



20MCA136 - NETWORKING & SYSTEM ADMINISTRATION LAB

RECORD



K M ABHIJITH
S2-REG-MCA-B
ROLL NO :05

TABLE OF CONTENTS

EXP NO	EXPERIMENT	PAGE NO
1	BASIC LINUX COMMANDS	3
2	NETWORK COMMANDS	32
3	LAMP INSTALATION	50
4	ANSIBLE INSTALLATION	57
5	TCPDUMP	58
6	SHELL SCRIPTING	63
7	DOCKER INSTALLATION	76
8	WIRESHARK INSTALLATION	82

BASIC LINUX COMMANDS

1. `pwd` — When you first open the terminal, you are in the home directory of your user. To know which directory you are in, you can use the “**pwd**” command. It gives us the absolute path, which means the path that starts from the root. The root is the base of the Linux file system. It is denoted by a forward slash(/). The user directory is usually something like “/home/username”.

2. `ls` — Use the “**ls**” command to know what files are in the directory you are in. You can see all the hidden files by using the command “**ls -a**”.

3. `cd` — Use the “**cd**” command to go to a directory.

4. `mkdir & rmdir` — Use the **mkdir** command when you need to create a folder or a directory. Use **rmdir** to delete a directory. But **rmdir** can only be used to delete an empty directory. To delete a directory containing files, use **rm**.

5. `rm` - Use the **rm** command to delete files and directories

6. `touch` — The **touch** command is used to create a file. It can be anything, from an empty txt file to an empty zip file

7. Use the `cat` command to display the contents of a file. It is usually used to easily view programs.

Cat >> filename : append new content to existing content in a file.

Cat>filename: overwrite existing content in a file

8. `man`— To know more about a command and how to use it, use the **man** command. It shows the manual pages of the command. For example, “**man cd**” shows the manual pages of the **cd** command.

9. `history`: this command is used to get command history

```
K_M_Abhijith@kali: ~/newdirectory
└$ pwd
/home/K_M_Abhijith
└(K_M_Abhijith@kali)-[~]
└$ mkdir newdirectory
└(K_M_Abhijith@kali)-[~]
└$ cd newdirectory
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ pwd
/home/K_M_Abhijith/newdirectory
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ touch newfile
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ cat >> newfile
hai
hello
^C
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ cat >> newfile
hai everyone
^C
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ cat newfile
hai
hello
hai everyone
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ cat > newfile
new content
^C
└(K_M_Abhijith@kali)-[~/newdirectory]

K_M_Abhijith@kali: ~/newdirectory
└$ cat > newfile
new content
^C
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ cat newfile
new content
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ ls
newfile
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ ls -l
total 4
-rw-r--r-- 1 K_M_Abhijith K_M_Abhijith 12 Jun 14 16:13 newfile
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ ls -d
.
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ ls -ld
drwxr-xr-x 2 K_M_Abhijith K_M_Abhijith 4096 Jun 14 16:09 .
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ ls -a
. ..
newfile
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ ls -lt
total 4
-rw-r--r-- 1 K_M_Abhijith K_M_Abhijith 12 Jun 14 16:13 newfile
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ ^C
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ 

K_M_Abhijith@kali: ~/newdirectory
total 4
-rw-r--r-- 1 K_M_Abhijith K_M_Abhijith 12 Jun 14 16:13 newfile
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ ^C
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ history
 1 pwd
 2 mkdir newdir
 3 pwd
 4 mkdir newdirectory
 5 cd newdirectory
 6 pwd
 7 touch newfile
 8 cat >> newfile
 9 cat newfile
10 cat > newfile
11 cat newfile
12 ls
13 ls -l
14 ls -d
15 ls -ld
16 ls -a
17 ls -lt
18 history
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ rm newfile
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ ls -l
total 0
└(K_M_Abhijith@kali)-[~/newdirectory]
└$ rmdir . .
└(K_M_Abhijith@kali)-[~/newdirectory]
```

1) echo

- to move some data into a file
- to add a text

```
[~] (K_M_Abhijith㉿kali)-[~/country]
[~] $ echo "enter your name";read name;echo "i am $name"
enter your name
abhijith
i am abhijith
```

2) head

- used to view the first lines of any text file
- default it shows 10 lines

```
[~] (K_M_Abhijith㉿kali)-[~/country]
[~] $ touch states.txt
[~] (K_M_Abhijith㉿kali)-[~/country]
[~] $ cat >> states.txt
jammu kashmir
andra pradesh
kerala
delhi
rajasthan
gujrath
mizoram
tamil nadu
[~] (K_M_Abhijith㉿kali)-[~/country]
[~] $ head states.txt
jammu kashmir
andra pradesh
kerala
delhi
rajasthan
gujrath
mizoram
```

```
[~] (K_M_Abhijith㉿kali)-[~/country]
[~] $ head -n 5 states.txt
jammu kashmir
andra pradesh
kerala
delhi
rajasthan
```

3) tail

- will display the last ten lines of a text files

```
(K_M_Abhijith㉿kali)-[~/country]
$ tail states.txt
jammu kashmir
andra pradesh
kerala
delhi
rajasthan
gujrath
mizoram
tamil nadu
```

4) read

- read the contents of a line into a variable

```
(K_M_Abhijith㉿kali)-[~/country]
$ echo "enter your name";read name;echo "i am $name"
enter your name
abhijith
i am abhijith
```

5) more

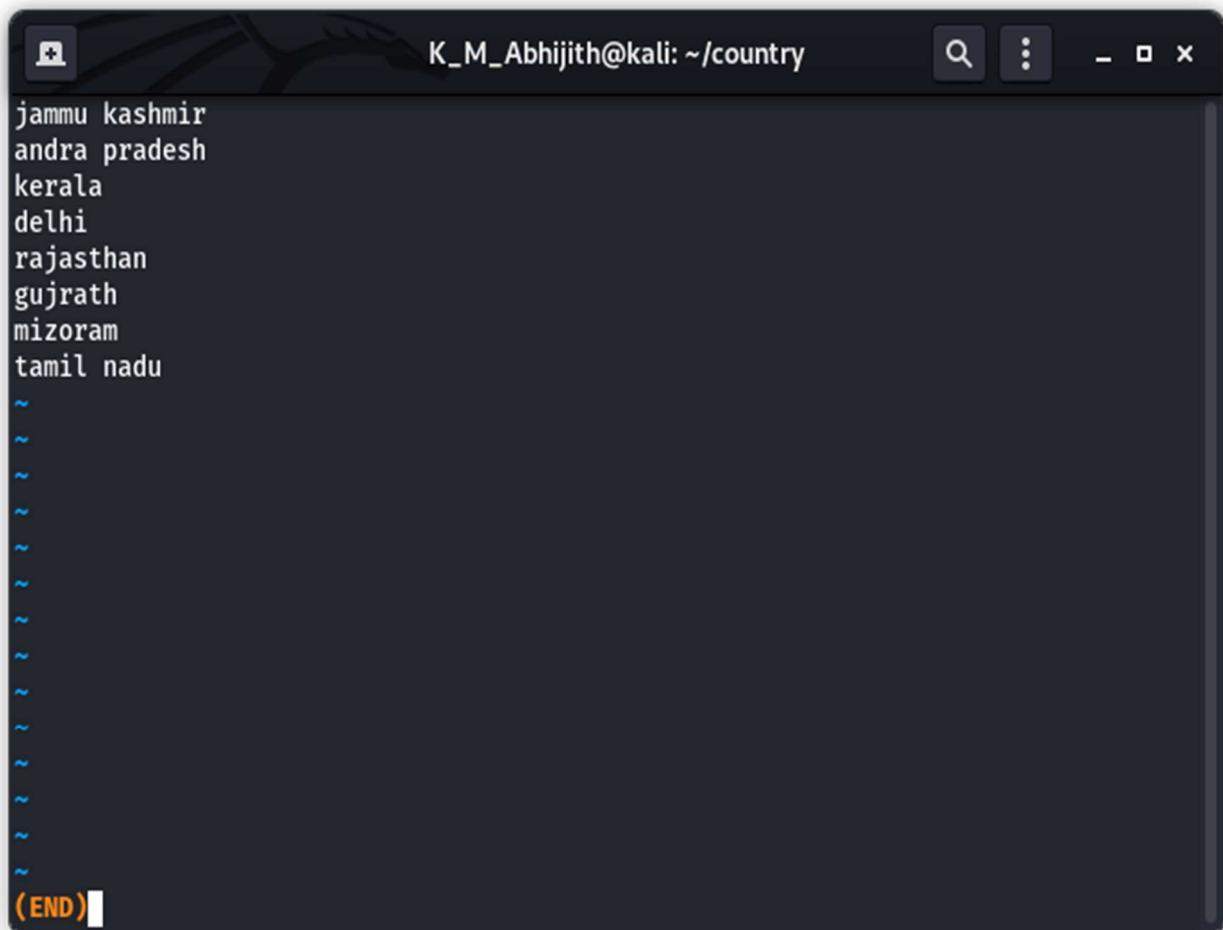
- displays content of the file. Only difference is that in case of larger files cat command output will scroll off your screen while more command displays output one screenful at a time.
- Enter key : to scroll down page line by line
- Space bar : to go to next page
- b key : to go to the backward page
- /key : to search string

```
(K_M_Abhijith㉿kali)-[~/country]
$ more states.txt
jammu kashmir
andra pradesh
kerala
delhi
rajasthan
gujrath
mizoram
tamil nadu
```

6) less

- Automatically adjust with the width and height of terminal window

```
[root@kali ~]# touch file.txt
```



7) cut

- used for cutting out the section from each lines of files and writing the standard output.
- It can be used to cut parts of a line by byte position character and field

```
└──(K_M_Abhijith㉿kali)-[~]
└─$ cd country
└──(K_M_Abhijith㉿kali)-[~/country]
└─$ cat > name.txt
abhijith
sam
joice
nimisha
└──(K_M_Abhijith㉿kali)-[~/country]
└─$ cut -b 1,2,3 name.txt
abh
sam
joi
nim
```

8) paste

- used to join files horizontally by outputting lines consisting of lines from each file specified, separated by tab as delimiter, to the standard output.

```
└──(K_M_Abhijith㉿kali)-[~/country]
└─$ paste states.txt region.txt
jammu kashmir    north
andra pradesh   south
kerala    south
delhi      north
rajasthan     north
gujrath    north
mizoram    north
tamil nadu    south
```

9) uname

- will print detailed information about your linux system like machine name, operating system,kernel etc..

```
(K_M_Abhijith㉿kali)-[~/country]
$ uname -a
Linux kali 5.10.0-kali3-amd64 #1 SMP Debian 5.10.13-1kali1 (2021-02-08) x86_64 GNU/Linux
(K_M_Abhijith㉿kali)-[~/country]
$ uname -s
Linux
(K_M_Abhijith㉿kali)-[~/country]
$ uname -n
kali
(K_M_Abhijith㉿kali)-[~/country]
$ uname -v
```

```
(K_M_Abhijith㉿kali)-[~/country]
$ uname -v
#1 SMP Debian 5.10.13-1kali1 (2021-02-08)
(K_M_Abhijith㉿kali)-[~/country]
$ uname -r
5.10.0-kali3-amd64
(K_M_Abhijith㉿kali)-[~/country]
$ uname -p
unknown
(K_M_Abhijith㉿kali)-[~/country]
$ uname -m
x86_64
(K_M_Abhijith㉿kali)-[~/country]
$ uname -i
unknown
(K_M_Abhijith㉿kali)-[~/country]
$ uname -o
GNU/Linux
```

10)cp

- used to copy files from the current directory to a different directory
- cp -i (will ask for user's consent in case of a potential file overwrite.)
- cp -p (will preserve source file mode, ownership and time stamp)
- cp -r (will copy directories recursively)
- cp -u (copies files only if the destination file is not existing or the source file is newer than the destination file)

```
└─(K_M_Abhijith㉿kali)-[~/country]
└─$ cp number.txt states.txt
└─(K_M_Abhijith㉿kali)-[~/country]
└─$ cat states.txt
1
2
3
4
5
6
7
8
└─(K_M_Abhijith㉿kali)-[~/country]
```

11)mv

- to move files
- rename files

```
└─(K_M_Abhijith㉿kali)-[~/country]
└─$ mv states.txt region.txt
└─(K_M_Abhijith㉿kali)-[~/country]
└─$ cat region.txt
1
2
3
4
5
6
7
8
```

12)locate

- to find a file
- locate -i filename (make it case insensitive you can search file if you don't remember its exact name)
- * (to search for a file that contains two or more words)

```
[~] (K_M_Abhijith㉿kali)-[~/country]
└─$ locate ".txt"
/boot/grub/themes/kali/theme.txt
/etc/X11/rgb.txt
/etc/java-11-openjdk/security/policy/README.txt
```

```
find: possibly unquoted pattern after predicate ~name :
[~] (K_M_Abhijith㉿kali)-[~/country]
└─$ locate -c ".txt"
31312
[~] (K_M_Abhijith㉿kali)-[~/country]
└─$ find . -name number.txt
```

13)find

- To search for files or directories
- Find. -name filename (to find files in the current directory)

```
31312
[~] (K_M_Abhijith㉿kali)-[~/country]
└─$ find . -name number.txt
./number.txt
[~] (K_M_Abhijith㉿kali)-[~/country]
```

14)grep

- Search through all the text in a given file

```
[~] (K_M_Abhijith㉿kali)-[~/country]
└─$ grep -i "1" states.txt
grep: states.txt: No such file or directory
[~] (K_M_Abhijith㉿kali)-[~/country]
└─$ grep -i "1" region.txt
1
```

15) df

- To get report on the system's disk space usage shows in percentage and kbs.

```
(K_M_Abhijith㉿kali)-[~/country]
└─$ df
Filesystem      1K-blocks    Used Available Use% Mounted on
udev              981336       0   981336   0% /dev
tmpfs             203244    1104   202140   1% /run
/dev/sda1        81000912 10199976  66640324 14% /
tmpfs             1016208       0  1016208   0% /dev/shm
tmpfs               5120       0     5120   0% /run/lock
tmpfs             203240       60   203180   1% /run/user/1001
```

16) du

- to check how many space a file or directory takes.

```
tmpfs          203240       60   203180   1% /run/user/1001
(K_M_Abhijith㉿kali)-[~/country]
└─$ du
16 .
```

17) useradd

- available only for system admins.
- To create new user

```
root@kali:~# useradd abhijith
root@kali:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
```

```
kali:x:1000:1000:kali,,,,:/home/kali:/usr/bin/zsh
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
beef-xss:x:130:141::/var/lib/beef-xss:/usr/sbin/nologin
dnsmasq:x:131:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
K_M_Abhijith:x:1001:1001::/home/K_M_Abhijith:/bin/bash
abhijith:x:1002:1002::/home/abhijith:/bin/sh
```

18) userdel

- remove user or delete user account

```
root@kali:~# userdel abhijith
root@kali:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
Debian-gdm:x:129:138:Gnome Display Manager:/var/lib/gdm3:/bin/false
kali:x:1000:1000:kali,,,:/home/kali:/usr/bin/zsh
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
beef-xss:x:130:141::/var/lib/beef-xss:/usr/sbin/nologin
dnsmasq:x:131:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
K_M_Abhijith:x:1001:1001::/home/K_M_Abhijith:/bin/bash
root@kali:~#
```

19) sudo

- SuperUserDo ,enables you to perform tasks that require administrative or root permissions.

```
root@kali:~# sudo -V
Sudo version 1.9.5p2
Configure options: --build=x86_64-linux-gnu --prefix=/usr --includedir=${prefix}/include --mandir=${prefix}/share/man --infodir=${prefix}/share/info --sysconfdir=/etc --localstatedir=/var --disable-option-checking --disable-silent-rules --libdir=${prefix}/lib/x86_64-linux-gnu --libexecdir=${prefix}/lib/x86_64-linux-gnu --disable-maintainer-mode --disable-dependency-tracking -v --with-all-insults --with-pam --with-fqdn --with-logging=syslog --with-logfac=authpriv --with-env-editor --with-editor=/usr/bin/editor --with-exampledir=/usr/share/doc/sudo/examples --with-timeout=15 --with-password-timeout=0 --with-prompt=[sudo] password for %p: --disable-root-mailer --with-sendmail=/usr/sbin/sendmail --with-rundir=/run/sudo --libexecdir=/usr/lib --with-sssd --with-sssd-lib=/usr/lib/x86_64-linux-gnu --enable-zlib=system --with-selinux --with-linux-audit --enable-tmpfiles.d=yes MVPROG=/bin/mv
Sudoers policy plugin version 1.9.5p2
Sudoers file grammar version 48

Sudoers path: /etc/sudoers
Authentication methods: 'pam'
Syslog facility if syslog is being used for logging: authpriv
Syslog priority to use when user authenticates successfully: notice
Syslog priority to use when user authenticates unsuccessfully: alert
Send mail if user authentication fails
Send mail if the user is not in sudoers
Lecture user the first time they run sudo
```

```
root@kali:~# sudo -l
Matching Defaults entries for root on kali:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User root may run the following commands on kali:
    (ALL : ALL) ALL
root@kali:~# sudo -k
```

20) passwd

- to change passwords for user account.

```
root@kali:~# passwd
New password:
Retype new password:
passwd: password updated successfully
root@kali:~# █
```

⌚ **groupadd :**

- ✚ **groupadd** command creates a new group account using the values specified on the command line and the default values from the system.
- ✚ #groupadd student

```
user1:x:1007:1007 :: /home/user1:/bin/sh
root@kali:~# groupadd usrgrp
root@kali:~# groups
root
root@kali:~# cat /etc/groups
cat: /etc/groups: No such file or directory
root@kali:~# cat /etc/group
```

```
kaboxer:x:140:kali
systemd-coredump:x
beef-xss:x:141:
K_M_Abhijith:x:100
user2:x:1003:
usr1:x:1005:user3
user3:x:1006:
user1:x:1007:
usrgrp:x:1008:
```

⌚ **groupdel:**

groupdel command is used to delete a existing group. It will delete all entry that refers to the group, modifies the system account files, and it is handled by superuser or root user.

```
root@kali:~# groupdel newusergrp
root@kali:~# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
```

⌚ **usermod:**

usermod command is used to change the properties of a user in Linux through the commandline

- ✚ command-line utility that allows you to modify a user's login information
- ✚ #usermod --help
- ✚ #usermod -u 2000 Tom

```
root@kali:~# usermod -c "hello" K_M_Abhijith
```

```
root@kali:~# cat /etc/passwd
```

```
K_M_Abhijith:x:1001:1001:hello:/home/K_M_Abhijith:/bin/bash
```

⌚ **groups:**

- + print the groups a user is in
- + #groups alice

```
root@kali:~# groups
```

```
root
```

⌚ **groupmod:**

- + The groupmod command modifies the definition of the specified group by modifying the appropriate entry in the group database.
- + # groupmod -n group1 group2

```
root@kali:~# groupmod -n newusergrp usrgrp
```

```
root@kali:~# cat /etc/group
```

```
root:x:0:
```

```
daemon:x:1:
```

```
bin:x:2:
```

```
user3:x:1006:
```

```
user1:x:1007:
```

```
user:x:1009:
```

```
newusergrp:x:1008:user
```

⌚ **chmod:**

- + To change directory permissions of file/ Directory in Linux.

```
#chmod whowhatwhich file/directory
```

```
+ chmod +rwx filename // To add permissions.
```

```
+ chmod -rwx directoryname // To remove permissions.
```

```
+ chmod +x filename // To allow executable permissions.
```

```
+ chmod -wx filename // to take out write and executable permissions.
```

```
#chmod u+x test
```

```
#chmod g-rwx test
```

```
#chmod o-r test
```

```
-rw-r--r-- 1 root root 10 Aug 12 13:01 myfile2.txt  
root@kali:~# chmod g+rw myfile2.txt  
-rwxr--r-- 1 root root 10 Aug 12 13:01 myfile2.txt
```

⌚ **ps:**

- ✚ The ps command, **short for Process Status**, is a command line utility that is used to display or view information related to the processes running in a Linux system.
- ✚ PID – This is the unique process ID
- ✚ TTY – This is the type of terminal that the user is logged in to
- ✚ TIME – This is the time in minutes and seconds that the process has been running
- ✚ CMD – The command that launched the process #ps -a

```
root@kali:~# ps  
  PID TTY      TIME CMD  
 3714 pts/0    00:00:00 bash  
 3716 pts/0    00:00:00 ps  
root@kali:~# id  
uid=0(root) gid=0(root) groups=0(root)  
root@kali:~#
```

⌚ **chown:**

The chown command allows you to change the user and/or group ownership of a given file, directory.

- ✚ #chown Tom Test

```
-rwxrwxr-- 1 root root 59 Aug 12 12:55 myfile.txt  
root@kali:~# chown K_M_Abhijith myfile.txt  
-rwxrwxr-- 1 K_M_Abhijith root 59 Aug 12 12:55 myfile.txt
```

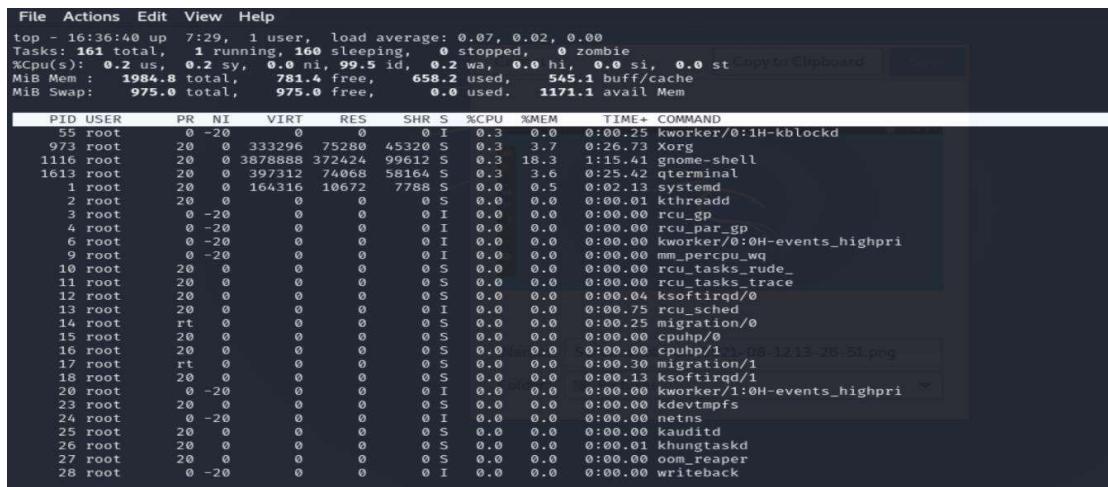
⌚ **id:**

id command in Linux is **used to find out user and group names** and numeric ID's (UID or group ID) of the current user or any other user in the server. List out all the groups a user belongs to. Display security context of the current user

```
root@kali:~# id  
uid=0(root) gid=0(root) groups=0(root)  
root@kali:~#
```

⌚ **top:**

top command is used to show the Linux processes. It provides a dynamic real-time view of the running system. Usually, this command shows the summary information of the system and the list of processes or threads which are currently managed by the Linux Kernel.



The screenshot shows the terminal window of the top command. At the top, it displays system statistics: tasks (161 total), CPU usage (0.2 us, 0.2 sy, 0.0 ni, 99.5 id), memory usage (1984.8 total, 785.4 free, 658.2 used, 545.1 buff/cache, 975.0 total, 975.0 free, 0.0 used, 1171.1 avail Mem). Below this is a detailed process list with columns for PID, USER, PR, NI, VIRT, RES, SHR, S, %CPU, %MEM, TIME+, and COMMAND. The list includes various kernel threads like kworker, Xorg, gnome-shell, terminal, systemd, and rcu_gp, along with user processes like ksoftirqd and migration.

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
55	root	0	-20	0	0	0	I	0.3	0.0	0:00.25	kworker/0:1H-kblockd
973	root	20	0	333296	75280	45320	S	0.3	3.7	0:26.73	Xorg
1116	root	20	0	3878886	372424	99612	S	0.3	18.3	1:15.41	gnome-shell
1613	root	20	0	397312	74068	58164	S	0.3	3.6	0:25.42	terminal
1	root	20	0	164316	10672	7788	S	0.0	0.5	0:02.13	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.01	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/0:0H-events_highpri
9	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
10	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_tasks_rude_
11	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_tasks_trace
12	root	20	0	0	0	0	S	0.0	0.0	0:00.04	ksoftirqd/0
13	root	20	0	0	0	0	I	0.0	0.0	0:00.75	rcu_sched
14	root	rt	0	0	0	0	S	0.0	0.0	0:00.25	migration/0
15	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/0
16	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/1
17	root	rt	0	0	0	0	S	0.0	0.0	0:00.30	migration/1
18	root	20	0	0	0	0	S	0.0	0.0	0:00.13	ksoftirqd/1
20	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/1:0H-events_highpri
23	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kdevtmpfs
24	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
25	root	20	0	0	0	0	S	0.0	0.0	0:00.00	Kaudited
26	root	20	0	0	0	0	S	0.0	0.0	0:00.01	khungtaskd
27	root	20	0	0	0	0	S	0.0	0.0	0:00.00	oom_reaper
28	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	writeback

⌚ wc:

wc stands for word count.

✚ Used for counting purpose.

✚ It is used to find out number of lines, word count, byte and characters count in the files specified in the file arguments.

✚ #wc state.txt 6 8 54 state.txt

✚ #wc state.txt capital.txt

✚ wc -l state.txt

✚ wc -w state.txt capital.txt

✚ wc -c state.txt

✚ wc -m state.txt

```
root@kali:~# cat > myfile.txt
helloeveryone
hope u all are fine
hai hello,helllo hi
hehe
root@kali:~# cat > myfile2.txt
hai hello
root@kali:~# wc myfile.txt
 4 10 59 myfile.txt
root@kali:~# wc myfile2.txt
 1 2 10 myfile2.txt
root@kali:~# wc -l myfile.txt
4 myfile.txt
root@kali:~# wc -w myfile.txt myfile2.txt
10 myfile.txt
 2 myfile2.txt
12 total
root@kali:~# wc -c myfile.txt
59 myfile.txt
root@kali:~# wc -m myfile.txt
59 myfile.txt
```

⌚ Tar:

- The Linux ‘tar’stands for tape archive, is used to create Archive and extract the Archive files
- Linux tar command to create compressed or uncompressed Archive files

Options:

✚ -c : Creates Archive

✚ -x : Extract the archive

✚ -f : creates archive with given filename

✚ -t: displays or lists files in archived file

✚ -u: archives and adds to an existing archive file

✚ -v: Displays Verbose Information

✚ -A : Concatenates the archive files

✚ -z : zip, tells tar command that creates tar file using gzip

- ✚ -j : filter archive tar file using tbzip
- ✚ -W : Verify a archive file
- ✚ -r : update or add file or directory in already existed .tar file

```
#tar cf archive.tar state.txt capital.txt //create archive file
#ls archive.tar
#tar tf /archive.tar // list contents of tar archive file
✚ Extract an archive created with tar
#mkdir backup
#cd backup
#tar xf/home/meera/Documents/Meera_Linux/archive.tar
```

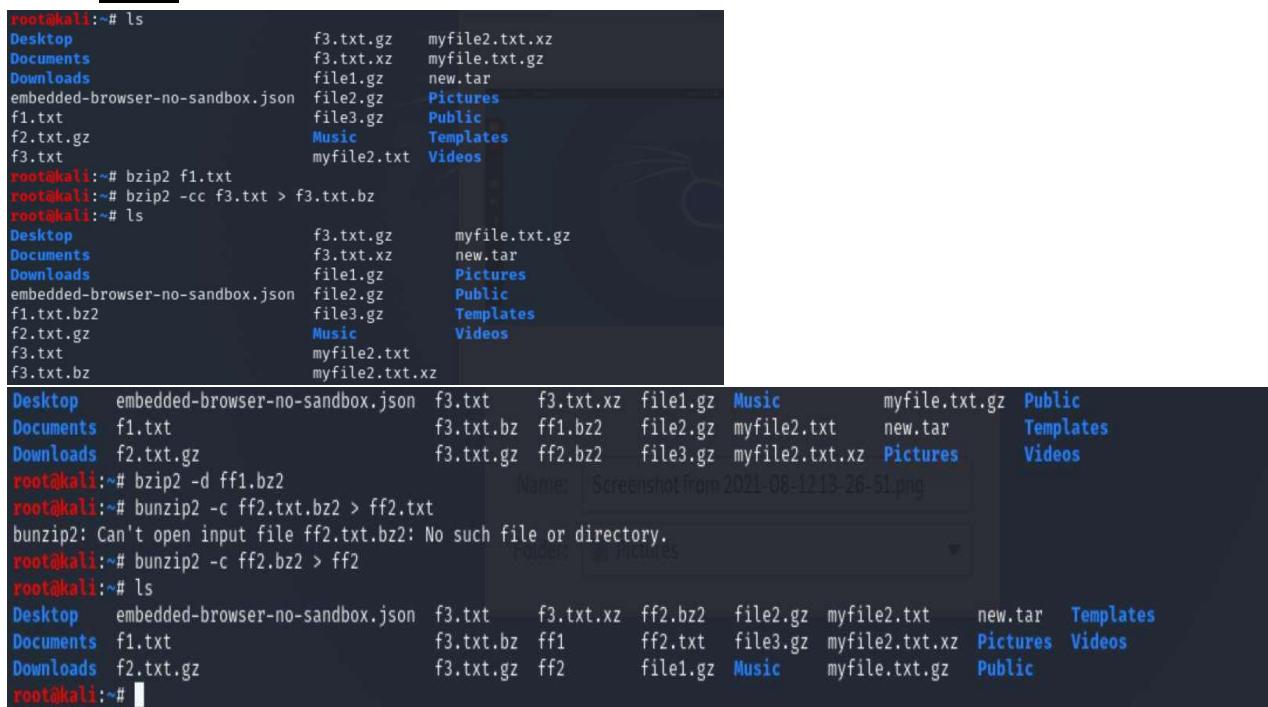
➤ Compression Types

```
gzip(z),bzip2(j), xz(J) #tar czf /abc.tar.gz /etc
#tar cjf /abcd.tar.bz2 /etc
#tar cJf /abcde.tar.xz /etc
```

➤ Extract an archive

```
#mkdir backup1
#cd backup1
#tar xzf /abc.tar.gz
#mkdir backup2
#cd backup2
#tar xjf /abcd.tar.bz2
#mkdir backup3
#cd backup3
#tar xJf /abcde.tar.xz
```

✚ Bzip2



The screenshot shows a terminal session on a Kali Linux system. The user runs several commands related to file compression:

```
root@kali:~# ls
Desktop          f3.txt.gz    myfile2.txt.xz
Documents         f3.txt.xz   myfile.txt.gz
Downloads        file1.gz     new.tar
embedded-browser-no-sandbox.json file2.gz    Pictures
f1.txt           file3.gz    Public
f2.txt.gz        Music       Templates
f3.txt          myfile2.txt  Videos

root@kali:~# bzip2 f1.txt
root@kali:~# bzip2 -cc f3.txt > f3.txt.bz
root@kali:~# ls
Desktop          f3.txt.gz    myfile.txt.gz
Documents         f3.txt.xz   new.tar
Downloads        file1.gz     Pictures
embedded-browser-no-sandbox.json file2.gz    Public
f1.txt.bz2        file3.gz    Templates
f2.txt.gz        Music       Videos
f3.txt          myfile2.txt  myfile2.txt.xz
f3.txt.bz        myfile2.txt.xz

root@kali:~# bzzip2 -d ff1.bz2
root@kali:~# bunzip2 -c ff2.txt.bz2 > ff2.txt
bunzip2: Can't open input file ff2.txt.bz2: No such file or directory.
root@kali:~# bunzip2 -c ff2.bz2 > ff2
root@kali:~# ls
Desktop          embedded-browser-no-sandbox.json f3.txt      f3.txt.xz   ff2.bz2   file2.gz  myfile2.txt    new.tar    Templates
Documents         f1.txt                  f3.txt.bz   ff1        ff2.txt   file3.gz  myfile2.txt.xz  Pictures  Videos
Downloads        f2.txt.gz               f3.txt.gz   ff2        file1.gz  myfile.txt.gz  Public
```

gzip

```
root@kali:~# apt-get install gzip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gzip is already the newest version (1.10-2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:~# ls
Desktop          f2.txt      new.tar
Documents        f3.txt      Pictures
Downloads        Music       Public
embedded-browser-no-sandbox.json myfile2.txt  Templates
f1.txt.gz        myfile.txt.gz Videos
root@kali:~# gzip f2.txt
root@kali:~# ls
Desktop          f2.txt.gz   new.tar
Documents        f3.txt      Pictures
Downloads        Music       Public
embedded-browser-no-sandbox.json myfile2.txt  Templates
f1.txt.gz        myfile.txt.gz Videos
root@kali:~# touch file1 file2 file3
root@kali:~# gzip file1.txt file2.txt file3.txt
gzip: file1.txt: No such file or directory
gzip: file2.txt: No such file or directory
gzip: file3.txt: No such file or directory
root@kali:~# gzip file1 file2 file3
root@kali:~# ls
Desktop          f3.txt      myfile.txt.gz
Documents        file1.gz   new.tar
Downloads        file2.gz   Pictures
embedded-browser-no-sandbox.json file3.gz   Public
f1.txt.gz        Music      Templates
root@kali:~# gzip -c f3.txt > f3.txt.gz
root@kali:~# ls
Desktop          f3.txt.gz  new.tar
Documents        file1.gz   Pictures
Downloads        file2.gz   Public
embedded-browser-no-sandbox.json file3.gz   Templates
f1.txt           Music      Videos
f2.txt.gz        myfile2.txt
f3.txt           myfile.txt.gz
root@kali:~# gzip -d f1.txt.gz
root@kali:~# ls
Desktop          f3.txt.gz  new.tar
Documents        file1.gz   Pictures
Downloads        file2.gz   Public
embedded-browser-no-sandbox.json file3.gz   Templates
f1.txt           Music      Videos
f2.txt.gz        myfile2.txt
f3.txt           myfile.txt.gz
root@kali:~# gzip -c f2.txt > f2.txt.gz
gzip: f2.txt: No such file or directory
root@kali:~# gzip -c f2.txt.gz > f2.txt.gz
root@kali:~# ls
Desktop          f3.txt.gz  new.tar
Documents        file1.gz   Pictures
Downloads        file2.gz   Public
embedded-browser-no-sandbox.json file3.gz   Templates
f1.txt           Music      Videos
f2.txt.gz        myfile2.txt
f3.txt           myfile.txt.gz
root@kali:~#
```

XZ

```
root@kali:~# apt-get install xz-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
xz-utils is already the newest version (5.2.5-1.0).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:~# ls
Desktop          f3.txt.gz  new.tar
Documents        file1.gz   Pictures
Downloads        file2.gz   Public
embedded-browser-no-sandbox.json file3.gz   Templates
f1.txt           Music      Videos
f2.txt.gz        myfile2.txt
f3.txt           myfile.txt.gz
root@kali:~# xz f1.txt
root@kali:~# xz -k f3.txt
root@kali:~# xz -c myfile2.txt > myfile2.txt.xz
root@kali:~# ls
Desktop          f3.txt.gz  myfile2.txt.xz
Documents        f3.txt.xz  myfile.txt.gz
Downloads        file1.gz   new.tar
embedded-browser-no-sandbox.json file2.gz   Pictures
f1.txt.xz        file3.gz   Public
f2.txt.gz        Music      Templates
f3.txt           myfile2.txt Videos
root@kali:~#
```

```
root@kali:~# xz -d f1.txt.xz
root@kali:~# unxz -k f2.txt.xz
unxz: f2.txt.xz: No such file or directory
root@kali:~#
root@kali:~# unxz -k f3.txt.xz
unxz: f3.txt: File exists
root@kali:~# ls
Desktop           f3.txt.gz    myfile2.txt.xz
Documents         f3.txt.xz    myfile.txt.gz
Downloads        file1.gz     new.tar
embedded-browser-no-sandbox.json file2.gz    Pictures
f1.txt            file3.gz    Public
f2.txt.gz          Music      Templates
f3.txt            myfile2.txt Videos
root@kali:~#
```

⌚ expr

- + The expr command evaluates a given expression and displays its corresponding output. It is used for:
 - + Basic operations like addition, subtraction, multiplication, division, and modulus on integers.
 - + Evaluating regular expressions, string operations like substring, length of strings etc.
 - + Performing operations on variables inside a shell script

```
#expr 10 + 2
```

```
root@kali:~# expr 12 + 10
22
root@kali:~# expr 12 \* 10
120
root@kali:~# expr 12 - 10
2
```

⌚ Redirections & Piping :

- + A pipe is a form of redirection to send the output of one command/program/process to another command/program/process for further processing.
- + Pipe is used to combine two or more commands, the output of one command acts as input to another command, and this command's output may act as input to the next command and so on.

```
#ls -l | wc -l
```

```
#cat /etc/passwd.txt | head -7 | tail -5
```

```
root@kali:~# cat /etc/myfile.txt|head -5 | tail -3
cat: /etc: Is a directory
hope u all are fine
hai hello,helllo hi
hehe
root@kali:~#
```

⌚ ssh

- + ssh stands for “Secure Shell”.
- + It is a protocol used to securely connect to a remote server/system.
- + ssh is secure in the sense that it transfers the data in encrypted form between the host and the client.

- + It transfers inputs from the client to the host and relays back the output. ssh runs at TCP/IP port 22.

```
#ssh user_name@host(IP/Domain_name)
```

```
#ssh -X root@server1.example.com
```

```
root@kali:~# ssh --help
unknown option -- -
usage: ssh [-46AaCfGgKkMNqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
```

⌚ scp

- + SCP (secure copy) is a command-line utility that allows you to securely

- + copy files and directories between two locations.

- + With scp, you can copy a file or directory:

- + From your local system to a remote system.

- + From a remote system to your local system.

- + Between two remote systems from your local system.

- + Remote file system locations are specified in format

- + [user@]host:/path Syntax:

```
scp [OPTION] [user@]SRC_HOST:]file1 [user@]DEST_HOST:]file2
```

```
$scp/etc/yum.config/etc/hosts ServerX:/home/student
```

```
$scp ServerX:/etc/hostname /home/student
```

```
root@kali:~# ssh root@kali
ssh: connect to host kali port 22: Connection refused
```

⌚ ssh-keygen

ssh-keygen command to generate a public/private authentication key pair. Authentication keys allow a user to connect to a remote system without supplying a password. Keys must be generated for each user separately. If you generate key pairs as the root user, only the root can use the keys.

```
$ssh-keygen -t rsa
```

```
root@kali:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in rsa
Your public key has been saved in rsa.pub
The key fingerprint is:
SHA256:Si7sd5154YckqJXUKTLk0d4y66S9FBkcQilN3epryM root@kali
The key's randomart image is:
+---[RSA 3072]---+
 .oo+.
 .B.o .
 ==oO.oo
 .Oo*o
 .oSB.
 . oo.+ o.o
 o.o* o *o
 . *= E = .+
 .. o ..o .
+---[SHA256]---+
```

⌚ ssh-copy-id

- The ssh-copy-id command allows you to install an SSH key on a remote server's authorized keys.
- This command facilitates SSH key login, which removes the need for a password for each login, thus ensuring a password-less, automatic login process.
- \$ssh-copy-id username@remote_host

Managing Files, Creating Users and Groups Using Command-line tools

1. a. Create six files with name of the form songX.mp3
- b. Create six files with name of the form snapX.mp3
- c. Create six files with name of the form filmX.mp3 (In each set, replace X with the numbers 1 through 6)

```
kmabhijith@kmabhijith-VirtualBox:~$ touch song1.mp3 song2.mp3 song3.mp3 song4.mp3 song5.mp3 song6.mp3
kmabhijith@kmabhijith-VirtualBox:~$ touch snap1.mp3 snap2.mp3 snap3.mp3 snap4.mp3 snap5.mp3 snap6.mp3
kmabhijith@kmabhijith-VirtualBox:~$ touch film1.mp3 film2.mp3 film3.mp3 film4.mp3 film5.mp3 film6.mp3
```

2. From your home directory, move the song files into your music subdirectory, the snapshot files into your pictures subdirectory, and the movie files into videos subdirectory.

```
root@kmabhijith-VirtualBox:/home# mv snap1.mp3 snap2.mp3 snap3.mp3 snap4.mp3 snap5.mp3 snap6.mp3 kmabhijith/Pictures
root@kmabhijith-VirtualBox:/home# mv song1.mp3 song2.mp3 song3.mp3 song4.mp3 song5.mp3 song6.mp3 kmabhijith/Music
```

3. In your home directory, create three subdirectories for organizing your files. Call these directories friends, family, and work. Create all three with one command

```
root@kmabhijith-VirtualBox:/home# mkdir {friends,family,works}
```

4. Copy song files to the friends folder and snap files to family folder

```
root@kmabhijith-VirtualBox:/home# cp Music/ song1.mp3 song2.mp3 song3.mp3 song4.mp3 song5.mp3 song6.mp3 /friends
root@kmabhijith-VirtualBox:/home/friends# cp Pictures/ snap1.mp3 snap2.mp3 snap3.mp3 snap4.mp3 snap5.mp3 snap6.mp3 /family
```

5. Attempt to delete both family and friends projects with a single rmdir command.

```
root@kmabhijith-VirtualBox:/home# rmdir family friends
```

6. Use another command that will succeed in deleting both the family and friends folder.

```
root@kmabhijith-VirtualBox:/home# rm -r family friends
```

7. Redirect a long listing of all home directory files, including hidden, into a file named allfiles.txt. Confirm that the file contains the listing.

```
root@kmabhijith-VirtualBox:/home# ls -a >allfiles.txt
root@kmabhijith-VirtualBox:/home# ls
allfiles.txt  film2.mp3  film4.mp3  film6.mp3  work
film1.mp3    film3.mp3  film5.mp3  kmabhijith
root@kmabhijith-VirtualBox:/home# ls -al
total 16
drwxr-xr-x  4 root      root      4096 Aug 17 21:46 .
drwxr-xr-x 20 root      root      4096 Aug 16 22:21 ..
-rw-r--r--  1 root      root      0 Aug 17 21:46 allfiles.txt
-rw-r--r--  1 root      root      0 Aug 17 20:39 film1.mp3
-rw-r--r--  1 root      root      0 Aug 17 20:39 film2.mp3
-rw-r--r--  1 root      root      0 Aug 17 20:39 film3.mp3
-rw-r--r--  1 root      root      0 Aug 17 20:39 film4.mp3
-rw-r--r--  1 root      root      0 Aug 17 20:39 film5.mp3
-rw-r--r--  1 root      root      0 Aug 17 20:39 film6.mp3
drwxr-xr-x 16 kmabhijith kmabhijith 4096 Aug 17 20:32 kmabhijith
drwxr-xr-x  2 root      root      4096 Aug 17 20:40 work
```

8. In the command window, display today's date with day of the week, month, date and year

```
root@kmabhijith-VirtualBox:/home# date
Tuesday 17 August 2021 09:47:06 PM IST
```

9. Add the user Juliet

```
root@kmabhijith-VirtualBox:/home# useradd juliet
```

10. Confirm that Juliet has been added by examining the /etc/passwd file

```
root@kmabhijith-VirtualBox:/home# cat /etc/passwd
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
kmabhijith:x:1000:1000:K M Abhijith,,,:/home/kmabhijith:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:126:133:MySQL Server,,,:/nonexistent:/bin/false
lightdm:x:127:134:Light Display Manager:/var/lib/lightdm:/bin/false
juliet:x:1001:1001::/home/juliet:/bin/sh
```

11. Use the passwd command to initialize Juliet's password

```
root@kmabhijith-VirtualBox:/home# passwd juliet
New password:
Retype new password:
passwd: password updated successfully
```

12. Create a supplementary group called Shakespeare with a group id of 30000

```
root@kmabhijith-VirtualBox:/home# groupadd -g 30000 shakespeare
```

13. Create a supplementary group called artists.

```
root@kmabhijith-VirtualBox:/home# groupadd -g 20000 artists
```

14. Confirm that Shakespeare and artists have been added by examining the /etc/group file.

```
root@kmabhijith-VirtualBox:/home# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,kmabhijith
tty:x:5:syslog
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
ssl-cert:x:113:
uuidd:x:114:
tcpdump:x:115:
avahi-autoipd:x:116:
rtkit:x:117:
ssh:x:118:
netdev:x:119:
lpadmin:x:120:kmabhijith
avahi:x:121:
scanner:x:122:saned
saned:x:123:
nm-openvpn:x:124:
whoopsie:x:125:
colord:x:126:
geoclue:x:127:
pulse:x:128:
pulse-access:x:129:
gdm:x:130:
lxde:x:131:kmabhijith
kmabhijith:x:1000:
sambashare:x:132:kmabhijith
systemd-coredump:x:999:
mysql:x:133:
lightdm:x:134:
nopasswdlogin:x:135:
juliet:x:1001:
shakesphere:x:3000:
artists:x:20000:
```

15. Add the Juliet user to the Shakespeare group as a supplementary group.

```
root@kmabhijith-VirtualBox:/home# groups juliet
juliet : juliet
root@kmabhijith-VirtualBox:/home# usermod -a -G shakesphere juliet
root@kmabhijith-VirtualBox:/home#
```

16. Confirm that Juliet has been added using the id command.

```
root@kmabhijith-VirtualBox:/home# id juliet
uid=1001(juliet) gid=1001(juliet) groups=1001(juliet),3000(shakesphere)
```

17. Add Romeo and Hamlet to the Shakespeare group.

```
root@kmabhijith-VirtualBox:/home# useradd romeo
root@kmabhijith-VirtualBox:/home# useradd hamlet
root@kmabhijith-VirtualBox:/home# usermod -a -G shakesphere romeo
root@kmabhijith-VirtualBox:/home# usermod -a -G shakesphere hamlet
root@kmabhijith-VirtualBox:/home# id romeo
uid=1002(romeo) gid=1002(romeo) groups=1002(romeo),3000(shakesphere)
root@kmabhijith-VirtualBox:/home# id hamlet
uid=1003(hamlet) gid=1003(hamlet) groups=1003(hamlet),3000(shakesphere)
root@kmabhijith-VirtualBox:/home#
```

18. Add Reba, Dolly and Elvis to the artists group

```
root@kmabhijith-VirtualBox:/home# useradd reba
root@kmabhijith-VirtualBox:/home# useradd dolly
root@kmabhijith-VirtualBox:/home# useradd elvis
root@kmabhijith-VirtualBox:/home# usermod -a -G artists reba
root@kmabhijith-VirtualBox:/home# usermod -a -G artists dolly
root@kmabhijith-VirtualBox:/home# usermod -a -G artists elvis
root@kmabhijith-VirtualBox:/home# id reba
uid=1004(reba) gid=1004(reba) groups=1004(reba),20000(artists)
root@kmabhijith-VirtualBox:/home# id dolly
uid=1005(dolly) gid=1005(dolly) groups=1005(dolly),20000(artists)
root@kmabhijith-VirtualBox:/home# id elvis
uid=1006(elvis) gid=1006(elvis) groups=1006(elvis),20000(artists)
```

19. Verify the supplemental group memberships by examining the /etc/group file

```
root@kmabhijith-VirtualBox:/home# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,kmabhijith
tty:x:5:syslog
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
```

```
avahi:x:121:  
scanner:x:122:saned  
saned:x:123:  
nm-openvpn:x:124:  
whoopsie:x:125:  
colord:x:126:  
geoclue:x:127:  
pulse:x:128:  
pulse-access:x:129:  
gdm:x:130:  
lxd:x:131:kmabhijith  
kmabhijith:x:1000:  
sambashare:x:132:kmabhijith  
systemd-coredump:x:999:  
mysql:x:133:  
lightdm:x:134:  
nopasswdlogin:x:135:  
juliet:x:1001:  
shakesphere:x:3000:juliet,romeo,hamlet  
artists:x:20000:reba,dolly,elvis  
romeo:x:1002:  
hamlet:x:1003:  
reba:x:1004:  
dolly:x:1005:  
elvis:x:1006:
```

20. Attempt to remove user Dolly.

```
root@kmabhijith-VirtualBox:/home# userdel -r dolly  
userdel: dolly mail spool (/var/mail/dolly) not found  
userdel: dolly home directory (/home/dolly) not found
```

NETWORK COMMANDS

WINDOWS

1. Ping & traceroute tests

Ping and Trace Route tests can help to identify any connection issues between your network and a specified server (or website) address.

PING test:

The PING command is used to test the connection and latency between two network connections. The PING command sends packets of information to a specified IP Address and then measures the time it takes to get a response from the specified computer or device.

Trace Route test:

The TRACERT command is used to conduct a similar test to PING, but instead of displaying the time it takes to connect, it looks at the exact server hops required to connect your computer to the server.

You should already have the CMD prompt dialogue box open, after performing the PING test above.

```
C:\ Command Prompt

C:\Users\K M Abhijith>ping www.google.com

Pinging www.google.com [142.250.205.228] with 32 bytes of data:
Reply from 142.250.205.228: bytes=32 time=24ms TTL=119
Reply from 142.250.205.228: bytes=32 time=26ms TTL=119
Reply from 142.250.205.228: bytes=32 time=23ms TTL=119
Reply from 142.250.205.228: bytes=32 time=24ms TTL=119

Ping statistics for 142.250.205.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 26ms, Average = 24ms

C:\Users\K M Abhijith>tracert www.google.com

Tracing route to www.google.com [142.250.205.228]
over a maximum of 30 hops:

 1      1 ms      1 ms      1 ms  192.168.1.1
 2      2 ms      5 ms      2 ms  172.16.10.1
 3     24 ms     23 ms     23 ms  45.125.116.205
 4     23 ms     23 ms     23 ms  45.125.116.86
 5     56 ms     25 ms     26 ms  216.239.54.75
 6     24 ms     24 ms     24 ms  142.251.60.187
 7     23 ms     23 ms     23 ms  maa05s28-in-f4.1e100.net [142.250.205.228]

Trace complete.
```

1. Nslookup

Microsoft Windows includes a tool called NSLOOKUP that you can use via the command prompt. This tool can be used to check DNS records propagation and resolution using different servers, and perform other troubleshooting steps.

```
C:\Users\K M Abhijith>nslookup aesajce.in
Server: ns3.blss.in
Address: 45.125.117.250

Non-authoritative answer:
Name: aesajce.in
Address: 103.120.179.46
```

- ⑤ Type nslookup -q=XX where XX is a type of a DNS record. Some of the available types are MX, A, CNAME, and TXT. The records are then displayed, to exit the tool type exit

```
C:\Users\K M Abhijith>nslookup -type=ns aesajce.in
Server: ns3.blss.in
Address: 45.125.117.250

Non-authoritative answer:
aesajce.in      nameserver = ns2.ajaxca.in
aesajce.in      nameserver = ns1.ajaxca.in
aesajce.in      nameserver = ns1.aessas.com
aesajce.in      nameserver = ns2.aessas.com

ns2.aessas.com  internet address = 103.120.179.46
ns1.aessas.com  internet address = 103.120.179.46
ns2.ajaxca.in   internet address = 103.120.179.46
ns1.ajaxca.in   internet address = 103.120.179.46

C:\Users\K M Abhijith>
```

- ⑤ To use **nslookup** as a troubleshooting tool, you can set the specific type of record to lookup for a domain by using the **-type=record_type** where **record_type** is A, CNAME, MX, PTR, NS, ANY.

Type **nslookup -type=ns domain_name** where **domain_name** is the domain for your query and hit **Enter**. Now the tool will display the name servers for the domain you specified.

```
C:\Users\K M Abhijith>nslookup -q=MX aesajce.in
Server: ns3.blss.in
Address: 45.125.117.250

Non-authoritative answer:
aesajce.in      MX preference = 1, mail exchanger = aspmx.l.google.com
aesajce.in      MX preference = 10, mail exchanger = aspmx3.googlemail.com
aesajce.in      MX preference = 5, mail exchanger = alt2.aspmx.l.google.com
aesajce.in      MX preference = 5, mail exchanger = alt1.aspmx.l.google.com
aesajce.in      MX preference = 10, mail exchanger = aspmx2.googlemail.com

aesajce.in      nameserver = ns1.ajaxemca.in
aesajce.in      nameserver = ns2.ajaxemca.in
aesajce.in      nameserver = ns2.aessas.com
aesajce.in      nameserver = ns1.aessas.com
ASPMX.l.google.com   internet address = 142.250.4.27
ns1.ajaxemca.in  internet address = 103.120.179.46
ns2.aessas.com   internet address = 103.120.179.46
ns1.aessas.com   internet address = 103.120.179.46
ns2.ajaxemca.in  internet address = 103.120.179.46

C:\Users\K M Abhijith>
```

2. Netstat

On Windows 10, netstat (network statistics) has been around for a long time, and it's a command-line tool that you can use in Command Prompt to display statistics for all network connections. It allows you to understand open and connected ports to monitor and troubleshoot networking problems for system or applications.

```
C:\Users\K M Abhijith>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49670        DESKTOP-ILB31AE:49671  ESTABLISHED
  TCP    127.0.0.1:49671        DESKTOP-ILB31AE:49670  ESTABLISHED
  TCP    127.0.0.1:49672        DESKTOP-ILB31AE:49673  ESTABLISHED
  TCP    127.0.0.1:49673        DESKTOP-ILB31AE:49672  ESTABLISHED
  TCP    127.0.0.1:51374        DESKTOP-ILB31AE:65001  ESTABLISHED
  TCP    127.0.0.1:56487        DESKTOP-ILB31AE:57828  ESTABLISHED
  TCP    127.0.0.1:57828        DESKTOP-ILB31AE:56487  ESTABLISHED
  TCP    127.0.0.1:65001        DESKTOP-ILB31AE:51374  ESTABLISHED
  TCP    192.168.1.33:49494     ec2-35-169-11-179:https CLOSE_WAIT
  TCP    192.168.1.33:49495     52.242.17.32:https   ESTABLISHED
  TCP    192.168.1.33:49496     13.107.3.254:https  ESTABLISHED
```

netstat -n

command to display active connections showing numeric IP address and port number instead of trying to determine the names .

netstat -n INTERVAL

In the command, make sure to replace INTERVAL for the number (in seconds) you want to redisplay the information.

Active Connections			
Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:49670	127.0.0.1:49671	ESTABLISHED
TCP	127.0.0.1:49671	127.0.0.1:49670	ESTABLISHED
TCP	127.0.0.1:49672	127.0.0.1:49673	ESTABLISHED
TCP	127.0.0.1:49673	127.0.0.1:49672	ESTABLISHED
TCP	127.0.0.1:51374	127.0.0.1:65001	ESTABLISHED
TCP	127.0.0.1:56487	127.0.0.1:57828	ESTABLISHED
TCP	127.0.0.1:57828	127.0.0.1:56487	ESTABLISHED
TCP	127.0.0.1:65001	127.0.0.1:51374	ESTABLISHED
TCP	192.168.1.33:49192	44.240.40.22:443	ESTABLISHED
TCP	192.168.1.33:49204	23.215.204.209:443	ESTABLISHED
TCP	192.168.1.33:49643	52.46.130.91:443	ESTABLISHED
TCP	192.168.1.33:49654	23.215.205.13:443	ESTABLISHED
TCP	192.168.1.33:49675	52.207.5.56:443	ESTABLISHED
TCP	192.168.1.33:49774	52.201.138.78:443	ESTABLISHED
TCP	192.168.1.33:49790	52.201.138.78:443	ESTABLISHED
TCP	192.168.1.33:49828	76.223.111.131:443	ESTABLISHED
TCP	192.168.1.33:49843	142.250.71.46:443	TIME_WAIT
TCP	192.168.1.33:49969	64.38.119.27:443	ESTABLISHED
TCP	192.168.1.33:50048	104.89.172.189:443	ESTABLISHED
TCP	192.168.1.33:50067	52.84.6.102:443	ESTABLISHED
TCP	192.168.1.33:50077	13.251.78.15:443	ESTABLISHED
TCP	192.168.1.33:50081	44.233.174.75:443	ESTABLISHED
TCP	192.168.1.33:50142	67.202.105.21:443	ESTABLISHED
TCP	192.168.1.33:50261	52.84.12.165:443	ESTABLISHED
TCP	192.168.1.33:50346	104.18.188.55:443	ESTABLISHED
TCP	192.168.1.33:50423	69.173.158.65:443	ESTABLISHED
TCP	192.168.1.33:50610	35.71.178.8:443	ESTABLISHED
TCP	192.168.1.33:50682	52.30.185.188:443	ESTABLISHED
TCP	192.168.1.33:50693	52.84.6.84:443	ESTABLISHED
TCP	192.168.1.33:50709	103.231.98.193:443	ESTABLISHED
TCP	192.168.1.33:50716	104.80.62.113:443	ESTABLISHED
TCP	192.168.1.33:50742	18.139.237.11:443	ESTABLISHED
TCP	192.168.1.33:50763	52.46.130.91:443	ESTABLISHED
TCP	192.168.1.33:50819	142.250.182.34:443	ESTABLISHED
TCP	192.168.1.33:50881	23.215.205.13:443	ESTABLISHED
TCP	192.168.1.33:50887	34.95.69.49:443	ESTABLISHED
TCP	192.168.1.33:50933	103.43.90.178:443	ESTABLISHED
TCP	192.168.1.33:51043	142.250.196.86:443	ESTABLISHED
TCP	192.168.1.33:51373	20.198.162.76:443	ESTABLISHED
TCP	192.168.1.33:51459	35.213.120.246:443	ESTABLISHED
TCP	192.168.1.33:51460	104.26.3.146:443	ESTABLISHED
TCP	192.168.1.33:51555	142.250.183.229:443	ESTABLISHED

netstat -a

The netstat -a command displays all active and inactive connections, and the TCP and UDP ports the device is currently listening.

```
C:\Users\K M Abhijith>netstat -a
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	DESKTOP-ILB31AE:0	LISTENING
TCP	0.0.0.0:445	DESKTOP-ILB31AE:0	LISTENING
TCP	0.0.0.0:3305	DESKTOP-ILB31AE:0	LISTENING
TCP	0.0.0.0:5040	DESKTOP-ILB31AE:0	LISTENING
TCP	0.0.0.0:5357	DESKTOP-ILB31AE:0	LISTENING
TCP	0.0.0.0:7680	DESKTOP-ILB31AE:0	LISTENING
TCP	0.0.0.0:33060	DESKTOP-ILB31AE:0	LISTENING
TCP	0.0.0.0:49664	DESKTOP-ILB31AE:0	LISTENING
TCP	0.0.0.0:49665	DESKTOP-ILB31AE:0	LISTENING
TCP	0.0.0.0:49666	DESKTOP-ILB31AE:0	LISTENING
TCP	0.0.0.0:49667	DESKTOP-ILB31AE:0	LISTENING
TCP	0.0.0.0:49668	DESKTOP-ILB31AE:0	LISTENING
TCP	0.0.0.0:49669	DESKTOP-ILB31AE:0	LISTENING
TCP	127.0.0.1:1001	DESKTOP-ILB31AE:0	LISTENING
TCP	127.0.0.1:27017	DESKTOP-ILB31AE:0	LISTENING
TCP	127.0.0.1:49670	DESKTOP-ILB31AE:49671	ESTABLISHED
TCP	127.0.0.1:49671	DESKTOP-ILB31AE:49670	ESTABLISHED
TCP	127.0.0.1:49672	DESKTOP-ILB31AE:49673	ESTABLISHED
TCP	127.0.0.1:49673	DESKTOP-ILB31AE:49672	ESTABLISHED
TCP	127.0.0.1:51374	DESKTOP-ILB31AE:65001	ESTABLISHED
TCP	127.0.0.1:56487	DESKTOP-ILB31AE:0	LISTENING
TCP	127.0.0.1:56487	DESKTOP-ILB31AE:57828	ESTABLISHED
TCP	127.0.0.1:56525	DESKTOP-ILB31AE:0	LISTENING
TCP	127.0.0.1:57828	DESKTOP-ILB31AE:56487	ESTABLISHED
TCP	127.0.0.1:65001	DESKTOP-ILB31AE:0	LISTENING
TCP	127.0.0.1:65001	DESKTOP-ILB31AE:51374	ESTABLISHED
TCP	192.168.1.33:139	DESKTOP-ILB31AE:0	LISTENING
TCP	192.168.1.33:49265	103.229.205.243:https	ESTABLISHED

netstat -b

The netstat -b command lists all the executables (applications) associated with each connection. Sometimes, applications may open multiple connections.

netstat -e

The netstat -e command generates a statistic of the network interface, which shows information like the number of bytes, unicast and non-unicast sent and received packets. You can also see discarded packets and errors and unknown protocols, which can you troubleshoot networking problems.

```
C:\Users\K M Abhijith>netstat -b
The requested operation requires elevation.

C:\Users\K M Abhijith>netstat -e
Interface Statistics

          Received          Sent
Bytes      1317589146    1499692775
Unicast packets    13295065    7846391
Non-unicast packets    5383    102956
Discards          0          0
Errors            0          0
Unknown protocols    0          0

C:\Users\K M Abhijith>
```

3. ipconfig

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

PARAMETERS:

/all: Displays the full TCP/IP configuration for all adapters. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.

/displaydns: Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.

/flushdns: Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.

/registerdns: Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a failed DNS name registration or resolve a dynamic update problem between a client and the DNS server without rebooting the client computer. The DNS settings in the advanced properties of the TCP/IP protocol determine which names are registered in DNS.

```
C:\Users\K M Abhijith>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-ILB31AE
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : hgu_lan

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : 04-92-26-1D-65-3B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-11
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c4ce:386:c0a0:f75%17(Preferred)
IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 621412391
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-51-CF-D1-04-92-26-1D-65-3B
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 48-F1-7F-04-07-82
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
```

```
C:\Users\K M Abhijith>
C:\Users\K M Abhijith>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::c4ce:386:c0a0:f75%17
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . : hgu_lan
    Link-local IPv6 Address . . . . . : fe80::fc84:9747:b0c8:3f89%4
    IPv4 Address. . . . . : 192.168.1.33
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
```

Other Networking Commands

1. Hostname Command

A very simple command that displays the host name of your machine. This is much quicker than going to the control **panel>system** route.

2. getmac Command

Another very simple command that shows the MAC address of your network interfaces

3.arp Command

This is used for showing the address resolution cache. This command must be used with a command line switch arp -a is the most common.

4. Nbtstat

Diagnostic tool for troubleshooting netBIOS problems.

5. Net Command

Used for managing users, service, shares etc..

```
H:\>net
The syntax of this command is:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

```
H:\>hostname
DESKTOP-ILB31AE
```

```
H:\>
```

```
H:\>nbtstat
```

```
Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).
```

```
NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]
```

-a (adapter status)	Lists the remote machine's name table given its name
-A (Adapter status)	Lists the remote machine's name table given its IP address.
-c (cache)	Lists NBT's cache of remote [machine] names and their IP addresses
-n (names)	Lists local NetBIOS names.
-r (resolved)	Lists names resolved by broadcast and via WINS
-R (Reload)	Purges and reloads the remote cache name table
-S (Sessions)	Lists sessions table with the destination IP addresses
-s (sessions)	Lists sessions table converting destination IP addresses to computer NETBIOS names.
-RR (ReleaseRefresh)	Sends Name Release packets to WINS and then, starts Refresh

```
RemoteName  Remote host machine name.
IP address  Dotted decimal representation of the IP address.
interval    Redisplays selected statistics, pausing interval seconds
            between each display. Press Ctrl+C to stop redisplaying
            statistics.
```

```
H:\>
```

```
H:\>getmac

Physical Address      Transport Name
=====
48-F1-7F-04-07-81    \Device\Tcpip_{083275F0-5D75-483E-9CA1-5D2B536909B7}
04-92-26-1D-65-3B    Media disconnected
48-F1-7F-04-07-85    Media disconnected
0A-00-27-00-00-11    \Device\Tcpip_{A74689BB-EA25-4EFA-8DC2-57AA7FC4E351}

H:\>arp -a

Interface: 192.168.1.33 --- 0x4
 Internet Address      Physical Address      Type
 192.168.1.1            14-a7-2b-83-03-34    dynamic
 192.168.1.255          ff-ff-ff-ff-ff-ff    static
 224.0.0.22              01-00-5e-00-00-16    static
 224.0.0.251             01-00-5e-00-00-fb    static
 224.0.0.252             01-00-5e-00-00-fc    static
 239.255.255.250        01-00-5e-7f-ff-fa    static
 255.255.255.255        ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0x11
 Internet Address      Physical Address      Type
 192.168.56.255         ff-ff-ff-ff-ff-ff    static
 224.0.0.22              01-00-5e-00-00-16    static
 224.0.0.251             01-00-5e-00-00-fb    static
 224.0.0.252             01-00-5e-00-00-fc    static
 239.255.255.250        01-00-5e-7f-ff-fa    static
```

LINUX

Ifconfig:

ifconfig is used to configure, or view the configuration of, a network interface.

```
root@kmabhijith-VirtualBox:~# ifconfig -s
Iface      MTU     RX-OK RX-ERR RX-DRP RX-OVR     TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3     1500      323      0      0 0       238      0      0 0      BMRU
lo        65536     178      0      0 0       178      0      0 0      LRU
```

```
root@kmabhijith-VirtualBox:~# ifconfig -v
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::a179:f201:9541:fa3c prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:2c:9c:0c txqueuelen 1000 (Ethernet)
            RX packets 323 bytes 252665 (252.6 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 238 bytes 34544 (34.5 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 178 bytes 15314 (15.3 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 178 bytes 15314 (15.3 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kmabhijith-VirtualBox:~# ifconfig -s
Iface      MTU     RX-OK RX-ERR RX-DRP RX-OVR      TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3    1500      323      0      0 0        238      0      0      0 BMRU
lo       65536      178      0      0 0        178      0      0      0 LRU
root@kmabhijith-VirtualBox:~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::a179:f201:9541:fa3c prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:2c:9c:0c txqueuelen 1000 (Ethernet)
            RX packets 305 bytes 250421 (250.4 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 215 bytes 32491 (32.4 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 168 bytes 14448 (14.4 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 168 bytes 14448 (14.4 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Traceroute:

traceroute command in Linux prints the route that a packet takes to reach the host.

```
root@kmabhijith-VirtualBox:~# traceroute google.com
traceroute to google.com (142.250.196.78), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2)  4.080 ms  3.998 ms  3.924 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
```

Netstat:

The network statistics (netstat) command is a networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network.

```
root@kmabhijith-VirtualBox:~# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
udp      0      0 kmabhijith-Virtu:bootpc _gateway:bootps      ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type      State         I-Node      Path
unix    2      [ ]     DGRAM           29915      /run/user/0/systemd/n
otify
unix    3      [ ]     DGRAM           15454      /run/systemd/notify
unix    2      [ ]     DGRAM           15468      /run/systemd/journal/
syslog
unix   15      [ ]     DGRAM           15478      /run/systemd/journal/
dev-log
unix    8      [ ]     DGRAM           15482      /run/systemd/journal/
socket
unix    3      [ ]     STREAM     CONNECTED    30870

root@kmabhijith-VirtualBox:~# netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
udp      0      0 localhost:domain        0.0.0.0:*
udp      0      0 kmabhijith-Virtu:bootpc _gateway:bootps      ESTABLISHED
udp      0      0 0.0.0.0:mdns          0.0.0.0:*
udp      0      0 0.0.0.0:36230        0.0.0.0:*
udp      0      0 0.0.0.0:631          0.0.0.0:*
udp6     0      0 [::]:mdns            [::]:*
udp6     0      0 [::]:45477         [::]:*
```

```

root@kmabhijith-VirtualBox:~# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 localhost:mysql          0.0.0.0:*            LISTEN
tcp      0      0 localhost:domain        0.0.0.0:*            LISTEN
tcp      0      0 localhost:ipp           0.0.0.0:*            LISTEN
tcp6     0      0 [::]:http              [::]:*               LISTEN
tcp6     0      0 ip6-localhost:ipp       [::]:*               LISTEN
udp      0      0 localhost:domain        0.0.0.0:*            LISTEN
udp      0      0 kmabhijith-Virtu:bootpc _gateway:bootps      ESTABLISHED
udp      0      0 0.0.0.0:mdns           0.0.0.0:*            LISTEN
udp      0      0 0.0.0.0:36230          0.0.0.0:*            LISTEN
udp      0      0 0.0.0.0:631            0.0.0.0:*            LISTEN
udp6     0      0 [::]:mdns             [::]:*               LISTEN
udp6     0      0 [::]:45477            [::]:*               LISTEN
raw6    0      0 [::]:ipv6-icmp         [::]:*               7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State      I-Node Path
root@kmabhijith-VirtualBox:~# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 localhost:mysql          0.0.0.0:*            LISTEN
tcp      0      0 localhost:domain        0.0.0.0:*            LISTEN
tcp      0      0 localhost:ipp           0.0.0.0:*            LISTEN
tcp6     0      0 [::]:http              [::]:*               LISTEN
tcp6     0      0 ip6-localhost:ipp       [::]:*               LISTEN
root@kmabhijith-VirtualBox:~# 

```

Nslookup:

Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record.

```

root@kmabhijith-VirtualBox:~# nslookup
> google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.196.78
Name:   google.com
Address: 2404:6800:4007:82b::200e

```

```
root@kmabhijith-VirtualBox:~# nslookup -type=any google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
google.com      mail exchanger = 40 alt3.aspmx.l.google.com.
google.com      mail exchanger = 50 alt4.aspmx.l.google.com.
google.com      mail exchanger = 30 alt2.aspmx.l.google.com.
google.com      mail exchanger = 10 aspmx.l.google.com.
google.com      mail exchanger = 20 alt1.aspmx.l.google.com.
google.com
    origin = ns1.google.com
    mail addr = dns-admin.google.com
    serial = 396194125
    refresh = 900
    retry = 900
    expire = 1800
    minimum = 60
Name:  google.com
Address: 2404:6800:4007:822::200e
Name:  google.com
Address: 172.217.167.142
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns4.google.com.
```

```
root@kmabhijith-VirtualBox:~# nslookup -type=soa google.com
Server:      127.0.0.53
Address:     127.0.0.53#53
```

Non-authoritative answer:

```
google.com
    origin = ns1.google.com
    mail addr = dns-admin.google.com
    serial = 396194125
    refresh = 900
    retry = 900
    expire = 1800
    minimum = 60
```

Authoritative answers can be found from:

```
root@kmabhijith-VirtualBox:~# nslookup -type=ns google.com
Server:      127.0.0.53
Address:     127.0.0.53#53
```

Non-authoritative answer:

```
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns2.google.com.
```

Authoritative answers can be found from:

Ping:

PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host.

```
root@kmabhijith-VirtualBox:~# ping aesajce.in
PING aesajce.in (103.120.179.46) 56(84) bytes of data.
64 bytes from newvps.greenmatrimony.com (103.120.179.46): icmp_seq=1 ttl=54 time
=80.1 ms
64 bytes from newvps.greenmatrimony.com (103.120.179.46): icmp_seq=2 ttl=54 time
=70.6 ms
64 bytes from newvps.greenmatrimony.com (103.120.179.46): icmp_seq=3 ttl=54 time
=69.8 ms
64 bytes from newvps.greenmatrimony.com (103.120.179.46): icmp_seq=4 ttl=54 time
=72.8 ms
64 bytes from newvps.greenmatrimony.com (103.120.179.46): icmp_seq=5 ttl=54 time
=70.3 ms
64 bytes from newvps.greenmatrimony.com (103.120.179.46): icmp_seq=6 ttl=54 time
=70.0 ms
64 bytes from newvps.greenmatrimony.com (103.120.179.46): icmp_seq=7 ttl=54 time
=70.6 ms
64 bytes from newvps.greenmatrimony.com (103.120.179.46): icmp_seq=8 ttl=54 time
```

Other Networking Commands

ip route

Use the IP route to print or display the routing table. The following command displays the contents of the routing table:

```
root@kmabhijith-VirtualBox:~# ip route show
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
root@kmabhijith-VirtualBox:~# █
```

nmap:

nmap ("Network Mapper") is a powerful utility used for network discovery, security auditing, and administration. Many system admins use it to determine which of their systems are online, and also for OS detection and service detection.

```
root@kmabhijith-VirtualBox:~# nmap 10.0.0.05
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-14 19:31 IST
Nmap scan report for 10.0.0.5
Host is up (0.0011s latency).
All 1000 scanned ports on 10.0.0.5 are filtered

Nmap done: 1 IP address (1 host up) scanned in 4.25 seconds
```

iperf:

While ping verifies the availability of a host, iPerf helps analyze and measure network performance between two hosts. With iPerf, you open a connection between two hosts and send some data. iPerf then shows the bandwidth available between the two hosts.

```
root@kmabhijith-VirtualBox:~# iperf -s
-----
Server listening on TCP port 5001
TCP window size: 128 KByte (default)
-----
```

dig:

dig (Domain Information Groper) is a flexible tool for interrogating DNS name servers.

It performs DNS lookups and displays the answers that are returned from the name servers.

```
root@kmabhijith-VirtualBox:~# dig aesajce.in

; <>> DiG 9.16.1-Ubuntu <>> aesajce.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45933
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;aesajce.in.           IN      A

;; ANSWER SECTION:
aesajce.in.        8899    IN      A      103.120.179.46

;; Query time: 27 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Sep 14 19:40:30 IST 2021
;; MSG SIZE  rcvd: 55
```

telnet:

telnet connect destination's host and port via a telnet protocol if a connection establishes means connectivity between two hosts is working fine.

```
root@kmabhijith-VirtualBox:~# telnet aesajce.in 443
Trying 103.120.179.46...
Connected to aesajce.in.
Escape character is '^]'.
Connection closed by foreign host.
```

LAMP INSTALLATION PROCEDURE

Install Apache2

Update your system:

```
sudo apt update
```

Install Apache using apt:

```
sudo apt install apache2
```

Confirm that Apache is now running with the following command:

```
sudo systemctl status apache2
```

```
root@kmabhijith-VirtualBox:~# sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-09-28 21:05:10 IST; 2min 0s ago
     Docs: https://httpd.apache.org/docs/2.4/
 Main PID: 6237 (apache2)
    Tasks: 55 (limit: 2312)
   Memory: 5.0M
      CGroup: /system.slice/apache2.service
              ├─6237 /usr/sbin/apache2 -k start
              ├─6239 /usr/sbin/apache2 -k start
              └─6240 /usr/sbin/apache2 -k start

Sep 28 21:05:10 kmabhijith-VirtualBox systemd[1]: Starting The Apache HTTP Server...
Sep 28 21:05:10 kmabhijith-VirtualBox apachectl[6236]: AH00558: apache2: Could not reliably determine
Sep 28 21:05:10 kmabhijith-VirtualBox systemd[1]: Started The Apache HTTP Server.
lines 1-15/15 (END)
```

If it is not working !

```
sudo systemctl stop apache2 # to stop if running
sudo systemctl start apache2 # to start if not running
```

Once installed, test by accessing your server's IP in your browser:

```
http://127.0.0.1/
http://localhost/
```

OUTPUT :



Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

Install mariadb

```
sudo apt install mariadb-server mariadb-client  
  
sudo systemctl status mysql    # to check status  
  
sudo systemctl start mysql    # if not running  
  
sudo mysql_secure_installation # Secure your newly installed MariaDB service
```

```
root@kmabhijith-VirtualBox:~# sudo systemctl status mysql  
● mariadb.service - MariaDB 10.3.31 database server  
  Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)  
  Active: active (running) since Tue 2021-09-28 20:44:50 IST; 25min ago  
    Docs: man:mysqld(8)  
          https://mariadb.com/kb/en/library/systemd/  
 Main PID: 672 (mysqld)  
   Status: "Taking your SQL requests now..."  
     Tasks: 30 (limit: 2312)  
   Memory: 69.4M  
    CGroup: /system.slice/mariadb.service  
           └─672 /usr/sbin/mysqld
```

Install PHP and commonly used modules

```
sudo apt install php libapache2-mod-php php-opcache php-cli php-gd  
php-curl php-mysql
```

```
sudo systemctl restart apache2
```

Test PHP Processing on Web Server

```
sudo nano /var/www/html/phpinfo.php
```

Inside the file, type in the valid PHP code:

```
<?php  
    phpinfo();  
?>
```

Press CTRL + X to save and close the file. Press y and ENTER to confirm
Open a browser and type in your IP address/phpinfo.php

```
http://127.0.0.1/phpinfo.php
```

OUTPUT :

PHP Version 7.4.3	
System	Linux kmabhijith-VirtualBox 5.11.0-27-generic #29~20.04.1-Ubuntu SMP Wed Aug 11 15:58:17 UTC 2021 x86_64
Build Date	Aug 13 2021 05:39:12
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqlind.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/15-xml.ini, /etc/php/7.4/apache2/conf.d/20-bz2.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-dom.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-isbn.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-

Install phpmyadmin

```
sudo apt install phpmyadmin php-mbstring php-zip php-gd php-json php-curl
```

```
sudo systemctl restart apache2
```

Open a browser : <http://localhost/phpmyadmin>

username : root

password : yourpasswordIf phpmyadmin page not found :

```
nano /etc/apache2/apache2.conf
```

Add this line to last of the file.

Press CTRL + X to save and close the file. Press y and ENTER to confirm

```
Include /etc/phpmyadmin/apache.conf
```

restart apache2 - now try : <http://localhost/phpmyadmin>

```
sudo systemctl restart apache2
```

If any problem for login run the following command

```
sudo mysql
```

```
ALTER USER root@localhost IDENTIFIED BY "yourpassword";
```

OUTPUT :

The image shows two screenshots of the phpMyAdmin interface.

The top screenshot is the "Welcome to phpMyAdmin" page. It features the phpMyAdmin logo (a sailboat icon) and a "Language" dropdown set to "English". Below it is a "Log in" form with "Username" set to "root" and "Password" set to "....".

The bottom screenshot shows the main database structure view. The left sidebar lists databases: "New", "information_schema", "mysql", "performance_schema", "phpmyadmin", and "test". The "test" database is selected. The main area displays the "Structure" tab for the "user" table. The table has one row and one column, both labeled "user". The table structure is shown with columns: "Rows", "Type", "Collation", "Size", and "Overhead". The data is summarized as "1 InnoDB utf8mb4_general_ci 16.8 KB" and "1 InnoDB utf8mb4_general_ci 16.8 KB 0 B". Below the table, there are "Create table" and "Data dictionary" buttons.

ANSIBLE INSTALLATION

INSTALLATION:

STEP 1: sudo apt install ansible

```
root@kmabhijith-VirtualBox:~# apt install ansible
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27 linux-image-5.11.0-27-generic
  linux-modules-5.11.0-27-generic linux-modules-extra-5.11.0-27-generic
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  ieee-data python3-argcomplete python3-crypto python3-dnspython python3-jinja2 python3-jmespath
  python3-kerberos python3-libcloud python3-lockfile python3-markupsafe python3-netaddr python3-ntlm-auth
  python3-requests-kerberos python3-requests-ntlm python3-selinux python3-winrm python3-xmldict
Suggested packages:
  cowsay sshpass python-jinja2-doc python-lockfile-doc ipython3 python-netaddr-docs
The following NEW packages will be installed:
  ansible ieee-data python3-argcomplete python3-crypto python3-dnspython python3-jinja2 python3-jmespath
  python3-kerberos python3-libcloud python3-lockfile python3-markupsafe python3-netaddr python3-ntlm-auth
  python3-requests-kerberos python3-requests-ntlm python3-selinux python3-winrm python3-xmldict
0 upgraded, 18 newly installed, 0 to remove and 181 not upgraded.
Need to get 9,753 kB of archives.
After this operation, 90.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] ■
```

```
if x is 0 or x is 1:
/usr/lib/python3/dist-packages/jmespath/visitor.py:32: SyntaxWarning: "is" with a literal. Did you mean "=="?
  if x is 0 or x is 1:
/usr/lib/python3/dist-packages/jmespath/visitor.py:34: SyntaxWarning: "is" with a literal. Did you mean "=="?
  elif y is 0 or y is 1:
/usr/lib/python3/dist-packages/jmespath/visitor.py:34: SyntaxWarning: "is" with a literal. Did you mean "=="?
  elif y is 0 or y is 1:
/usr/lib/python3/dist-packages/jmespath/visitor.py:260: SyntaxWarning: "is" with a literal. Did you mean "=="?
  if original_result is 0:
Setting up python3-requests-kerberos (0.12.0-2) ...
Setting up ieee-data (20180805.1) ...
Setting up python3-dnspython (1.16.0-1build1) ...
Setting up python3-selinux (3.0-1build2) ...
Setting up python3-crypto (2.6.1-13ubuntu2) ...
Setting up python3-argcomplete (1.8.1-1.3ubuntu1) ...
Setting up python3-requests-ntlm (1.1.0-1) ...
Setting up python3-libcloud (2.8.0-1) ...
Setting up python3-netaddr (0.7.19-3) ...
/usr/lib/python3/dist-packages/netaddr/strategy/__init__.py:189: SyntaxWarning: "is not" with a literal. Did you
mean "!="?
  if word_sep is not '':
Setting up python3-winrm (0.3.0-2) ...
Setting up ansible (2.9.6+dfsg-1) ...
■
Progress: [ 97%] [#####
Setting up python3-requests-kerberos (0.12.0-2) ...
Setting up ieee-data (20180805.1) ...
Setting up python3-dnspython (1.16.0-1build1) ...
Setting up python3-selinux (3.0-1build2) ...
Setting up python3-crypto (2.6.1-13ubuntu2) ...
Setting up python3-argcomplete (1.8.1-1.3ubuntu1) ...
Setting up python3-requests-ntlm (1.1.0-1) ...
Setting up python3-libcloud (2.8.0-1) ...
Setting up python3-netaddr (0.7.19-3) ...
/usr/lib/python3/dist-packages/netaddr/strategy/__init__.py:189: SyntaxWarning: "is not" with a literal. Did you
mean "!="?
  if word_sep is not '':
Setting up python3-winrm (0.3.0-2) ...
Setting up ansible (2.9.6+dfsg-1) ...
Processing triggers for man-db (2.9.1-1) ...
root@kmabhijith-VirtualBox:~# ■
```

CHECK INSTALLATION :

STEP 2: ansible --version

```
root@kmabhijith-VirtualBox:~# ansible --version
ansible [core 2.11.5]
  config file = /etc/ansible/ansible.cfg
  configured module search path = ['/root/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/local/lib/python3.8/dist-packages/ansible
  ansible collection location = /root/.ansible/collections:/usr/share/ansible/collections
  executable location = /usr/local/bin/ansible
  python version = 3.8.10 (default, Jun  2 2021, 10:49:15) [GCC 9.4.0]
  jinja version = 3.0.1
  libyaml = True
root@kmabhijith-VirtualBox:~#
```

ANALYZING NETWORK PACKET STREAM USING TCPDUMP

tcpdump

tcpdump is a most powerful and widely used command-line packets sniffer or package analyzer tool which is used to capture or filter TCP/IP packets that are received or transferred over a network on a specific interface.

1. **tcpdump -D** : Print all available interfaces for capture

```
root@kmabhijith-VirtualBox:~# tcpdump -D
1.enp0s3 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
```

2. **tcpdump -XX -i eth0** :

The following command with option -XX capture the data of each packet, including its link level header in HEX and ASCII format.

```
root@kmabhijith-VirtualBox:~# tcpdump -xx -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
13:02:55.720558 IP 32.121.122.34.bc.googleusercontent.com.http > kmabhijith-VirtualBox.41412: Flags [S.], seq 92001, ack 3194587439, win 65535, options [mss 1460], length 0
    0x0000: 0800 272c 9c0c 5254 0012 3502 0800 4500
    0x0010: 002c 21d4 0000 4006 b14f 227a 7920 0a00
    0x0020: 020f 0050 a1c4 0095 6a01 be69 892f 6012
    0x0030: ffff 9c29 0000 0204 05b4 0000
13:02:55.720607 IP kmabhijith-VirtualBox.41412 > 32.121.122.34.bc.googleusercontent.com.http: Flags [R], seq 4587439, win 0, length 0
    0x0000: 5254 0012 3502 0800 272c 9c0c 0800 4500
    0x0010: 0028 0000 4000 4006 9327 0a00 020f 227a
    0x0020: 7920 a1c4 0050 be69 892f 0000 0000 5004
    0x0030: 0000 1e8a 0000
13:02:55.722591 IP kmabhijith-VirtualBox.51660 > ns3.bliss.in.domain: 38223+ [1au] PTR? 15.2.0.10.in-addr.arpa
51)
    0x0000: 5254 0012 3502 0800 272c 9c0c 0800 4500
    0x0010: 004f c0b9 4000 4011 ca5e 0a00 020f 2d7d
    0x0020: 75fa c9cc 0035 003b af2d 954f 0100 0001
    0x0030: 0000 0000 0001 0231 3501 3201 3002 3130
    0x0040: 0769 6e2d 6164 6472 0461 7270 6100 000c
```

3. **tcpdump -n -i enp0s3** :

To capture packets for a specific interface, run the following command with option -n.

```
root@kmabhijith-VirtualBox:~# tcpdump -n -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
13:17:52.481333 IP 10.0.2.15.42562 > 45.125.117.250.53: 46721+ [1au] A? connectivity-check.u
13:17:52.521974 IP 45.125.117.250.53 > 10.0.2.15.42562: 46721 3/0/1 A 34.122.121.32, A 35.22
11.17 (106)
13:17:52.523168 IP 10.0.2.15.51284 > 35.232.111.17.80: Flags [S], seq 2972868629, win 64240,
ackOK,TS val 2365974444 ecr 0,nop,wscale 7], length 0
13:17:52.777512 IP 35.232.111.17.80 > 10.0.2.15.51284: Flags [S.], seq 14208001, ack 2972868
ons [mss 1460], length 0
13:17:52.777578 IP 10.0.2.15.51284 > 35.232.111.17.80: Flags [..], ack 1, win 64240, length 0
13:17:52.778198 IP 10.0.2.15.51284 > 35.232.111.17.80: Flags [P.], seq 1:88, ack 1, win 6424
GET / HTTP/1.1
13:17:52.778738 IP 35.232.111.17.80 > 10.0.2.15.51284: Flags [..], ack 88, win 65535, length 0
13:17:53.029103 IP 35.232.111.17.80 > 10.0.2.15.51284: Flags [P.], seq 1:149, ack 88, win 65
P: HTTP/1.1 204 No Content
```

4. tcpdump -i ens0p :

The command screen will scroll up until you interrupt and when we execute the tcpdump command it will captures from all the interfaces, however with -i switch only capture from the desired interface.

```
root@kmabhijith-VirtualBox:~# tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
07:12:59.980509 IP kmabhijith-VirtualBox.41534 > 84.170.224.35.bc.googleusercontent.com.http: Flags [S], seq 53
375802, win 64240, options [mss 1460,sackOK,TS val 2466855538 ecr 0,nop,wscale 7], length 0
07:12:59.983240 IP kmabhijith-VirtualBox.53989 > ns3.blss.in.domain: 65524+ [1au] PTR? 84.170.224.35.in-addr.an
a. (55)
07:13:00.264031 IP 84.170.224.35.bc.googleusercontent.com.http > kmabhijith-VirtualBox.41534: Flags [S.], seq 2
168001, ack 532375803, win 65535, options [mss 1460], length 0
07:13:00.264074 IP kmabhijith-VirtualBox.41534 > 84.170.224.35.bc.googleusercontent.com.http: Flags [.], ack 1,
win 64240, length 0
07:13:00.264301 IP kmabhijith-VirtualBox.41534 > 84.170.224.35.bc.googleusercontent.com.http: Flags [P.], seq 1
, ack 1, win 64240, length 87, HTTP/1.1
```

SHELL SCRIPTING

SHELL SCRIPTING

1. Write a shell script to ask your name, and college name and print it on the screen.

```
#!/bin/bash
echo "enter your name";read you;
echo "enter college name"; read college;
echo $you;
echo $college;
```

Output:

```
root@kmabhijith-VirtualBox:~# ./1.sh
enter your name
abhijith
enter college name
amal jyothi
abhijith
amal jyothi
root@kmabhijith-VirtualBox:~#
```

2. Write a shell script to set a value for a variable and display it on command line interface.

```
#!/bin/bash
((sum=10))
echo "number is $sum"
```

Output:

```
root@kmabhijith-VirtualBox:~# vi 2.sh
root@kmabhijith-VirtualBox:~# chmod +x 2.sh
root@kmabhijith-VirtualBox:~# ./2.sh
number is 10
root@kmabhijith-VirtualBox:~#
```

3. Write a shell script to perform addition, subtraction, multiplication, division with two numbers that is accepted from user.

```
#!/bin/bash
echo "enter two numbers";
read a b;
echo "addition $((a+b))";
echo "subtraction $((a-b))";
echo "division $((a/b))";
echo "multiplication $((a*b))";
~
```

Output:

```
root@kmabhijith-VirtualBox:~# vi 3.sh
root@kmabhijith-VirtualBox:~# ./3.sh
enter two numbers
19 6
addition 25
subtraction 13
division 3
multiplication 114
root@kmabhijith-VirtualBox:~#
```

4. Write a shell script to check the value of a given number and display whether the number is found or not.

```
#!/bin/bash
echo "enter a number"
read a
if [[ $a -eq 10 ]]
then
    echo "number found"
else
    echo "number not found"
fi
~
```

Output:

```
root@kmabhijith-VirtualBox:~# ./4.sh
enter a number
10
number found
root@kmabhijith-VirtualBox:~# ./4.sh
enter a number
2
number not found
root@kmabhijith-VirtualBox:~#
```

5. Write a shell script to display current date, calendar.

```
#!/bin/bash
echo "$(date)";
echo "calnder :";
cal
```

Output:

```
root@kmabhijith-VirtualBox:~# vi 5.sh
root@kmabhijith-VirtualBox:~# ./5.sh
bash: ./5.sh: Permission denied
root@kmabhijith-VirtualBox:~# chmod +x 5.sh
root@kmabhijith-VirtualBox:~# ./5.sh
Saturday 02 October 2021 03:05:43 PM IST
calnder :
      October 2021
Su Mo Tu We Th Fr Sa
                  1  2
 3  4  5  6  7  8  9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
31
root@kmabhijith-VirtualBox:~#
```

6. Write a shell script to check a number is even or odd.

```
#!/bin/bash
echo "enter a number";
read a;
if [[ $((a%2)) -eq 0 ]]
then
    echo "$a is even";
else
    echo "$a is odd";
fi
```

Output:

```
root@kmabhijith-VirtualBox:~# vi 6.sh
root@kmabhijith-VirtualBox:~# ./6.sh
enter a number
10
10 is even
root@kmabhijith-VirtualBox:~# ./6.sh
enter a number
5
5 is odd
root@kmabhijith-VirtualBox:~#
```

7. Write a shell script to check a number is greater than, less than or equal to another number.

```
#!/bin/bash
echo "enter a number";
read a;
if [[ $a -gt 10 ]]
then
    echo "number is grater than 10";
fi

if [[ $a -le 10 ]]
then
    echo "number is less than or equal to 10"
fi
```

Output:

```
root@kmabhijith-VirtualBox:~# vi 7.sh
root@kmabhijith-VirtualBox:~# ./7.sh
enter a number
12
number is grater than 10
root@kmabhijith-VirtualBox:~# ./7.sh
enter a number
9
number is less than or equal to 10
root@kmabhijith-VirtualBox:~#
```

8. Write a shell script to find the sum of first 10 numbers.

```
#!/bin/bash
sum=0
n=10
echo "sum of first 10 numbers";
for ((i=1;i <= $n;i++ ))
do
    sum=$((sum+i))
done
echo "$sum";
~
```

Output:

```
root@kmabhijith-VirtualBox:~# vi 8.sh
root@kmabhijith-VirtualBox:~# ./8.sh
sum of first 10 numbers
55
root@kmabhijith-VirtualBox:~#
```

9. Write a shell script to find the sum, the average and the product of the four integers entered.

```
#!/bin/bash
echo "enter four numbers";
read a b c d;
sum=$((a+b+c+d))
echo "sum is $sum";
avg=$((sum/4))
echo "average is $avg";
pro=$((a*b*c*d))
echo "product is $pro";
~
```

Output:

```
root@kmabhijith-VirtualBox:~# vi 9.sh
root@kmabhijith-VirtualBox:~# ./9.sh
enter four numbers
10 34 56 33
sum is 133
average is 33
product is 628320
root@kmabhijith-VirtualBox:~#
```

10. Write a shell script to find the smallest of three numbers.

```
#!/bin/bash
echo "enter three numbers"
read a b c;
if [[ $a -lt $b ]]
then
    echo "$a is smaller";
elif [[ $b -lt $c ]]
then
    echo "$b is smaller";
else
    echo "$c is smaller";
fi
~
```

Output:

```
root@kmabhijith-VirtualBox:~# vi 10.sh
root@kmabhijith-VirtualBox:~# ./10.sh
enter three numbers
4 3 6
3 is smaller
root@kmabhijith-VirtualBox:~# ./10.sh
enter three numbers
5 7 9
5 is smaller
root@kmabhijith-VirtualBox:~# ./10.sh
enter three numbers
9 7 0
0 is smaller
root@kmabhijith-VirtualBox:~#
```

11. Write a shell program to find factorial of given number.

```
#!/bin/bash
echo "enter a number";
read a;
fact=1;
while [ $a -ge 1 ]
do
fact=$((fact * $a))
a=$((a-1))
done
echo "factorial is $fact";
```

~

Output:

```
root@kmabhijith-VirtualBox:~/# ./11.sh
enter a number
5
factorial is 120
root@kmabhijith-VirtualBox:~/#
```

12. Write a shell program to check a number is palindrome or not.

```
#!/bin/bash
echo "enter a number";
read a;
pali=$a;
num=0;
while [ $a -gt 0 ]
do
    digit=$((a%10));
    num=$((num*10))+$digit;
    a=$((a/10));

done
if [[ $num -eq $pali ]]
then
    echo "$pali is palindrome";
else
    echo "$pali is not palindrome";
fi
~
```

Output:

```
root@kmabhijith-VirtualBox:~# vi 12.sh
root@kmabhijith-VirtualBox:~# ./12.sh
enter a number
121
121 is palindrome
root@kmabhijith-VirtualBox:~# ./12.sh
enter a number
231
231 is not palindrome
root@kmabhijith-VirtualBox:~#
```

13. Write a shell script to find the average of the numbers entered in command line.

```
#!/bin/bash
echo "enter number of numbers";
read n;
sum=0;
echo "enter numbers";
for((i=0;i<n;i++))
do
    read a;
    sum=$((sum + a));
done
avg=$((sum/n));
echo "average is $avg"
```

Output:

```
root@kmabhijith-VirtualBox:~# vi 13.sh
root@kmabhijith-VirtualBox:~# ./13.sh
enter number of numbers
5
enter numbers
23
12
45
43
23
average is 29
root@kmabhijith-VirtualBox:~#
```

14. Write a shell program to find the sum of all the digits in a number.

```
#!/bin/bash
echo "enter a number";
read a;
pali=$a;
num=0;
while [ $a -gt 0 ]
do
    digit=$((a%10));
    num=$((digit+num));
    a=$((a/10));
done
echo "sum of digits of $pali is $num";
~
```

Output:

```
root@kmabhijith-VirtualBox:~# vi 14.sh
root@kmabhijith-VirtualBox:~# ./14.sh
enter a number
123
sum of digits of 123 is 6
```

15. Write a shell Script to check whether given year is leap year or not.

```
#!/bin/bash
echo "enter the year";
read a;
year=$((a%4));
if [[ $year -eq 0 ]]
then
    echo "$a is leap year";
else
    echo "$a is a normal year";
fi
```

Output:

```
root@kmabhijith-VirtualBox:~# vi 15.sh
root@kmabhijith-VirtualBox:~# ./15.sh
enter the year
2012
2012 is leap year
root@kmabhijith-VirtualBox:~# ./15.sh
enter the year
2007
2007 is a normal year
root@kmabhijith-VirtualBox:~#
```

INSTALLATION AND DEPLOYMENT OF DOCKER

DOCKER INSTALLATION

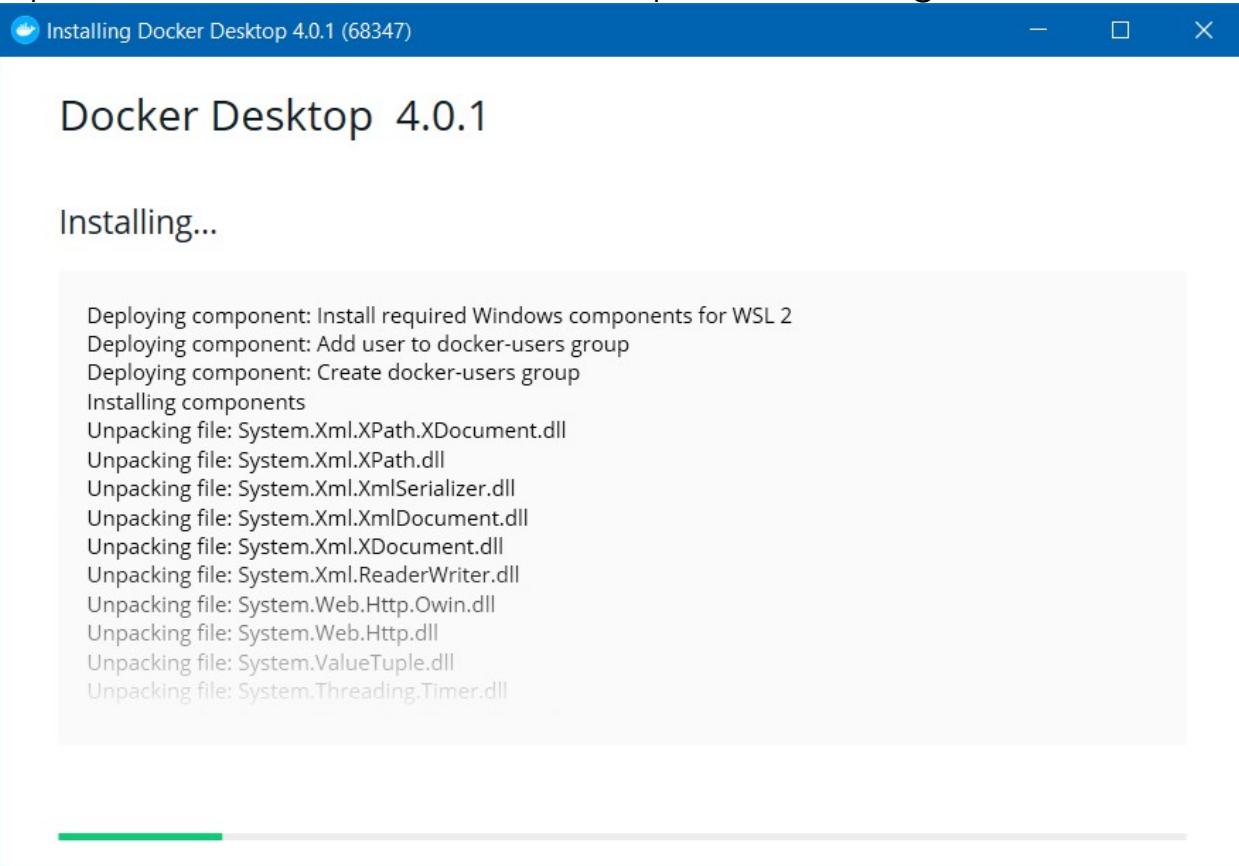
Step-I

Download Docker Desktop installer for Windows from <https://desktop.docker.com/win/main/amd64/Docker%20Desktop%20Installer.exe>

 Docker Desktop Installer	9/29/2021 2:51 PM	Application	522,896 KB
---	-------------------	-------------	------------

Step-II

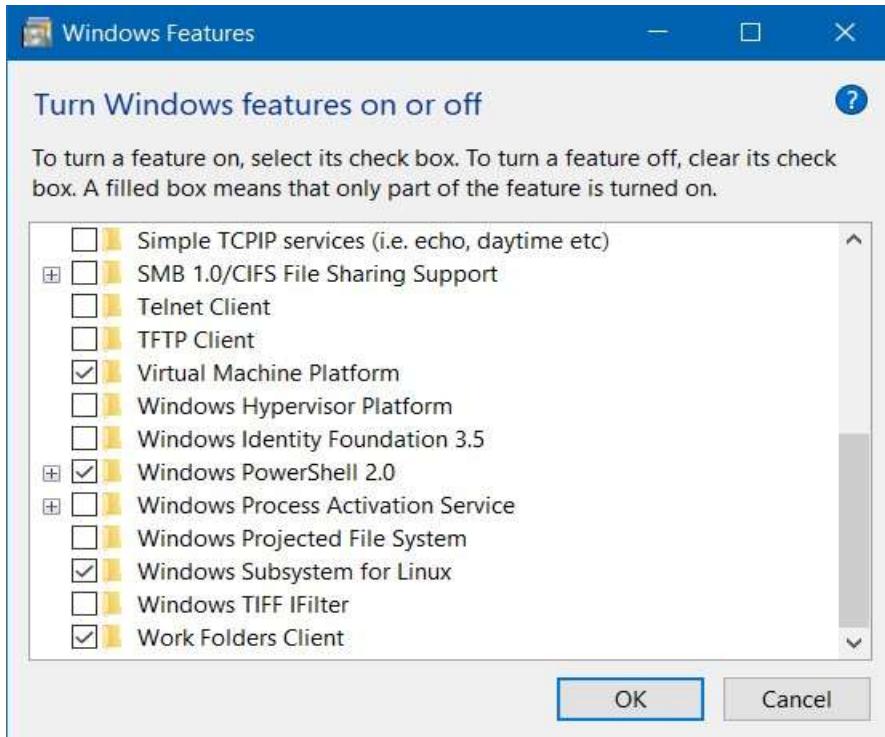
Open the .exe file and follow the steps after clicking install button.



Step-III

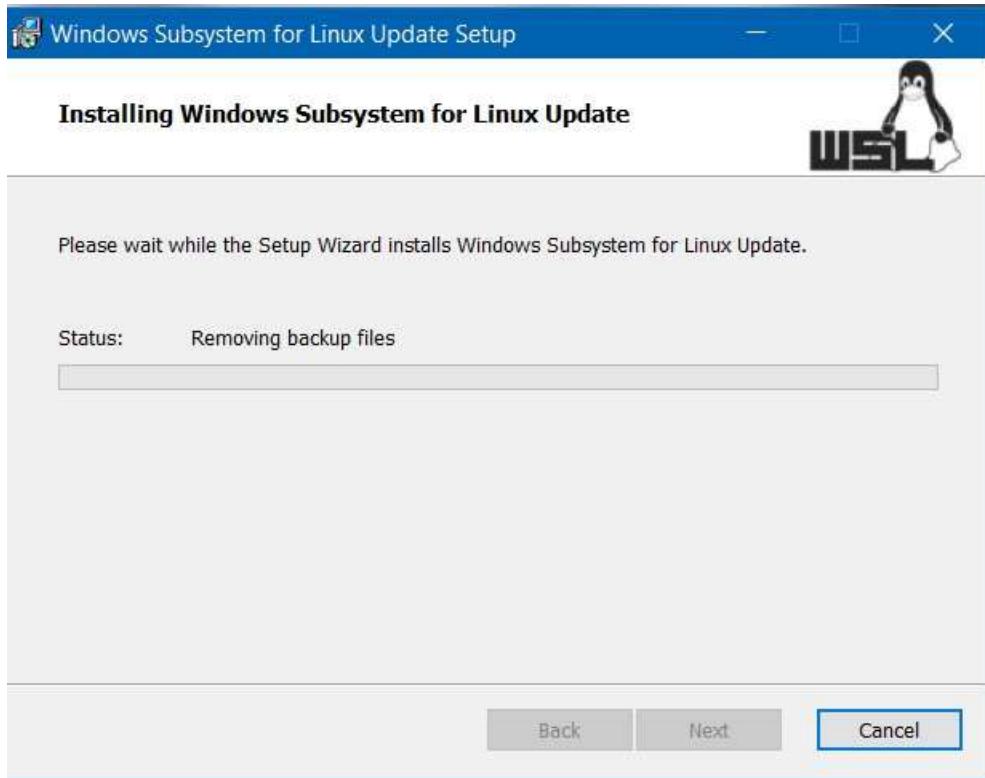
Once installed go to programs and features and click turn on windows features on or off

Scroll to the bottom and select windows subsystem for Linux



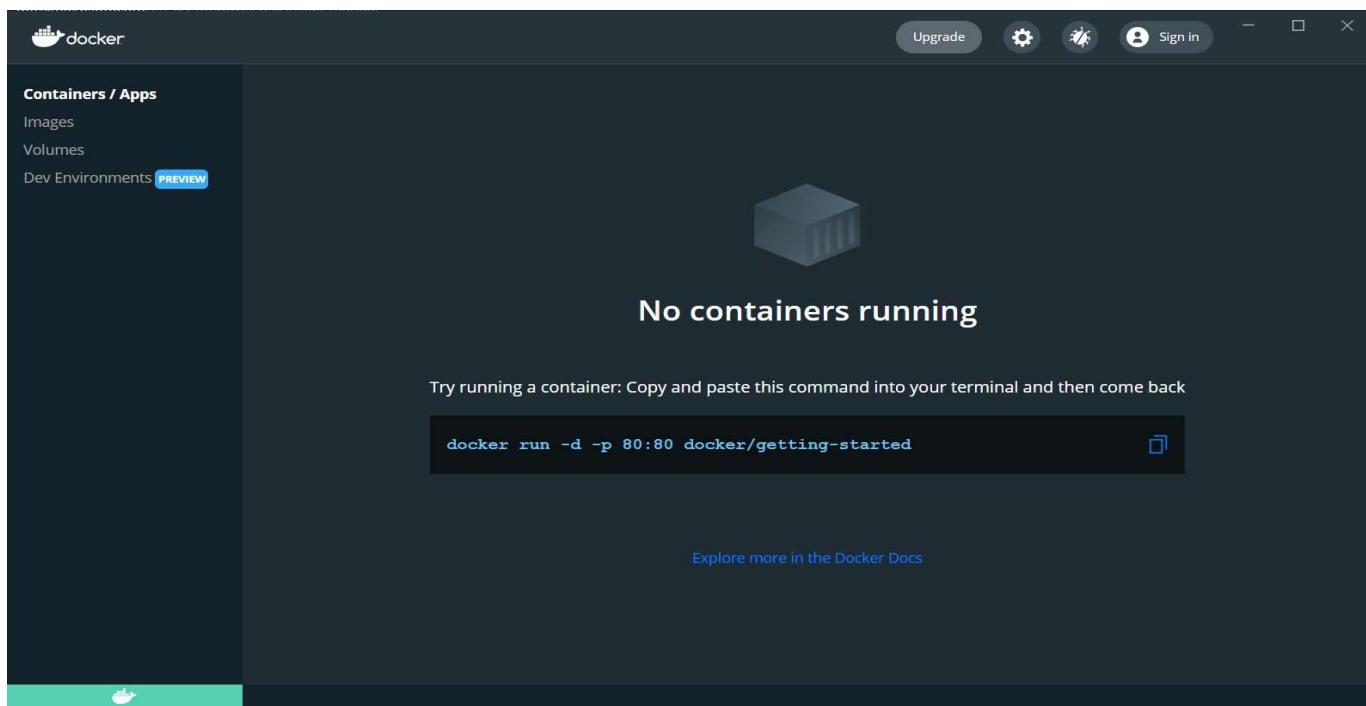
Step-IV

If any WSL 2 error occurs download windows subsystem for linux update package and install the .exe file, after the installation restart the windows device.



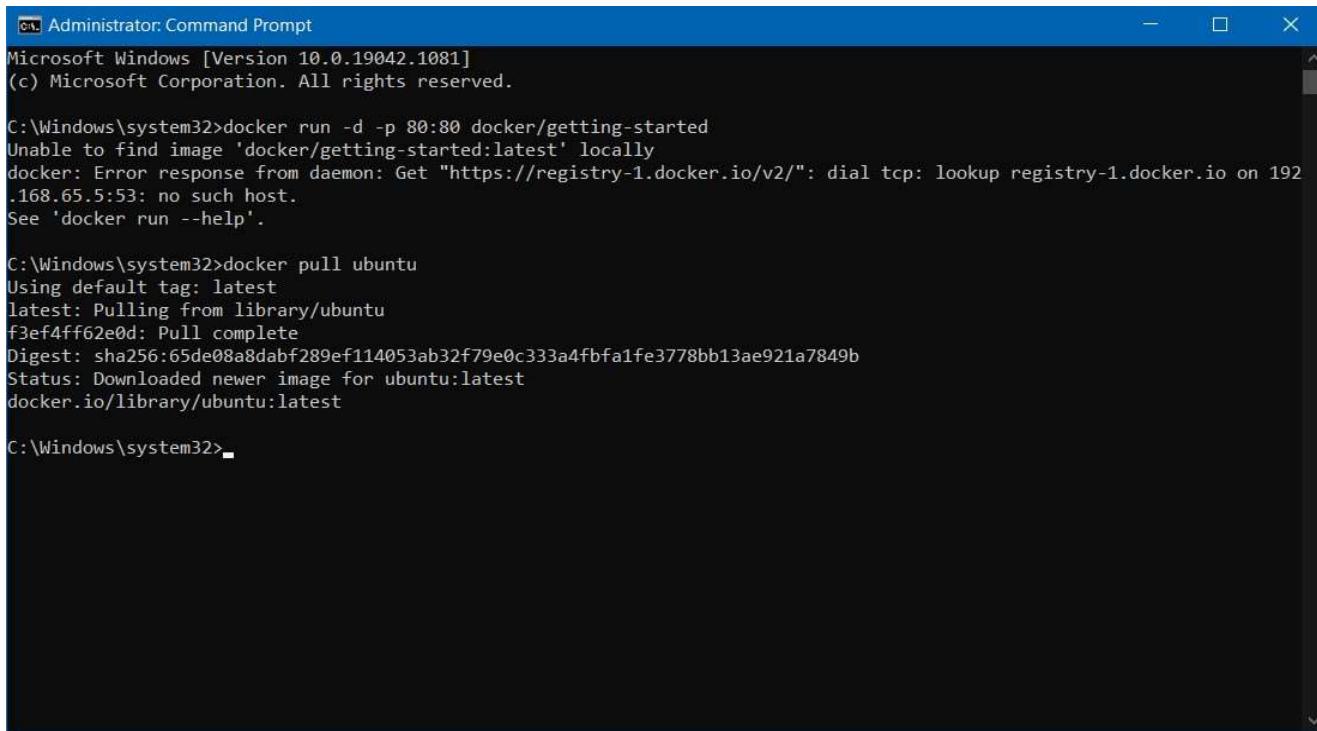
Step-V

Once installed, open the docker desktop app, and signin using the dockerID



Step-VI

Now pull any image from docker hub using the docker pull command in the command prompt (eg: docker pull ubuntu)



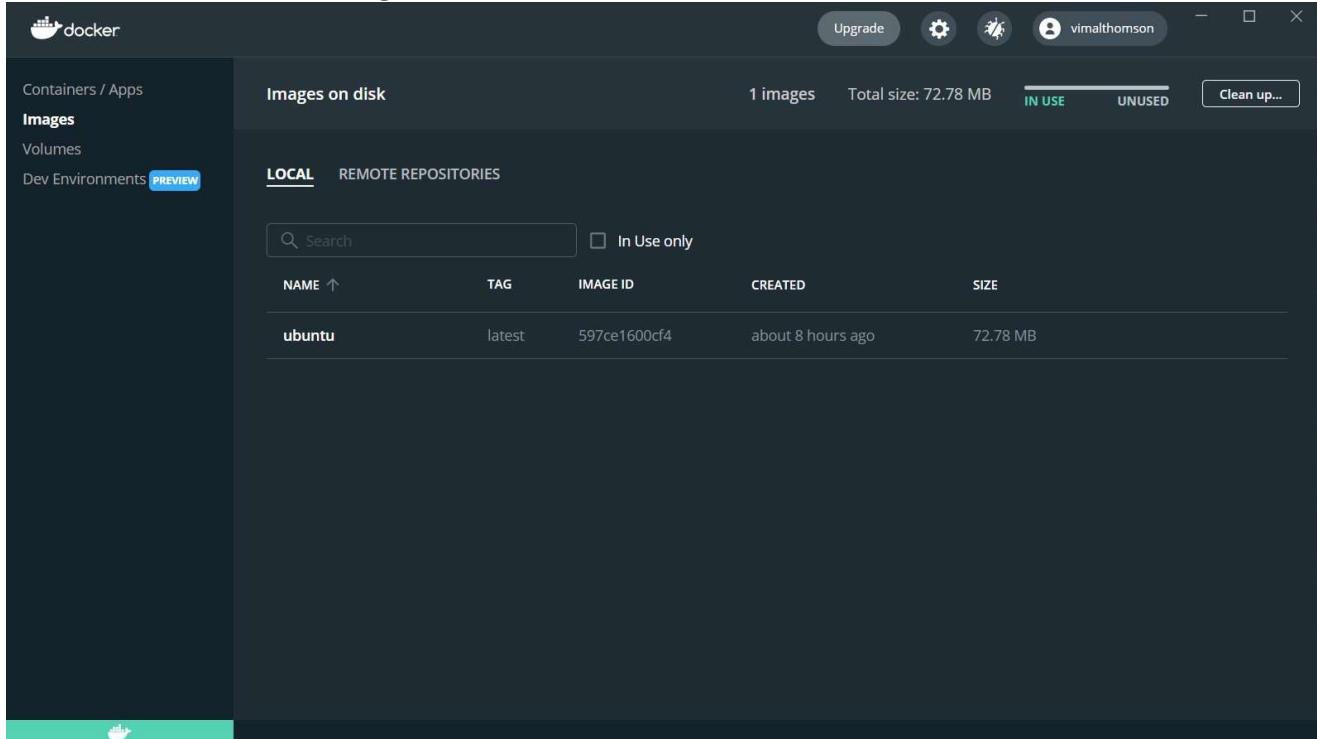
```
C:\ Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.1081]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>docker run -d -p 80:80 docker/getting-started
Unable to find image 'docker/getting-started:latest' locally
docker: Error response from daemon: Get "https://registry-1.docker.io/v2/": dial tcp: lookup registry-1.docker.io on 192.168.65.5:53: no such host.
See 'docker run --help'.

C:\Windows\system32>docker pull ubuntu
Using default tag: latest
latest: Pulling from library/ubuntu
f3ef4ff62e0d: Pull complete
Digest: sha256:65de08a8dabf289ef114053ab32f79e0c333a4fbfa1fe3778bb13ae921a7849b
Status: Downloaded newer image for ubuntu:latest
docker.io/library/ubuntu:latest

C:\Windows\system32>
```

Now in the images tab an image of ubuntu will be displayed, we can run the ubuntu instance using the cli.



ANALYZING NETWORK PACKET STREAM USING NC AND WIRESHARK

Wireshark installation

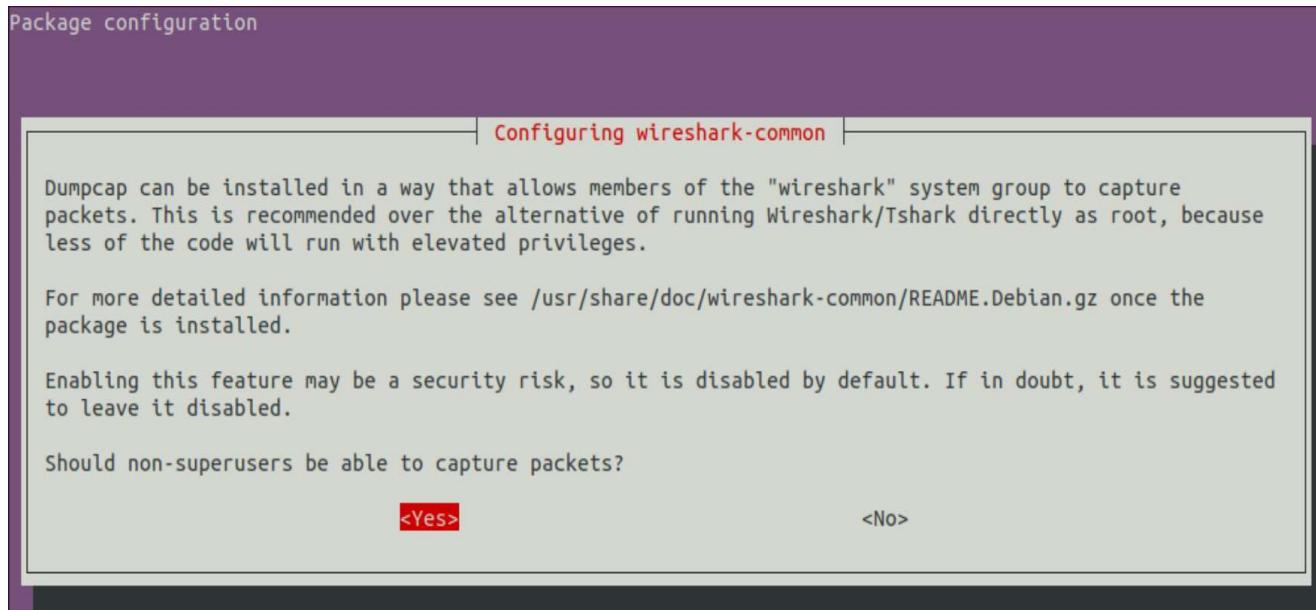
1. Sudo apt-get install wireshark

```
root@kmabhijith-VirtualBox:~# sudo apt-get install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27 linux-image-5.11.0-27-generic
  linux-modules-5.11.0-27-generic linux-modules-extra-5.11.0-27-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libc-ares2 libdouble-conversion3 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediasupports5 libqt5multimediamodels5 libqt5multimediacounters5 libqt5multimediacapabilities5 libqt5multimediacaptures5 libqt5multimediacards5 libqt5multimediacardsupports5 libqt5multimediacounterssupport5 libqt5multimediacountersmodels5 libqt5multimediacardsmodels5 libqt5multimediacardsupportssupport5 libqt5multimediacardsupportsmode
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate geoip-database geoip-database-
  libjs-leaflet libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libdouble-conversion3 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediasupports5 libqt5multimediamodels5 libqt5multimediacounters5 libqt5multimediacapabilities5 libqt5multimediacaptures5 libqt5multimediacards5 libqt5multimediacardsupports5 libqt5multimediacounterssupport5 libqt5multimediacountersmodels5 libqt5multimediacardsmodels5 libqt5multimediacardsupportssupport5 libqt5multimediacardsupportsmode
  qttranslations5-l10n wireshark wireshark-common wireshark-qt
0 upgraded, 29 newly installed, 0 to remove and 181 not upgraded.
```

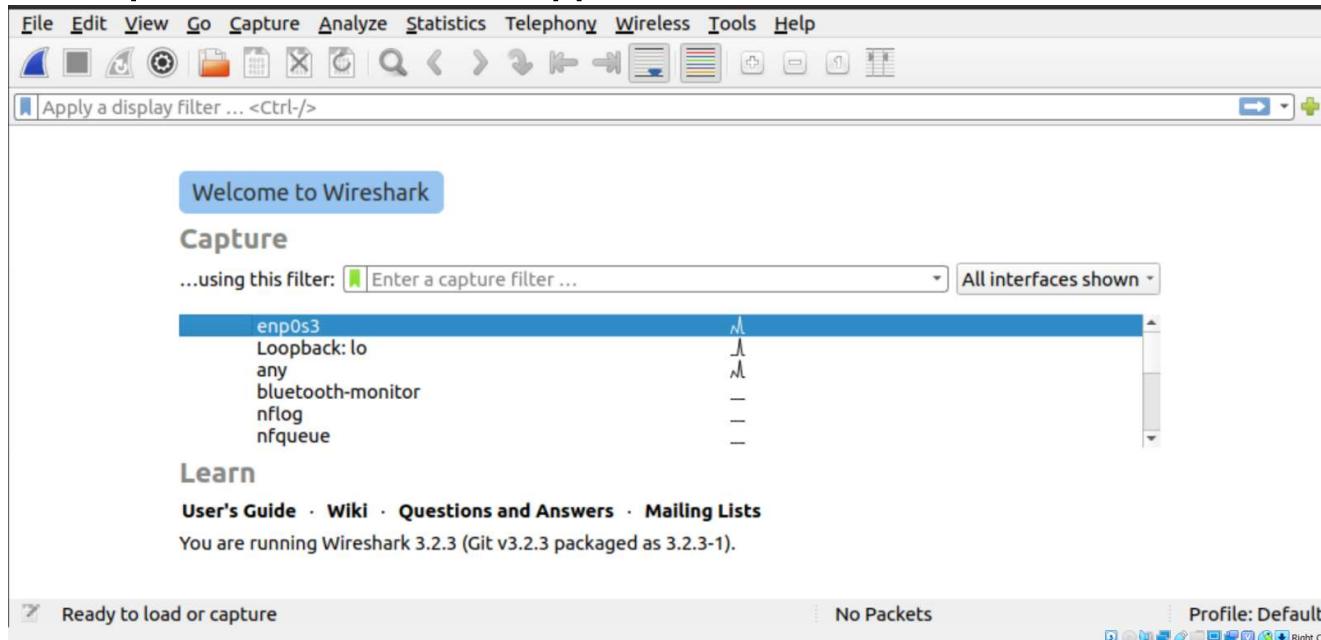
2. sudo dpkg-reconfigure wireshark-common

```
root@kmabhijith-VirtualBox:~# sudo dpkg-reconfigure wireshark-common
root@kmabhijith-VirtualBox:~# █
```

3. Select Yes and press enter



4. Open wireshark from the applist



5. Analyzing network packet stream

