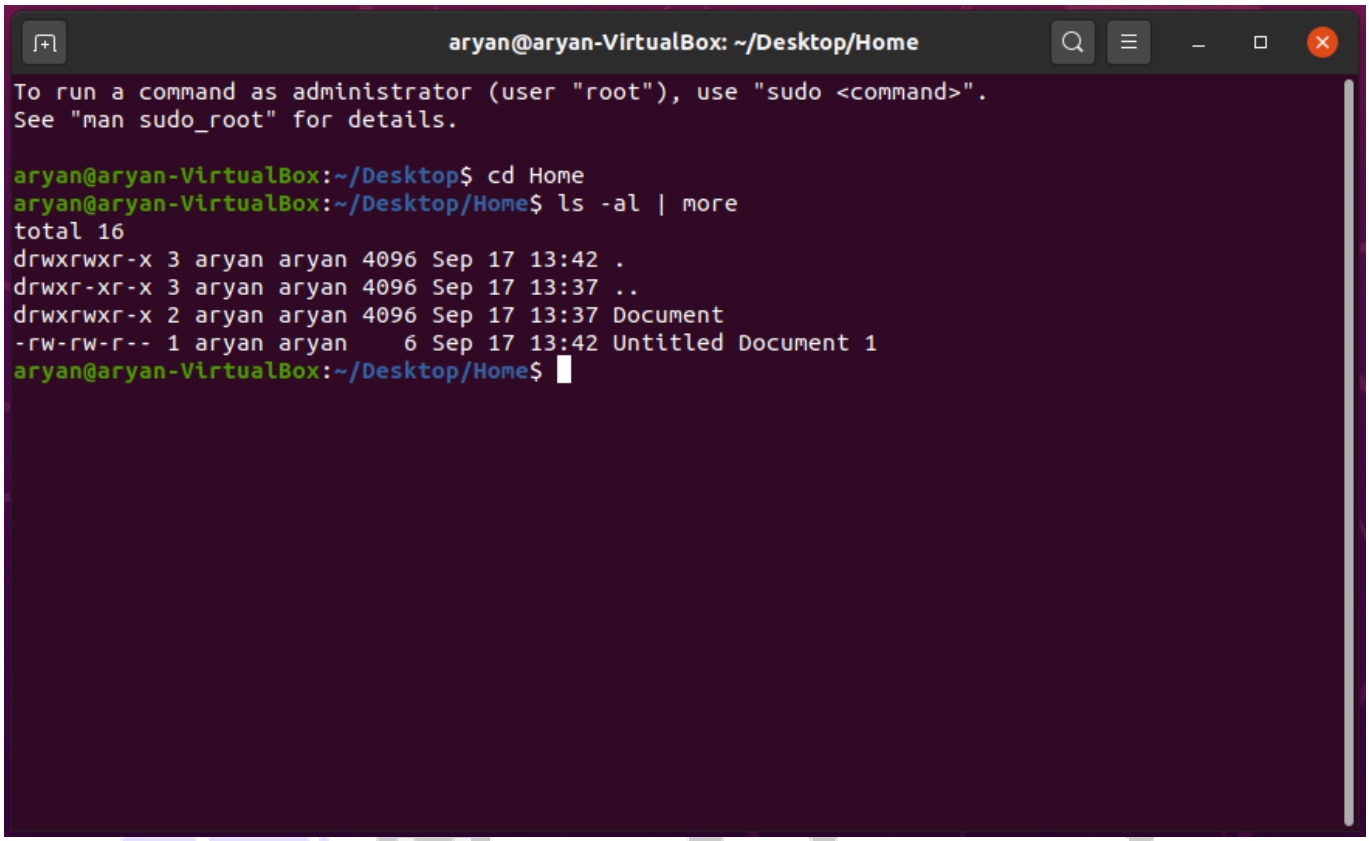
- **Which command is used to show files or directory, size, modified date and time, file permission, etc?**



- **Sort file or directory by file size**



- **What is the output of: ls-al | more?**



- **How to kill a process?**

Ans: Step 1: View Running Linux Processes

The top command is the easiest way to get a complete overview of the processes currently being run.

To view a list of all currently running processes, use the command:

Step 2: Locate the Process to Kill

Before you can kill a process, you need to find it. There are multiple ways you can search for a process in Linux. Processes can either be located by a process name (or a partial process name) or a process ID (also known as a “pid”).

Locate a Process with ps Command

The ps command displays similar information to top, though it will not be in the form of an interface. Instead, the ps command provides a complete listing of running processes, formatted based on the tags you add.

Step 3: Use Kill Command Options to Terminate a Process

killall Command

The killall command is used to kill processes by name. By default, it will send a SIGTERM signal. The killall command can kill multiple processes with a single command.

Q2. (a) Write a shell script to perform the following tasks:

- **(i) check to see if the file "my_file" exists**
- **(ii) display file "my_file passwords are enabled" if it exists.**
- **(iii) check the permission to write to the file "my_file"**
- **(iv) display " permissions to edit " my_file", if yes,**
- **(v) otherwise display " No permissions to edit " my_file"**

Ans:

```
#!/bin/bash
FILE="/home/aryan/Assignment/my_file"
If [ -e "$FILE"]
then
        echo "$my_file passwords are enabled"
fi
if [ -x "$FILE"]
then
        echo "You have permission to execute $FILE"
else
        echo "You do not have permission to execute $FILE"
fi
```


Output:

```
$./script.sh
/home/aryan/Assignment/my_file passwords are enabled
You do not have permission to execute /home/aryan/Assignment/my_file
```

Q2. (b) (i) write a shell script that prompts the user for a name of a file or directory and reports what type of this file is : regular file, a directory, or another type of file.

Ans:

checkfile.sh
~/Desktop

```
#!/bin/bash

echo "Enter the file path"
read FILE

if [ -f "$FILE" ]
        then
           echo "$FILE is a regular file"

elif [ -d "$FILE" ]
        then
           echo "$FILE is a directory"

else
   echo "FILE is another type of file"

fi

ls -l $FILE
```

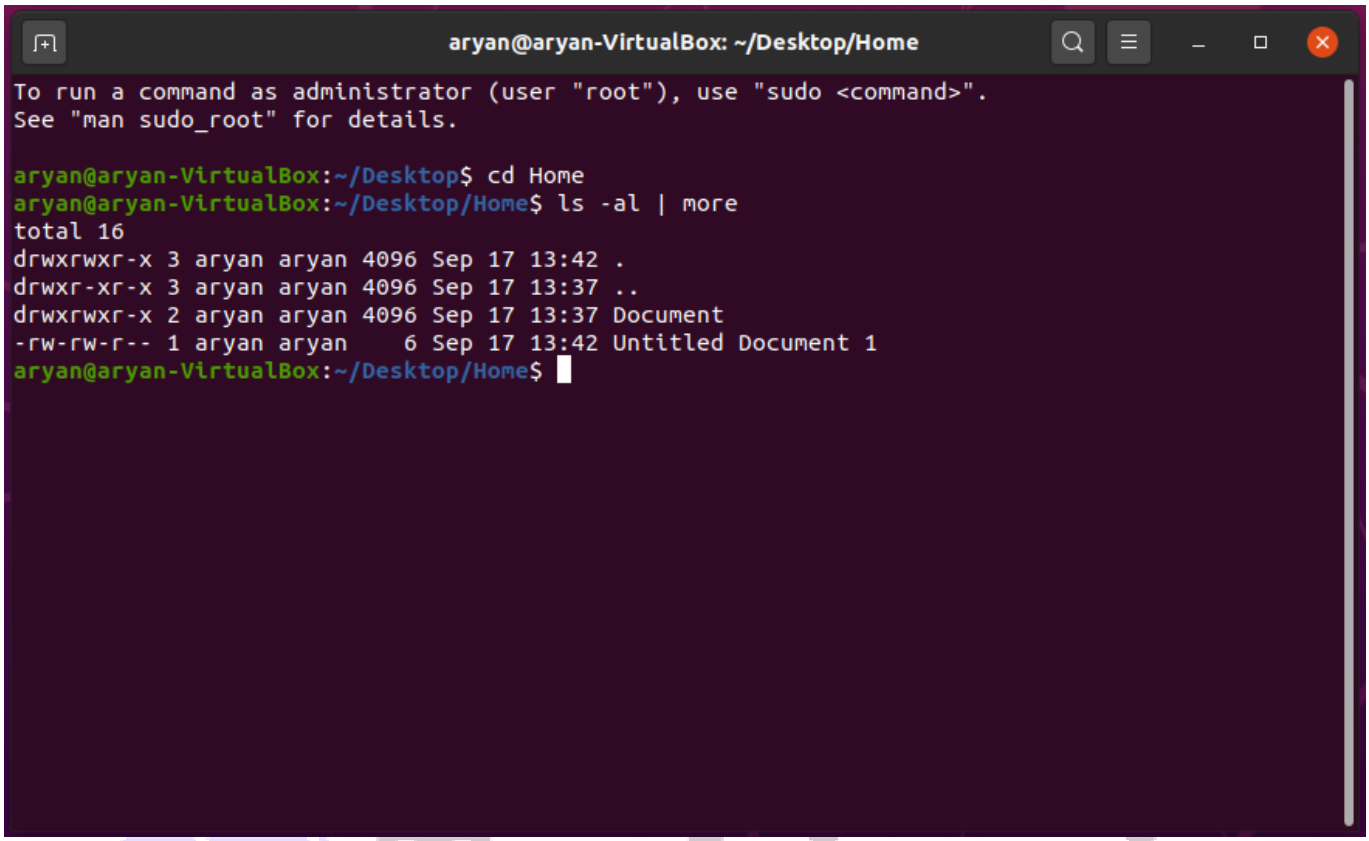
sh Tab Width: 8 Ln 21, Col 1 INS

Q2. (b) (ii) Execute an ls command against the file or directory with any two options you are aware of.

Ans: ls –a


```
aryan@aryan-VirtualBox: ~/Desktop
aryan@aryan-VirtualBox:~/Desktop$ ls -a
.  ..  checkfile.sh  Home
aryan@aryan-VirtualBox:~/Desktop$
```

ls –al



Q3. Perform the following tasks and write the procedures:

- **Configure VPN client as a VPN client**

Steps

Prerequisites

Step 1: Generate server and client certificates and keys

Step 2: Create a Client VPN endpoint

Step 3: Enable VPN connectivity for clients

Step 4: Authorize clients to access a network

Step 5: (Optional) Enable access to additional networks

Step 6: Download the Client VPN endpoint configuration file

Step 7: Connect to the Client VPN endpoint

Prerequisites

To complete this getting started tutorial, you need the following:

• The permissions required to work with Client VPN endpoints.

• A VPC with at least one subnet and an internet gateway. The route table that's associated with your subnet must have a route to the internet gateway.

Step 1: Generate server and client certificates and keys This tutorial uses mutual authentication. With mutual authentication, Client VPN uses certificates to perform authentication between the client and the server.

Step 2: Create a Client VPN endpoint When you create a Client VPN endpoint, you create the VPN construct to which clients can connect in order to establish a VPN connection.

Step 3: Enable VPN connectivity for clients To enable clients to establish a VPN session, you must associate a target network with the Client VPN endpoint. A target network is a subnet in a VPC.

Step 4: Authorize clients to access a network To authorize clients to access the VPC in which the associated subnet Is located, you must create an authorization rule. The authorization rule specifies which clients have access to the VPC. In this tutorial, you grant access to all users.

Step 5: (Optional) Enable access to additional networks

You can enable access to additional networks connected to the VPC, such as AWS services, peered VPCs, and on-premises networks. For each additional network, you must add a route to the network and configure an authorization rule to give clients access.

Step 6: Download the Client VPN endpoint configuration file

The final step is to download and prepare the Client VPN endpoint configuration file. The configuration file includes the Client VPN endpoint and certificate information required to establish a VPN connection. You must provide this file to the clients who need to connect to the Client VPN endpoint to establish a VPN connection. The client uploads this file into their VPN client application.

Step 7: Connect to the Client VPN endpoint

You can connect to the Client VPN endpoint using the AWS-provided client or another OpenVPN-based client application.

- **Set your printer on sharing and assign print permission according to different users, configuring printer priority for different groups**

When a printer is installed on a network, default printer permissions are assigned that allow all users to print, and allow select groups to manage the printer, the documents sent to it, or both. Because the printer is available to all users on the network, you might want to limit access for some users by assigning specific printer permissions. For

example, you could give all non-administrative users in a department the Print permission and give all managers the Print and Manage Documents permissions. In this way, all users and managers can print documents, but managers can also change the print status of any document sent to the printer. Windows provides three levels of printing security permissions: Print, Manage Printers, and Manage Documents. When multiple permissions are assigned to a group of users, the least restrictive permissions apply. However, when Deny is applied, it takes precedence over any permission. The following is a brief explanation of the types of tasks a user can perform at each permission level.

Printing permissions assigned to groups:

Windows assigns printer permissions to six groups of users. These groups include Administrators, Creator Owner, Everyone, Power Users, Print Operators, and Server Operators. By default, each group is assigned a combination of the Print, Manage Documents, and Manage Printers permissions as shown in the following table.

Group	Print	Manage Documents	Manage Printers
Administrators	X	X	X
Creator Owner		X	
Everyone	X		
Power User	X	X	X
Print Operators	X	X	X
Server Operators	X	X	X

The Print Operators and Server Operators groups are located only on domain controllers. Members of this group can manage, create, share, and delete printers and print queues. Members of this group can load and unload device drivers on the server. Users who can load and unload device drivers also have the ability to load malicious code on the server. As a security best practice, only add trusted users to this group. Each permission consists of a group of special rights that allow the user to perform specific tasks. The following table summarizes the level of access associated with each of the printing security permissions.

Task Permitted	Print	Manage Documents(Applies to Document only)	Manage printers
Print	X		X
Manage Printers			X
Manage Documents		X	
Read Permission	X	X	X
Change Permission		X	X

Take Ownership		X	X

- **How will you access your account available at a remote machine? Download some files from that machine to your machine**

Even if you conscientiously save your data to the cloud, there always comes a time when you're away from your home or office and need to edit a file that's stuck on that computer. Or you'll be sitting in a hotel room and have to run a program on your home PC. Maybe you're out and about and want to run a desktop app on your phone. That's where remote desktop tools come in. Once configured, these programs allow you to securely connect to a computer from another device. You'll be able to fully control your computer from any location, and it'll almost be like actually sitting down to the real machine from afar. Just a decade ago, you'd need a degree in computing to wrap your head around the ins and outs of remote desktop programs. Now, as we'll demonstrate, you can manage these tools with just a few clicks or taps.

Third-party tools: Google Chrome and TeamViewer

While Apple and Microsoft offer pricy remote tools aimed at IT professionals, anyone can use the free remote-access option Google built into Chrome. You gain access through your Google account, and the tool employs the same syncing technology that keeps your passwords and login information available in Chrome on multiple platforms. You can get Google's remote tool for your browser, as an Android app, and even for iOS and iPadOS devices.

Free and easy option is TeamViewer, though business use requires a paid license First, download the app onto the computer you'll want to connect to. Then open it and choose the option marked Installation to access this computer remotely (the other option is for accessing the computer while somebody else is using it). TeamViewer will guide you through the process of setting your computer up for unattended access, which basically involves giving it a name and a password. Your linked computers connect to each other through a TeamViewer account, which is free to set up and lets you see your devices wherever you sign in. Next, install TeamViewer on the devices you want to connect from. This time, you'll want to connect rather than set up unattended access. As soon as you sign in with the credentials you just created, the original computer should appear. You can connect by entering the password you've already set up. Along the top of the connection window, you'll see all the controls you're going to need, including options for transferring files between computers and setting the screen resolution and quality. You're essentially live streaming your desktop, so reducing the quality a little might lead to a smoother experience.