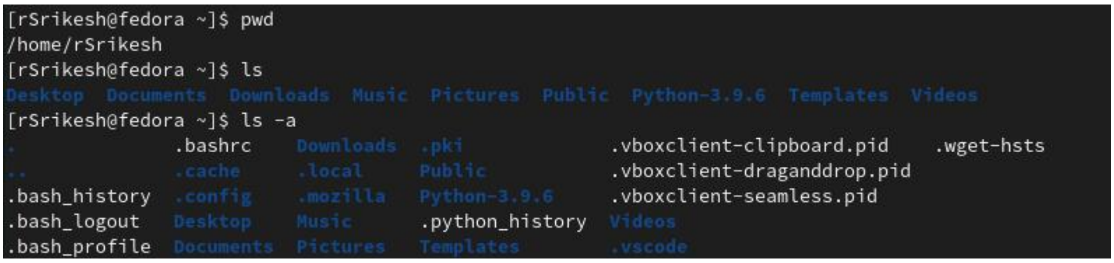
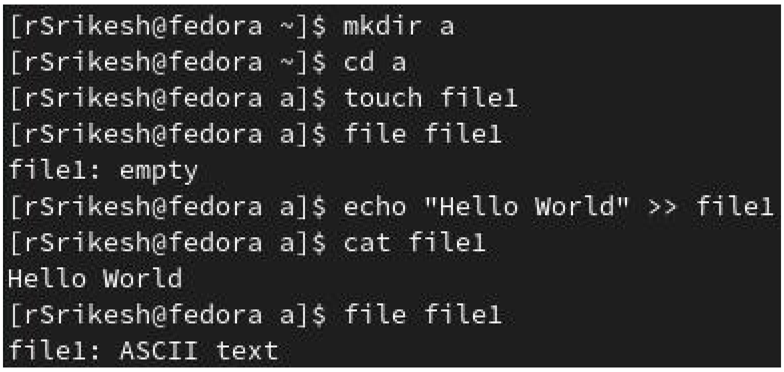
BASH Challenges

1. (a.) Display the path of your current directory
   (b.) List out the contents of your current
directory
   (c.) List out the contents of your current
directory
        including hidden files



```
[rSrikesh@fedora ~]$ pwd
/home/rSrikesh
[rSrikesh@fedora ~]$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Python-3.9.6  Templates  Videos
[rSrikesh@fedora ~]$ ls -a
.              .bashrc    Downloads  .pki             .vboxclient-clipboard.pid    .wget-hsts
..             .cache     .local     Public           .vboxclient-draganddrop.pid
.bash_history  .config    .mozilla   Python-3.9.6     .vboxclient-seamless.pid
.bash_logout   Desktop    Music      .python_history  Videos
.bash_profile  Documents  Pictures   Templates        .vscode
```

2. (a.) Create a new directory named **a**
   (b.) Move to the newly created directory **a**
   (c.) Create a blank file named "file1"
   (d.) Display the file type of "file1"
   (e.) Add the line "Hello World" to "file1" using
the
        command **echo**
   (f.) Display the contents of "file1"
   (g.) Display the file type of "file1" again



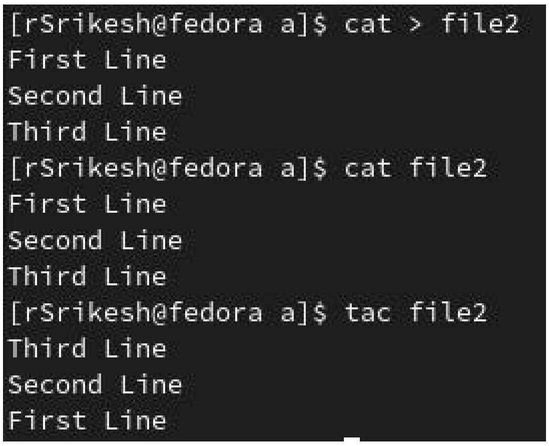
```
[rSrikesh@fedora ~]$ mkdir a
[rSrikesh@fedora ~]$ cd a
[rSrikesh@fedora a]$ touch file1
[rSrikesh@fedora a]$ file file1
file1: empty
[rSrikesh@fedora a]$ echo "Hello World" >> file1
[rSrikesh@fedora a]$ cat file1
Hello World
[rSrikesh@fedora a]$ file file1
file1: ASCII text
```

3. (a.) Stay in directory **a.** Create a file “file2” and add the contents below using the command **cat**

First Line **Second Line** **Third Line**

(b.) Display the contents of “file2”

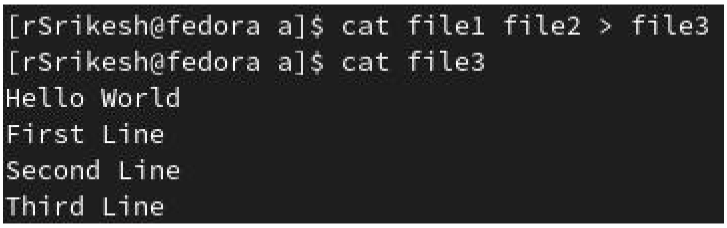
(c.) Display the contents of “file2” with the lines reversed



```
[rSrikesh@fedora a]$ cat > file2
First Line
Second Line
Third Line
[rSrikesh@fedora a]$ cat file2
First Line
Second Line
Third Line
[rSrikesh@fedora a]$ tac file2
Third Line
Second Line
First Line
```

4. (a.) Stay in directory **a.** Concatenate the contents of “file1” and “file2” and save them into a
new
file “file3”

(b.) Display the contents of “file3”



```
[rSrikesh@fedora a]$ cat file1 file2 > file3
[rSrikesh@fedora a]$ cat file3
Hello World
First Line
Second Line
Third Line
```

5. (a.) Stay in directory **a.** Create 2 directories **b/c** with a single command

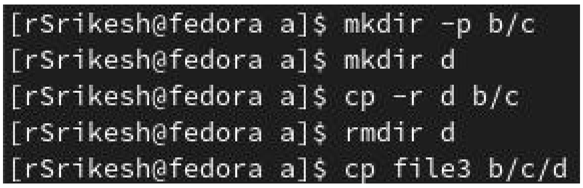
   (b.) Create a new directory **d**

   (c.) Copy the directory **d** to directory **c** using a single command

   (d.) Delete the directory **d** in the current directory

a

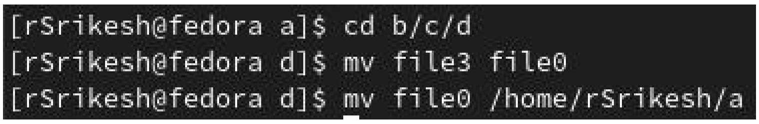
   (e.) Copy "file3" to the directory **d** with a single command



```
[rSrikesh@fedora a]$ mkdir -p b/c
[rSrikesh@fedora a]$ mkdir d
[rSrikesh@fedora a]$ cp -r d b/c
[rSrikesh@fedora a]$ rmdir d
[rSrikesh@fedora a]$ cp file3 b/c/d
```

6. (a.) Go to directory **d** and rename "file3" to "file0"

   (b.) Stay in the same directory and move "file0" to directory **a**

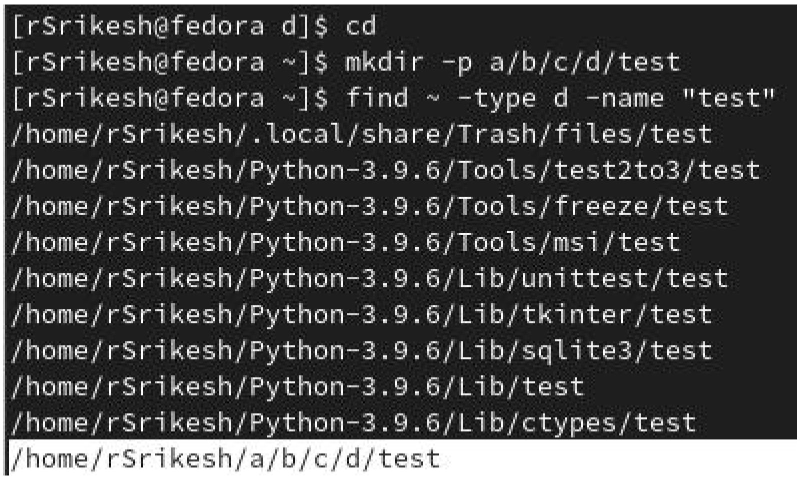


```
[rSrikesh@fedora a]$ cd b/c/d
[rSrikesh@fedora d]$ mv file3 file0
[rSrikesh@fedora d]$ mv file0 /home/rSrikesh/a
```

7. (a.) Go to your home directory

   (b.) Create a file named "test" in the directory **a/b/c/d**

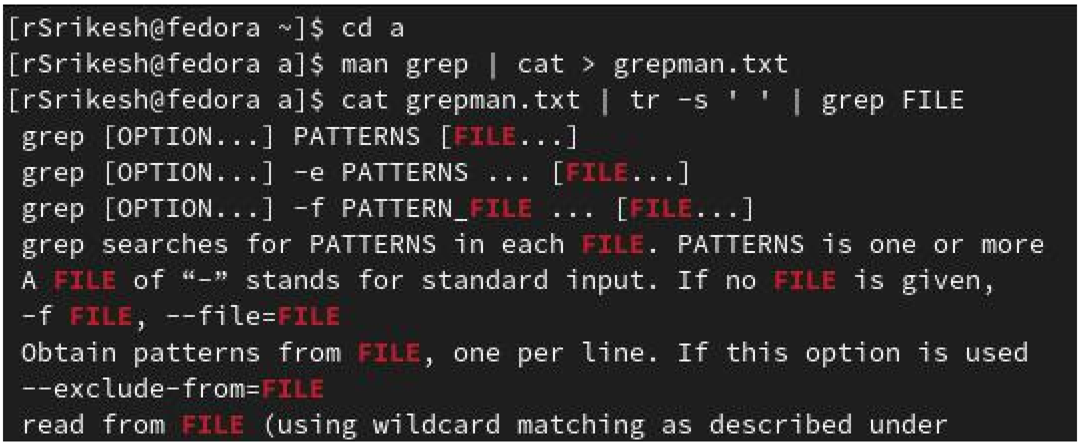
   (c.) Stay in the home directory. **Find** and display the path of "test"



```
[rSrikesh@fedora d]$ cd
[rSrikesh@fedora ~]$ mkdir -p a/b/c/d/test
[rSrikesh@fedora ~]$ find ~ -type d -name "test"
/home/rSrikesh/.local/share/Trash/files/test
/home/rSrikesh/Python-3.9.6/Tools/test2to3/test
/home/rSrikesh/Python-3.9.6/Tools/freeze/test
/home/rSrikesh/Python-3.9.6/Tools/msi/test
/home/rSrikesh/Python-3.9.6/Lib/unittest/test
/home/rSrikesh/Python-3.9.6/Lib/tkinter/test
/home/rSrikesh/Python-3.9.6/Lib/sqlite3/test
/home/rSrikesh/Python-3.9.6/Lib/test
/home/rSrikesh/Python-3.9.6/Lib/ctypes/test
/home/rSrikesh/a/b/c/d/test
```

8. (a.) Go to directory **a.** Get the man page of grep and save its contents to a file named "grepman.txt"

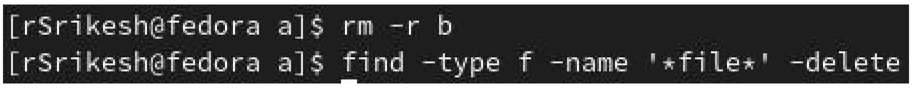
   (b.) Print the lines containing the word "**FILE**" (Case sensitive) in the file "grepman.txt"



```
[rSrikesh@fedora ~]$ cd a
[rSrikesh@fedora a]$ man grep | cat > grepman.txt
[rSrikesh@fedora a]$ cat grepman.txt | tr -s ' ' | grep FILE
 grep [OPTION...] PATTERNS [FILE...]
 grep [OPTION...] -e PATTERNS ... [FILE...]
 grep [OPTION...] -f PATTERN_FILE ... [FILE...]
 grep searches for PATTERNS in each FILE. PATTERNS is one or more
 A FILE of "-" stands for standard input. If no FILE is given,
 -f FILE, --file=FILE
 Obtain patterns from FILE, one per line. If this option is used
 --exclude-from=FILE
 read from FILE (using wildcard matching as described under
```

9. (a.) Go to directory **a** and remove the directory **b** with a single command

   (b.) Remove the files starting with the word "file" with a single command

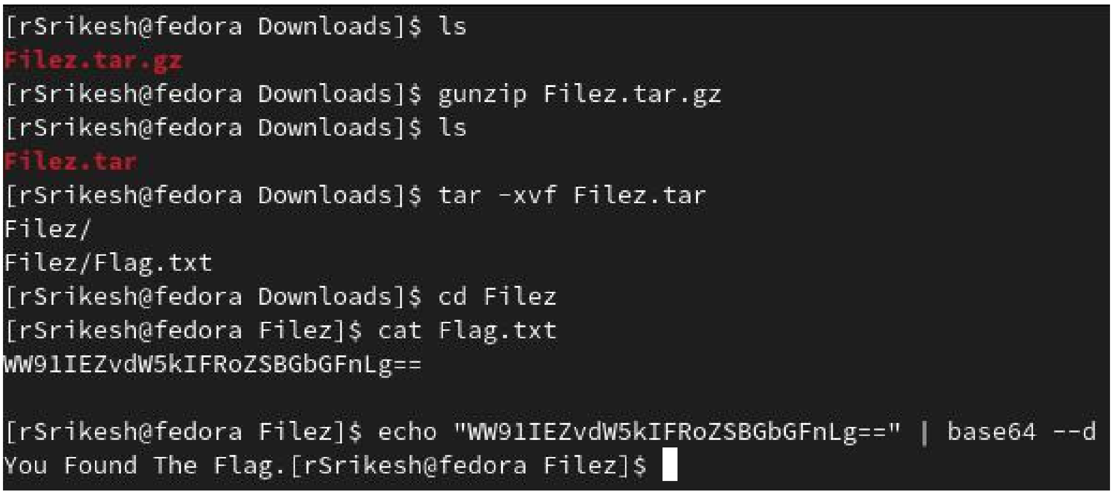


```
[rSrikesh@fedora a]$ rm -r b
[rSrikesh@fedora a]$ find -type f -name '*file*' -delete
```

10. (a.) Download the compressed file from the drive. https://drive.google.com/drive/folders/1PG3ZlpFu6nQSNjpCNuceoGcNey00bhPP?usp=sharing

(b.) Extract the compressed file using CLI.

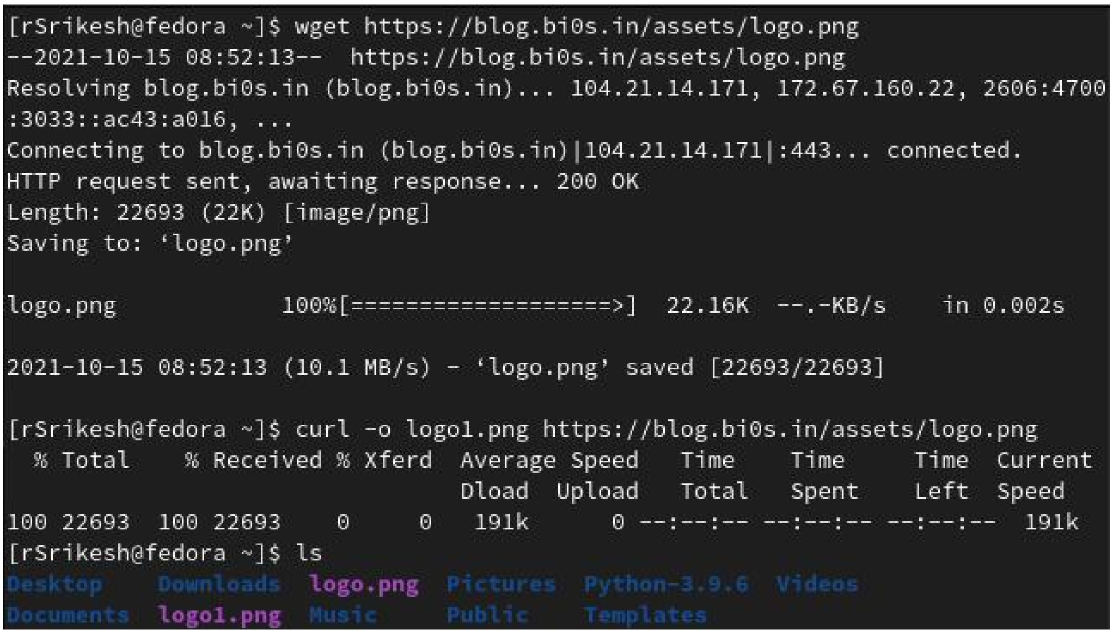
(c.) Decode the base64 content and display the content of "Flag.txt"



```
[rSrikesh@fedora Downloads]$ ls
Filez.tar.gz
[rSrikesh@fedora Downloads]$ gunzip Filez.tar.gz
[rSrikesh@fedora Downloads]$ ls
Filez.tar
[rSrikesh@fedora Downloads]$ tar -xvf Filez.tar
Filez/
Filez/Flag.txt
[rSrikesh@fedora Downloads]$ cd Filez
[rSrikesh@fedora Filez]$ cat Flag.txt
WW91IEZvdW5kIFRoZSBGbGFnLg==

[rSrikesh@fedora Filez]$ echo "WW91IEZvdW5kIFRoZSBGbGFnLg==" | base64 --d
You Found The Flag.[rSrikesh@fedora Filez]$ 
```

11. (a.) Go to https://blog.bi0s.in/ and download the **logo.png** image using **wget**

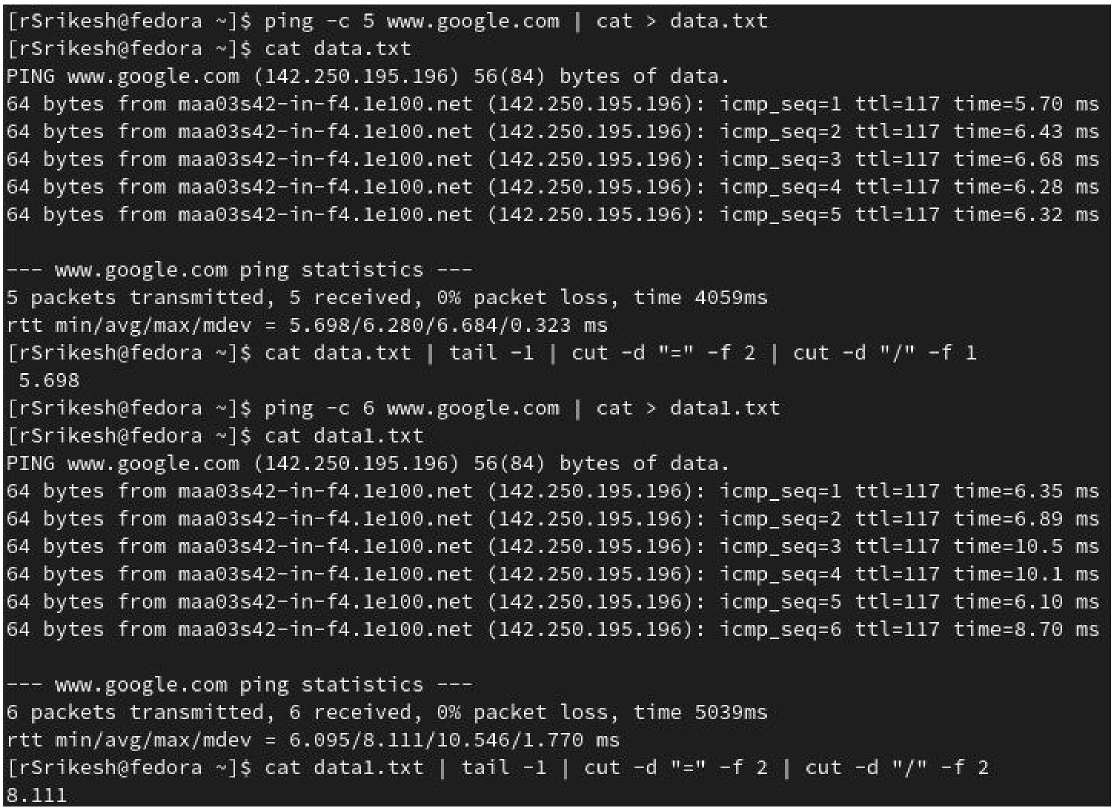
(b.) Do the same using **curl**



```
[rSrikesh@fedora ~]$ wget https://blog.bi0s.in/assets/logo.png
--2021-10-15 08:52:13--  https://blog.bi0s.in/assets/logo.png
Resolving blog.bi0s.in (blog.bi0s.in)... 104.21.14.171, 172.67.160.22, 2606:4700
:3033::ac43:a016, ...
Connecting to blog.bi0s.in (blog.bi0s.in)|104.21.14.171|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22693 (22K) [image/png]
Saving to: 'logo.png'

logo.png            100%[===================>]  22.16K  --.-KB/s    in 0.002s

2021-10-15 08:52:13 (10.1 MB/s) - 'logo.png' saved [22693/22693]

[rSrikesh@fedora ~]$ curl -o logo1.png https://blog.bi0s.in/assets/logo.png
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 22693  100 22693    0     0   191k      0 --:--:-- --:--:-- --:--:--  191k
[rSrikesh@fedora ~]$ ls
Desktop    Downloads  logo.png  Pictures  Python-3.9.6  Videos
Documents  logo1.png  Music     Public    Templates
```

12.(a.) Ping **google.com** and find the lowest time taken
to get a response (Stop pinging after getting
5
responses)

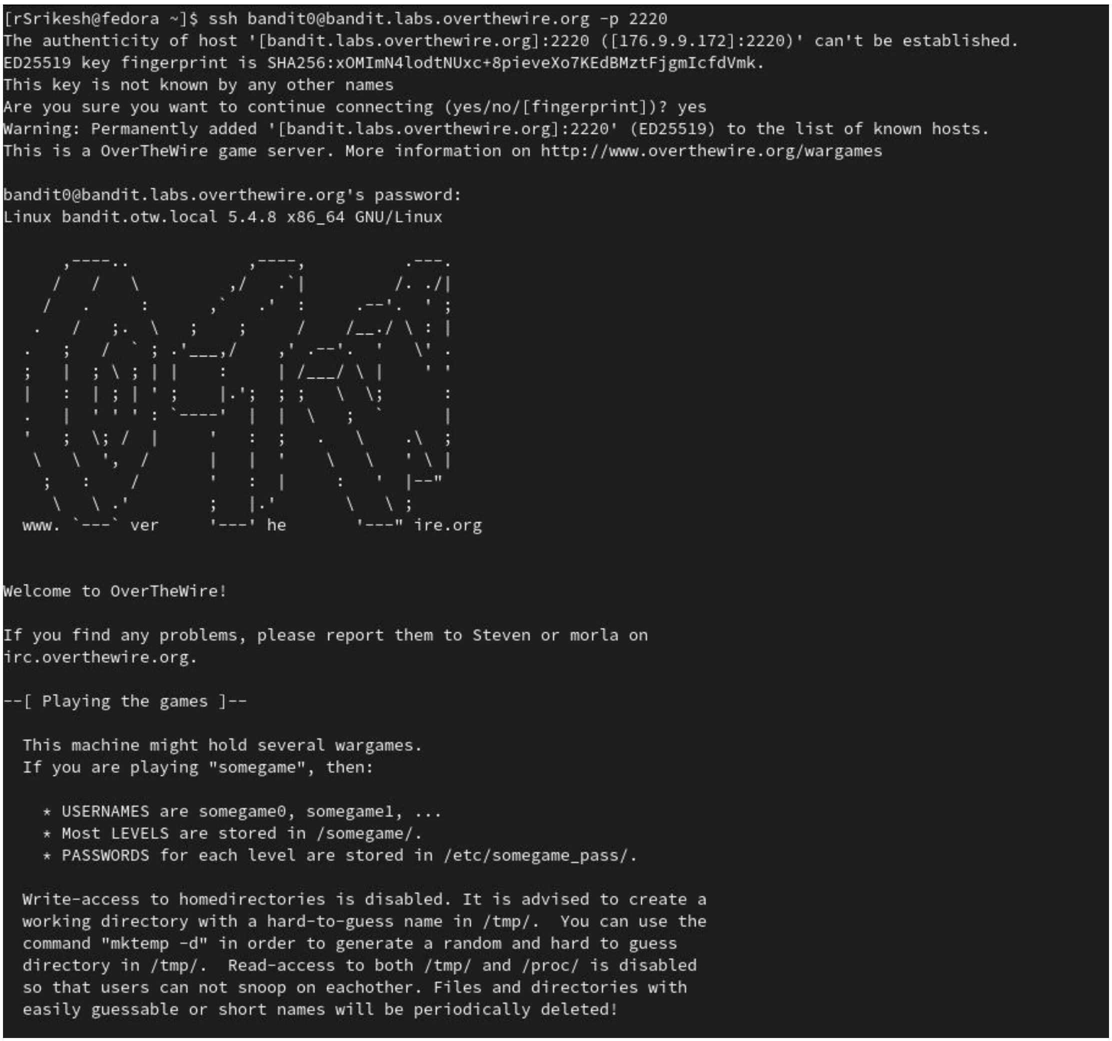
(b.) Ping **google.com** 6 times and find the average
time taken to get a response



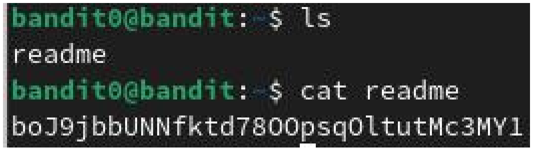
```
[rSrikesh@fedora ~]$ ping -c 5 www.google.com | cat > data.txt
[rSrikesh@fedora ~]$ cat data.txt
PING www.google.com (142.250.195.196) 56(84) bytes of data.
64 bytes from maa03s42-in-f4.1e100.net (142.250.195.196): icmp_seq=1 ttl=117 time=5.70 ms
64 bytes from maa03s42-in-f4.1e100.net (142.250.195.196): icmp_seq=2 ttl=117 time=6.43 ms
64 bytes from maa03s42-in-f4.1e100.net (142.250.195.196): icmp_seq=3 ttl=117 time=6.68 ms
64 bytes from maa03s42-in-f4.1e100.net (142.250.195.196): icmp_seq=4 ttl=117 time=6.28 ms
64 bytes from maa03s42-in-f4.1e100.net (142.250.195.196): icmp_seq=5 ttl=117 time=6.32 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4059ms
rtt min/avg/max/mdev = 5.698/6.280/6.684/0.323 ms
[rSrikesh@fedora ~]$ cat data.txt | tail -1 | cut -d "=" -f 2 | cut -d "/" -f 1
 5.698
[rSrikesh@fedora ~]$ ping -c 6 www.google.com | cat > data1.txt
[rSrikesh@fedora ~]$ cat data1.txt
PING www.google.com (142.250.195.196) 56(84) bytes of data.
64 bytes from maa03s42-in-f4.1e100.net (142.250.195.196): icmp_seq=1 ttl=117 time=6.35 ms
64 bytes from maa03s42-in-f4.1e100.net (142.250.195.196): icmp_seq=2 ttl=117 time=6.89 ms
64 bytes from maa03s42-in-f4.1e100.net (142.250.195.196): icmp_seq=3 ttl=117 time=10.5 ms
64 bytes from maa03s42-in-f4.1e100.net (142.250.195.196): icmp_seq=4 ttl=117 time=10.1 ms
64 bytes from maa03s42-in-f4.1e100.net (142.250.195.196): icmp_seq=5 ttl=117 time=6.10 ms
64 bytes from maa03s42-in-f4.1e100.net (142.250.195.196): icmp_seq=6 ttl=117 time=8.70 ms

--- www.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5039ms
rtt min/avg/max/mdev = 6.095/8.111/10.546/1.770 ms
[rSrikesh@fedora ~]$ cat data1.txt | tail -1 | cut -d "=" -f 2 | cut -d "/" -f 2
8.111
```

13. Complete bandit level 0 and get the flag.

https://overthewire.org/wargames/bandit/bandit0.html

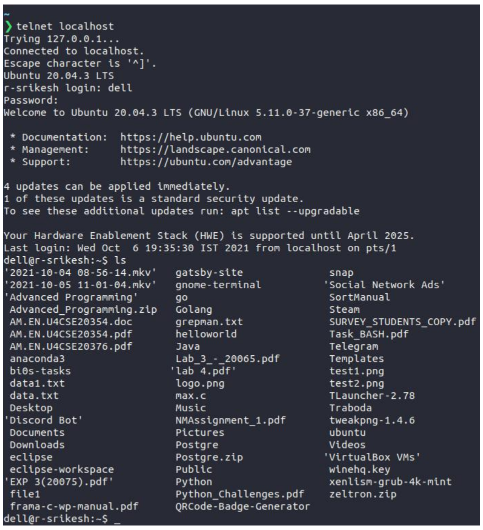


```
[rSrikesh@fedora ~]$ ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([176.9.9.172]:2220)' can't be established.
ED25519 key fingerprint is SHA256:xOMImN4lodtNUxc+8pieveXo7KEdBMztFjgmIcfdVmk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220' (ED25519) to the list of known hosts.
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!

If you find any problems, please report them to Steven or morla on
irc.overthewire.org.

--[ Playing the games ]--

  This machine might hold several wargames.
  If you are playing "somegame", then:

    * USERNAMES are somegame0, somegame1, ...
    * Most LEVELS are stored in /somegame/.
    * PASSWORDS for each level are stored in /etc/somegame_pass/.

  Write-access to homedirectories is disabled. It is advised to create a
  working directory with a hard-to-guess name in /tmp/.  You can use the
  command "mktemp -d" in order to generate a random and hard to guess
  directory in /tmp/.  Read-access to both /tmp/ and /proc/ is disabled
  so that users can not snoop on eachother. Files and directories with
  easily guessable or short names will be periodically deleted!
```



```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
```

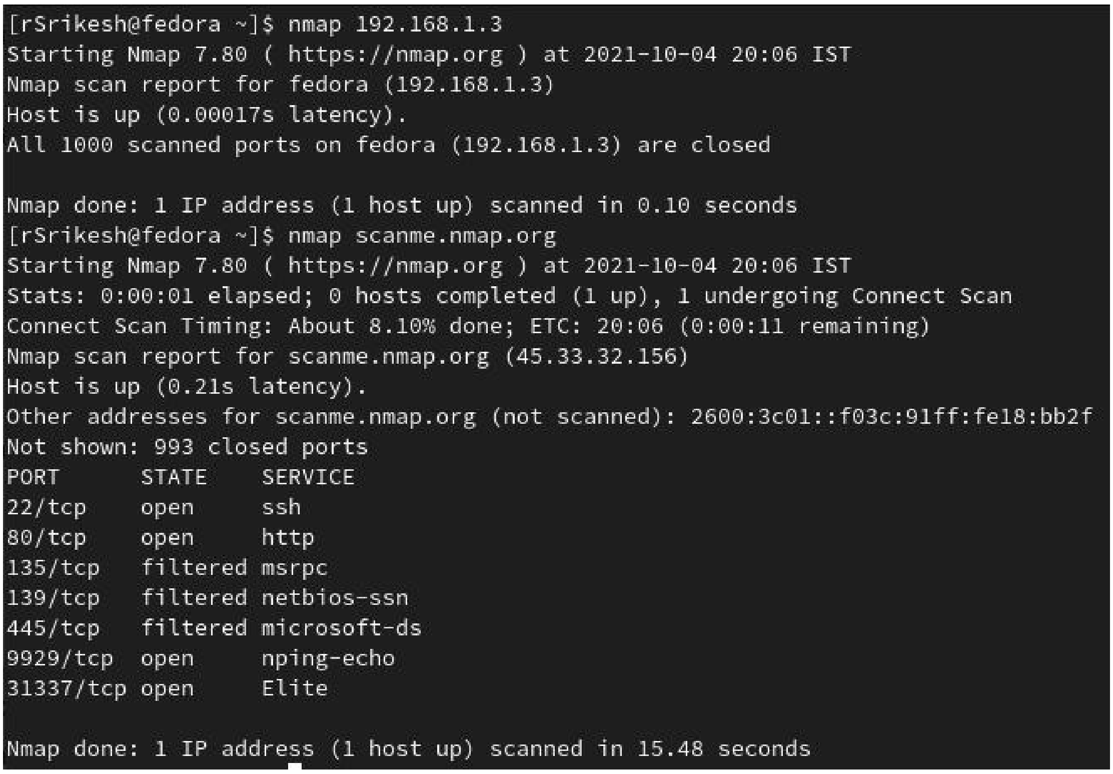
14. Connect to your own system using telnet



```
~
❯ telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 20.04.3 LTS
r-srikesh login: dell
Password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

4 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Wed Oct  6 19:35:30 IST 2021 from localhost on pts/1
dell@r-srikesh:~$ ls
'2021-10-04 08-56-14.mkv'   gatsby-site               snap
'2021-10-05 11-01-04.mkv'   gnome-terminal           'Social Network Ads'
'Advanced Programming'      go                        SortManual
 Advanced_Programming.zip   Golang                    Steam
 AM.EN.U4CSE20354.doc       grepman.txt               SURVEY_STUDENTS_COPY.pdf
 AM.EN.U4CSE20354.pdf       helloworld                Task_BASH.pdf
 AM.EN.U4CSE20376.pdf       Java                      Telegram
 anaconda3                  Lab_3_-_20065.pdf         Templates
 bi0s-tasks                'lab 4.pdf'                test1.png
 data1.txt                  logo.png                  test2.png
 data.txt                   max.c                     TLauncher-2.78
 Desktop                    Music                     Traboda
'Discord Bot'               NMAssignment_1.pdf        tweakpng-1.4.6
 Documents                  Pictures                  ubuntu
 Downloads                  Postgre                   Videos
 eclipse                    Postgre.zip              'VirtualBox VMs'
 eclipse-workspace          Public                    winehq.key
'EXP 3(20075).pdf'          Python                    xenlism-grub-4k-mint
 file1                      Python_Challenges.pdf     zeltron.zip
 frama-c-wp-manual.pdf      QRCode-Badge-Generator
dell@r-srikesh:~$ _
```

15. (a.) Learn about nmap and use that scanner to scan your own machine

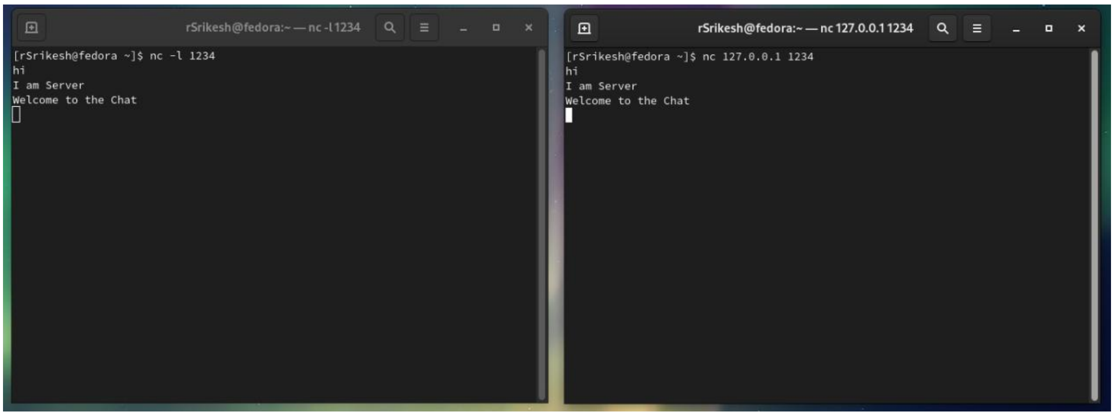
(b.) Use nmap to scan **scanme.nmap.org**



```
[rSrikesh@fedora ~]$ nmap 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-04 20:06 IST
Nmap scan report for fedora (192.168.1.3)
Host is up (0.00017s latency).
All 1000 scanned ports on fedora (192.168.1.3) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
[rSrikesh@fedora ~]$ nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-04 20:06 IST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 8.10% done; ETC: 20:06 (0:00:11 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 15.48 seconds
```

16. (a.) Create a chat application using **nc** on your local machine with one terminal as server and other as the client

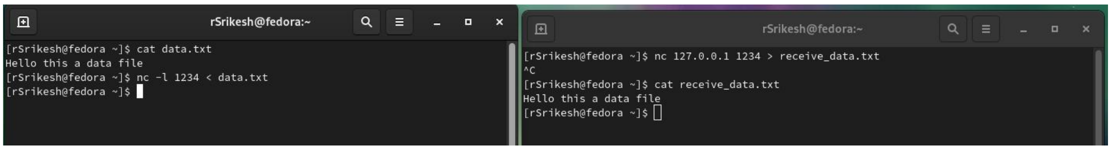
(b.) Transfer a file from server to client (save that file with another name) and display the file.



rSrikesh@fedora:~ — nc -l 1234
rSrikesh@fedora:~ — nc 127.0.0.1 1234

```
[rSrikesh@fedora ~]$ nc -l 1234
hi
I am Server
Welcome to the Chat
```

```
[rSrikesh@fedora ~]$ nc 127.0.0.1 1234
hi
I am Server
Welcome to the Chat
```



```
[rSrikesh@fedora ~]$ cat data.txt
Hello this a data file
[rSrikesh@fedora ~]$ nc -l 1234 < data.txt
[rSrikesh@fedora ~]$
```

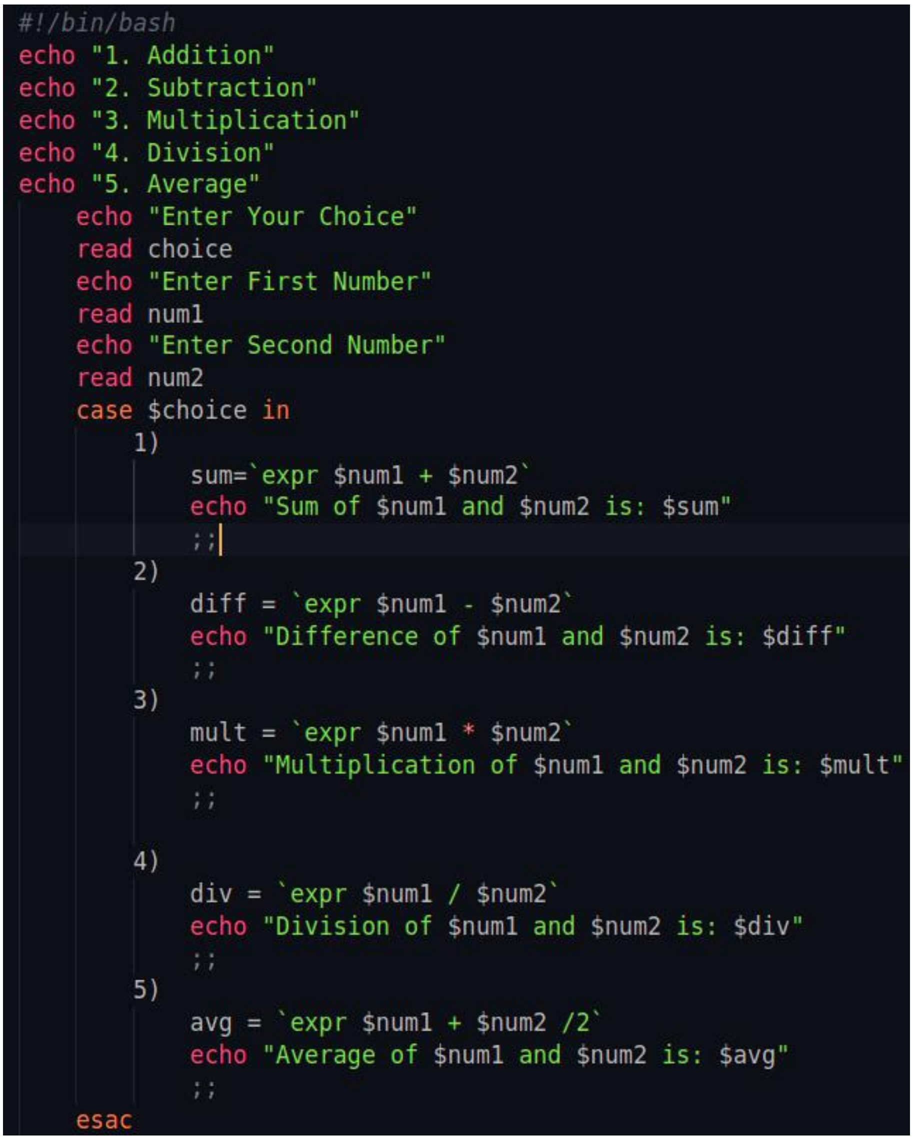
```
[rSrikesh@fedora ~]$ nc 127.0.0.1 1234 > receive_data.txt
^C
[rSrikesh@fedora ~]$ cat receive_data.txt
Hello this a data file
[rSrikesh@fedora ~]$
```

SHELL SCRIPTING

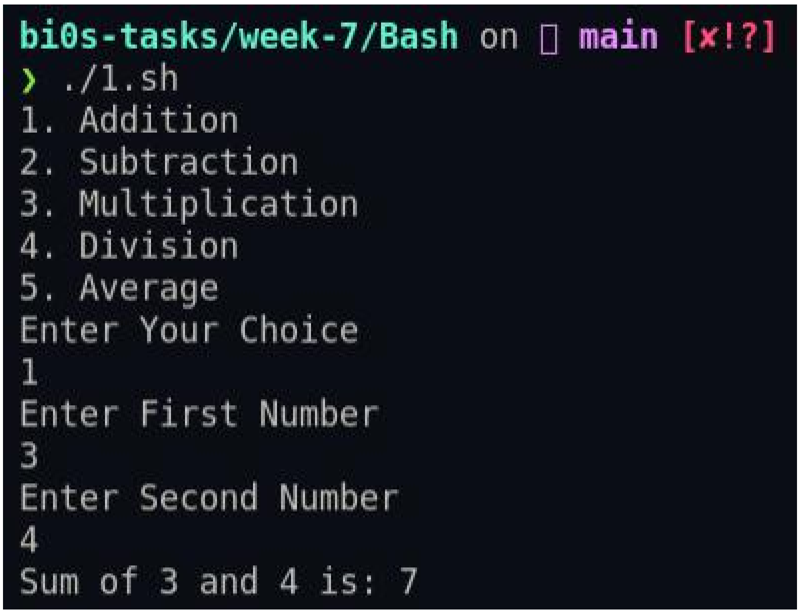
1. Write a shell script to run the following operations by reading 2 numbers and 1 choice from the user:

```
1:Addition
2:Subtraction
3:Multiplication
4:Division
5:Average
```

It should be a choice based program i.e. if the input is 1 Addition should be performed



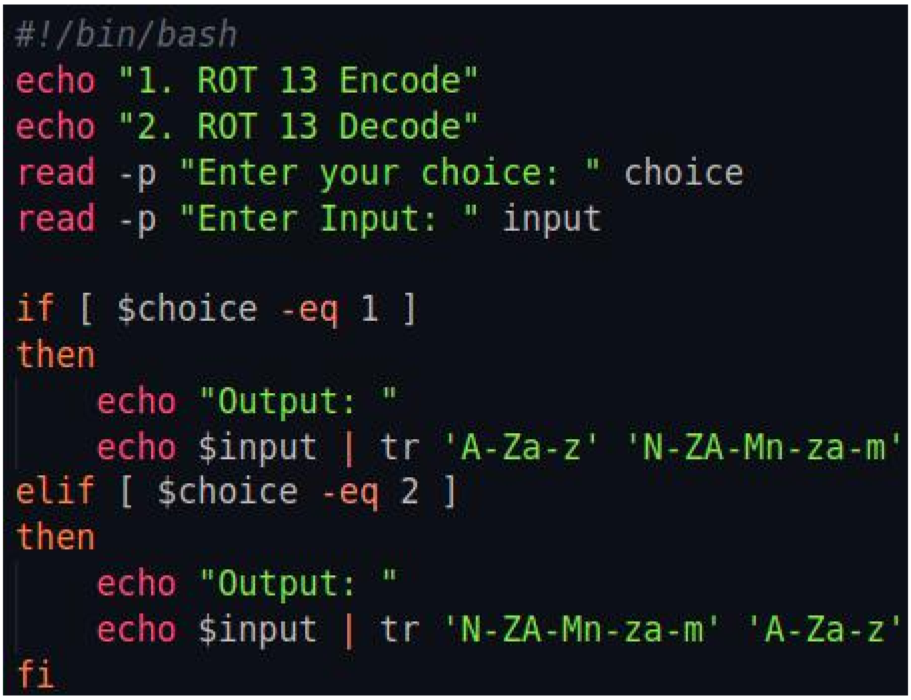
```bash
#!/bin/bash
echo "1. Addition"
echo "2. Subtraction"
echo "3. Multiplication"
echo "4. Division"
echo "5. Average"
    echo "Enter Your Choice"
    read choice
    echo "Enter First Number"
    read num1
    echo "Enter Second Number"
    read num2
    case $choice in
        1)
            sum=`expr $num1 + $num2`
            echo "Sum of $num1 and $num2 is: $sum"
            ;;
        2)
            diff = `expr $num1 - $num2`
            echo "Difference of $num1 and $num2 is: $diff"
            ;;
        3)
            mult = `expr $num1 * $num2`
            echo "Multiplication of $num1 and $num2 is: $mult"
            ;;

        4)
            div = `expr $num1 / $num2`
            echo "Division of $num1 and $num2 is: $div"
            ;;
        5)
            avg = `expr $num1 + $num2 /2`
            echo "Average of $num1 and $num2 is: $avg"
            ;;
    esac
```



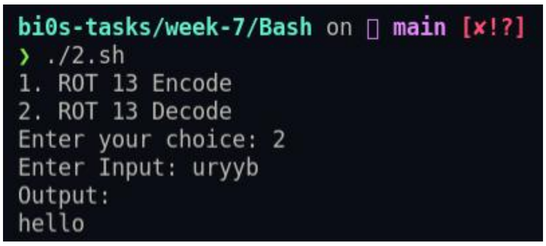
```
bi0s-tasks/week-7/Bash on  main [x!?]
❯ ./1.sh
1. Addition
2. Subtraction
3. Multiplication
4. Division
5. Average
Enter Your Choice
1
Enter First Number
3
Enter Second Number
4
Sum of 3 and 4 is: 7
```

2. Write a script to run the following operations by reading an input and a choice from the user:

1:ROT13 Encode
2:ROT13 Decode

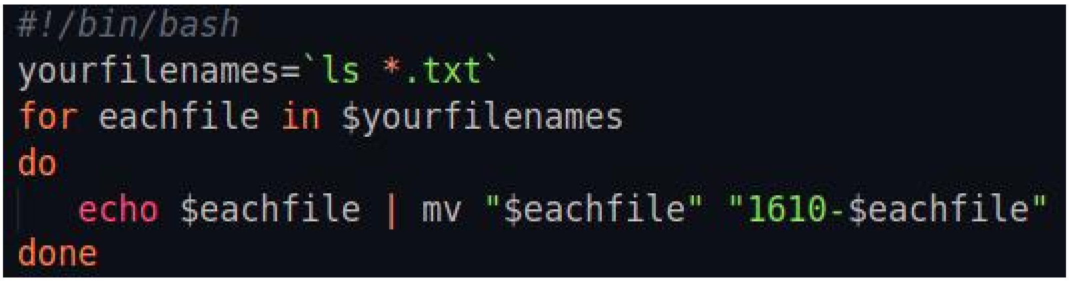


```bash
#!/bin/bash
echo "1. ROT 13 Encode"
echo "2. ROT 13 Decode"
read -p "Enter your choice: " choice
read -p "Enter Input: " input

if [ $choice -eq 1 ]
then
    echo "Output: "
    echo $input | tr 'A-Za-z' 'N-ZA-Mn-za-m'
elif [ $choice -eq 2 ]
then
    echo "Output: "
    echo $input | tr 'N-ZA-Mn-za-m' 'A-Za-z'
fi
```

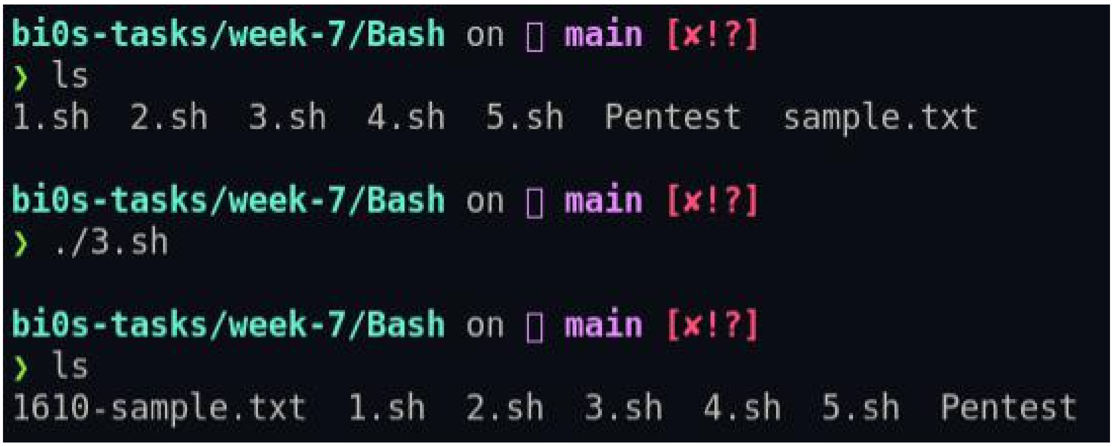


```
bi0s-tasks/week-7/Bash on  main [x!?]
❯ ./2.sh
1. ROT 13 Encode
2. ROT 13 Decode
Enter your choice: 2
Enter Input: uryyb
Output:
hello
```

3. Write a script to rename all the txt files in your current directory to begin with the current date and month.
For example, if the name of the file is **sample.txt** then the renamed filename should be **DDMM-sample.txt.**

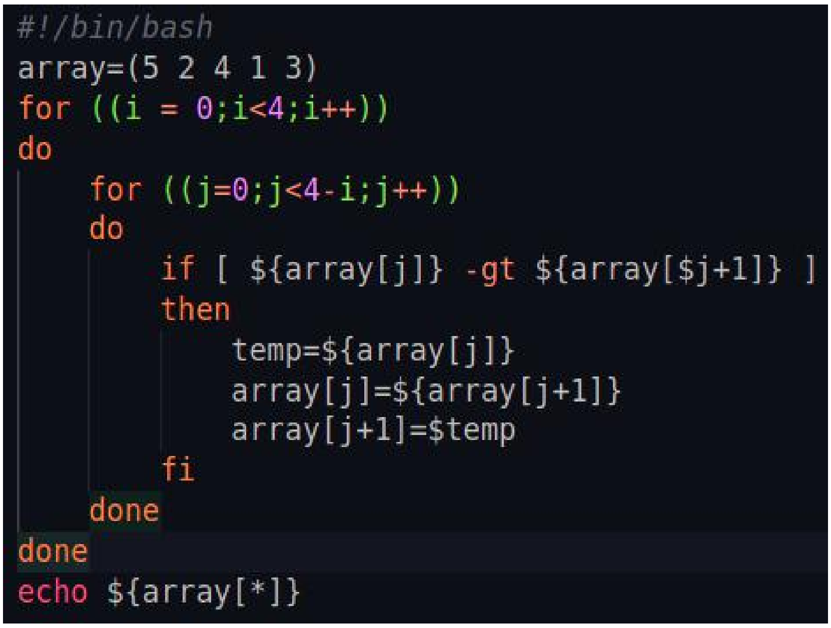


```
#!/bin/bash
yourfilenames=`ls *.txt`
for eachfile in $yourfilenames
do
    echo $eachfile | mv "$eachfile" "1610-$eachfile"
done
```

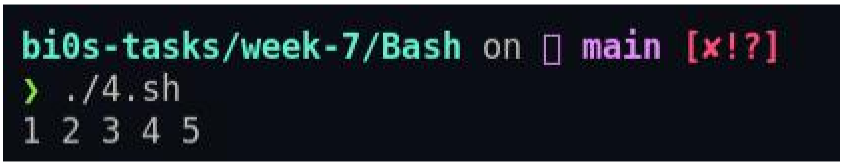


```
bi0s-tasks/week-7/Bash on □ main [✘!?]
❯ ls
1.sh  2.sh  3.sh  4.sh  5.sh  Pentest  sample.txt

bi0s-tasks/week-7/Bash on □ main [✘!?]
❯ ./3.sh

bi0s-tasks/week-7/Bash on □ main [✘!?]
❯ ls
1610-sample.txt  1.sh  2.sh  3.sh  4.sh  5.sh  Pentest
```

4. Write a shell script to sort an array using bubble sort.

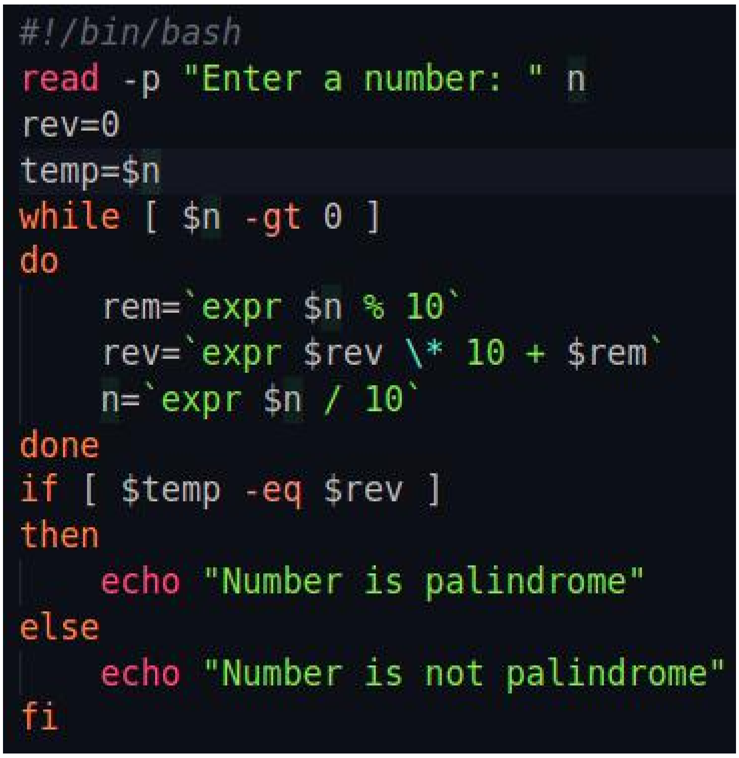


```
#!/bin/bash
array=(5 2 4 1 3)
for ((i = 0;i<4;i++))
do
    for ((j=0;j<4-i;j++))
    do
        if [ ${array[j]} -gt ${array[$j+1]} ]
        then
            temp=${array[j]}
            array[j]=${array[j+1]}
            array[j+1]=$temp
        fi
    done
done
echo ${array[*]}
```

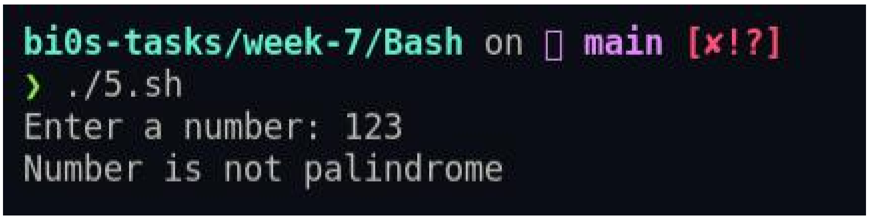


```
bi0s-tasks/week-7/Bash on  main [x!?]
❯ ./4.sh
1 2 3 4 5
```

5. Write a shell script to check whether a number is a palindrome or not.



```
#!/bin/bash
read -p "Enter a number: " n
rev=0
temp=$n
while [ $n -gt 0 ]
do
    rem=`expr $n % 10`
    rev=`expr $rev \* 10 + $rem`
    n=`expr $n / 10`
done
if [ $temp -eq $rev ]
then
    echo "Number is palindrome"
else
    echo "Number is not palindrome"
fi
```



```
bi0s-tasks/week-7/Bash on  main [x!?]
❯ ./5.sh
Enter a number: 123
Number is not palindrome
```