2. Create a file on your Linux system and try to copy from your system to neighbors Linux system using
 a. Destination folder is /home
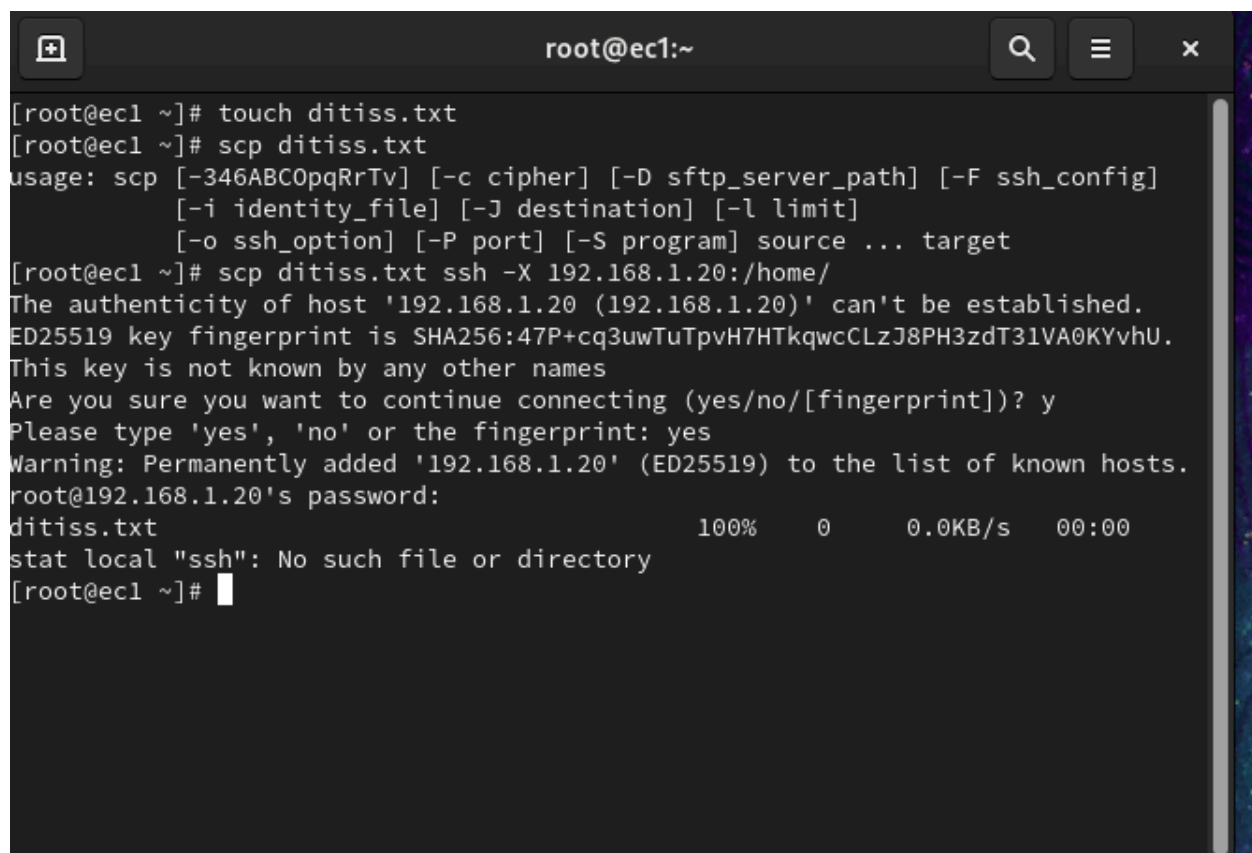 b. Destination folder is /root

a.
1.Now create empty file touch ditiss.txt in server side then copy this file in client side
/home
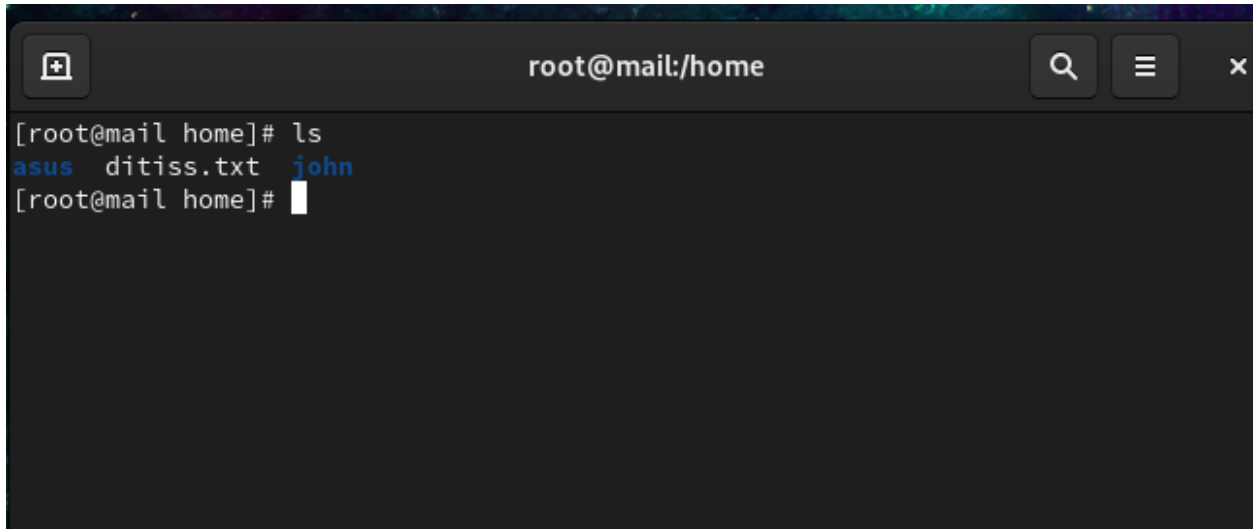#touch ditiss.txt   to create a txt file
scp ditiss.txt ssh-X 192.168.1.20:/home/

```
root@ec1:~

[root@ec1 ~]# touch ditiss.txt
[root@ec1 ~]# scp ditiss.txt
usage: scp [-346ABCOpqRrTv] [-c cipher] [-D sftp_server_path] [-F ssh_config]
           [-i identity_file] [-J destination] [-l limit]
           [-o ssh_option] [-P port] [-S program] source ... target
[root@ec1 ~]# scp ditiss.txt ssh -X 192.168.1.20:/home/
The authenticity of host '192.168.1.20 (192.168.1.20)' can't be established.
ED25519 key fingerprint is SHA256:47P+cq3uwTuTpvH7HTkqwcCLzJ8PH3zdT31VA0KYvhU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.20' (ED25519) to the list of known hosts.
root@192.168.1.20's password:
ditiss.txt                                        100%    0    0.0KB/s   00:00
stat local "ssh": No such file or directory
[root@ec1 ~]#
```
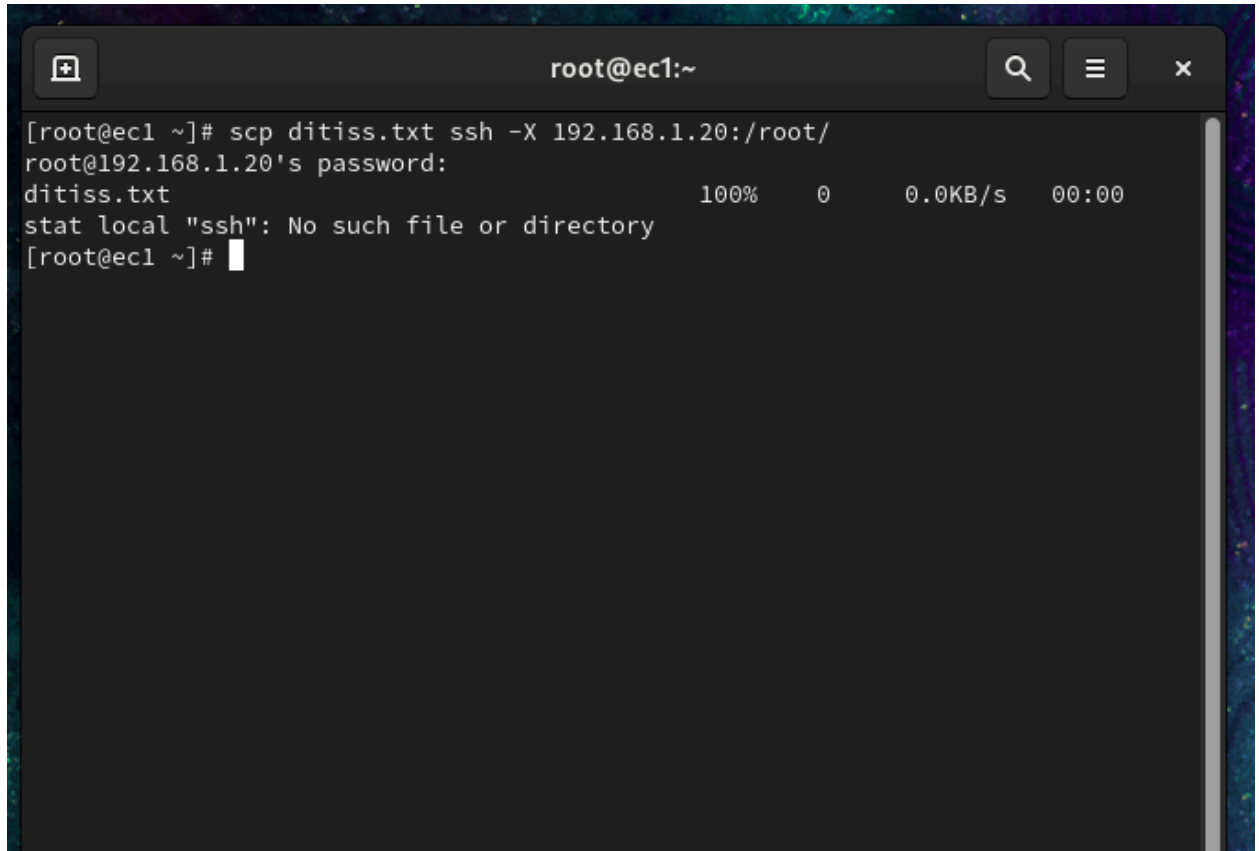
2. Check the file in client in /home folder

```
[root@mail home]# ls
asus   ditiss.txt   john
[root@mail home]#
```

B.
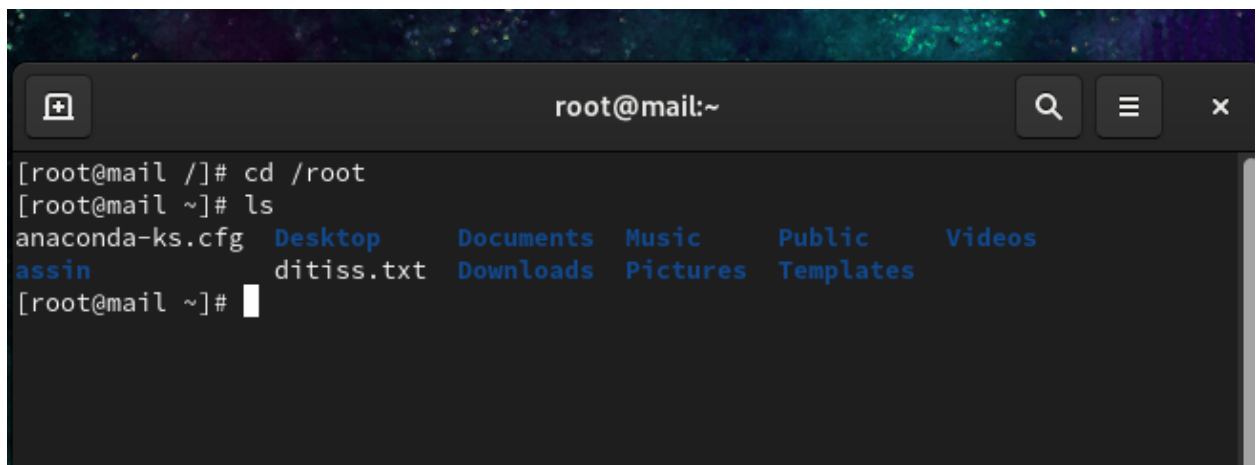
1. Create empty file touch ditiss.txt in server side then copy this file in client-side /root

```
[root@ec1 ~]# scp ditiss.txt ssh -X 192.168.1.20:/root/
root@192.168.1.20's password:
ditiss.txt                                      100%    0      0.0KB/s    00:00
stat local "ssh": No such file or directory
[root@ec1 ~]#
```

2. Check the file it is copied in client side
   #cd /root   to go to root

```
[root@mail /]# cd /root
[root@mail ~]# ls
anaconda-ks.cfg  Desktop       Documents  Music     Public     Videos
assin            ditiss.txt    Downloads  Pictures  Templates
[root@mail ~]#
```