LOVELY PROFESSIONAL UNIVERSITY

INT301: Open Source Technologies

Submitted By: Vishal Kumar

Reg. No.: 11904071

Roll No.: 10

Section: KE058

Academic Task No.: 03

Faculty Name: Navjot Kaur

1.Introduction

1.1 Objective of the project

- Transfer the files from server to client using any Open Source Software.
- Explore other options for this open-source software

1.2 Description of the project

Open-source software is based on the idea that the user cannot only view but also can change the source code of the existing application.

Here in this project, First I am using **SFTP** to transfer the files from server to client. And Then WinSCP Open Source Software.

1.3 Scope of the project

The purpose of the project is to transfer files from server to client. This project is based on the Open Source Software which helps you to transfer the files from one server to another.

2. System Description

2.1 Target System Description

SFTP

The SSH File Transfer Protocol (also Secure File Transfer Protocol, or SFTP) is a network protocol that provides file access, file transfer, and file management functionalities over any reliable data stream.

It was designed by the Internet Engineering Task Force (IETF) as an extension of the Secure Shell protocol (SSH) version 2.0 to provide secure file transfer capabilities.

This protocol assumes that it is run over a secure channel, such as SSH, that the server has already authenticated the client, and that the identity of the client user is available to the protocol.

SFTP Server and Client

SFTP Server:

- There are numerous SFTP server implementations both for UNIX, Windows and MacOS. The most widely known is perhaps OpenSSH, but there are also proprietary implementations. Typically the port used is 22. SFTP file transfer protocol is part of SSH protocol suite.

SFTP Client:

- It is a command-line program that implements the client part of this protocol. As an example, the sftp program supplied with OpenSSH implements this.
- Some implementations of the scp program support both the SFTP and SCP protocols to perform file transfers, depending on what the server supports.

OpenSSH

- OpenSSH is a free open source set of computer tools used to provide secure and encrypted communication over a computer network by using the ssh protocol.
- Many people, new to computers and protocols, create a misconception about OpenSSH, they think it is a protocol, but it is not, it is a set of computer programs that use the ssh protocol.
- OpenSSH is developed by the Open BSD group and it is released under Simplified BSD License.

- A main factor which has made possible for OpenSSH to be used so much among system administrators is its multi-platform capability and very useful nice features it has.
- The latest version — is OpenSSH 9.3 which has been released on 15 March 2023.

Why to use sftp over ftp/telnet?

- The most important reason why should use OpenSSH tools over ftp and telnet is that all communications and user credentials using OpenSSH are encrypted, they are also protected from man in the middle attacks.

- If a third party tries to intercept your connection, OpenSSH detects it and informs you about that.

Features of OpenSSH

- Secure Communication
- Strong Encryption (3DES, Blowfish, AES, Arcfour)
- X11 Forwarding (encrypt X Window System traffic)
- Port Forwarding (encrypted channels for legacy protocols)
- Strong Authentication (Public Key, One-Time Password and Kerberos Authentication)
- Agent Forwarding (Single-Sign-On)
- Interoperability (Compliance with SSH 1.3, 1.5, and 2.0 protocol Standards)
- SFTP client and server support in both SSH1 and SSH2 protocols.
- Data Compression
- Kerberos and AFS Ticket Passing

2.2 Assumptions

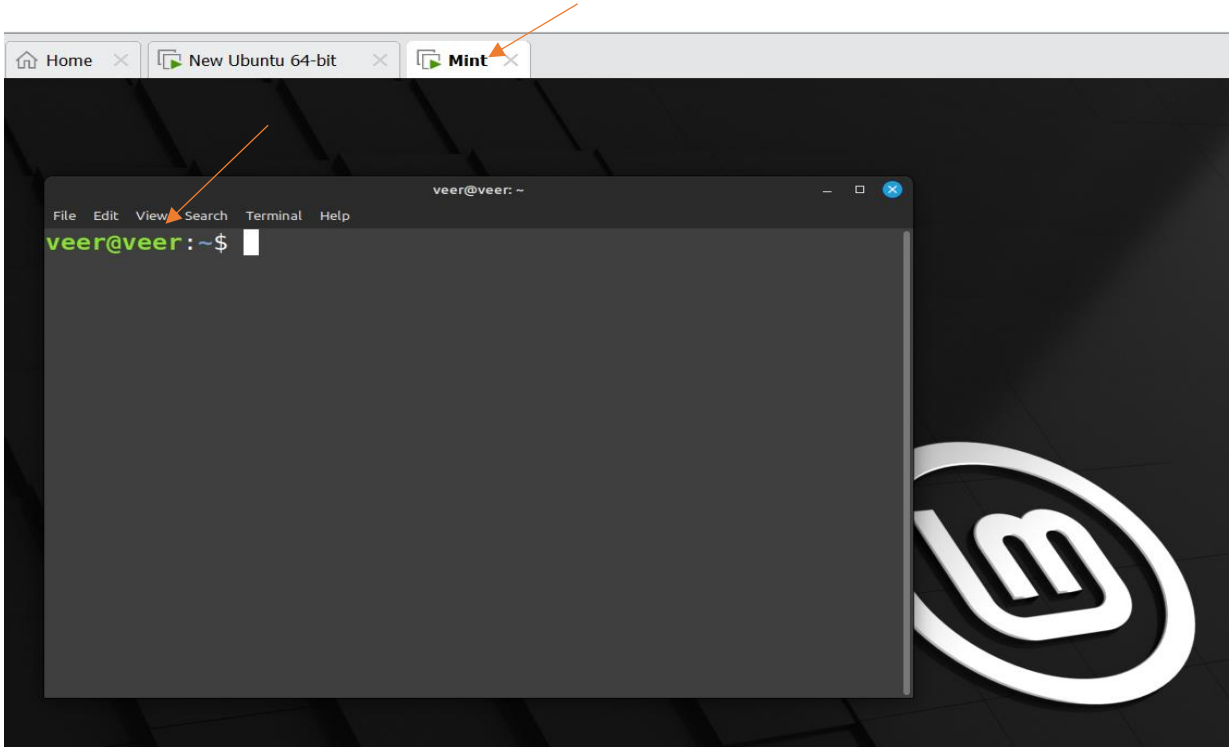
1. Assuming Linux Mint (As Server)
2. Assuming Ubuntu (As Client)
3. The protocol assumes that it is run over a secure channel, such as SSH.

3. Analysis Report

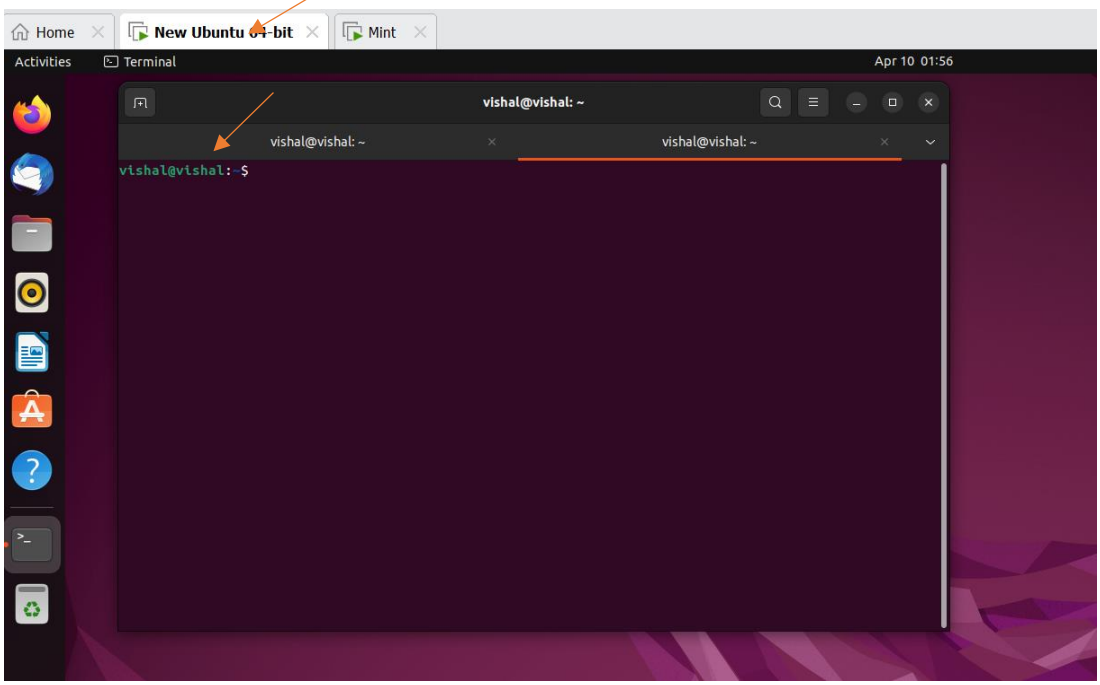
OpenSSH Requirements

- OpenSSH can be installed on any kind of Linux systems and any kind of network connections.
- I have used Ubuntu and Linux Mint in the demonstration.

1. Linux Mint (As Server)

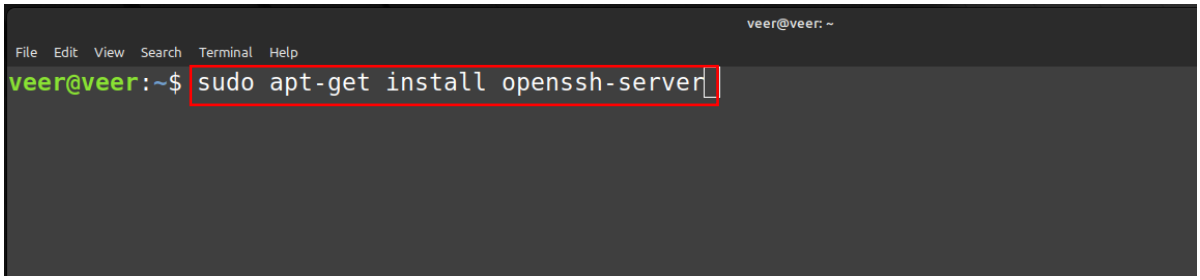


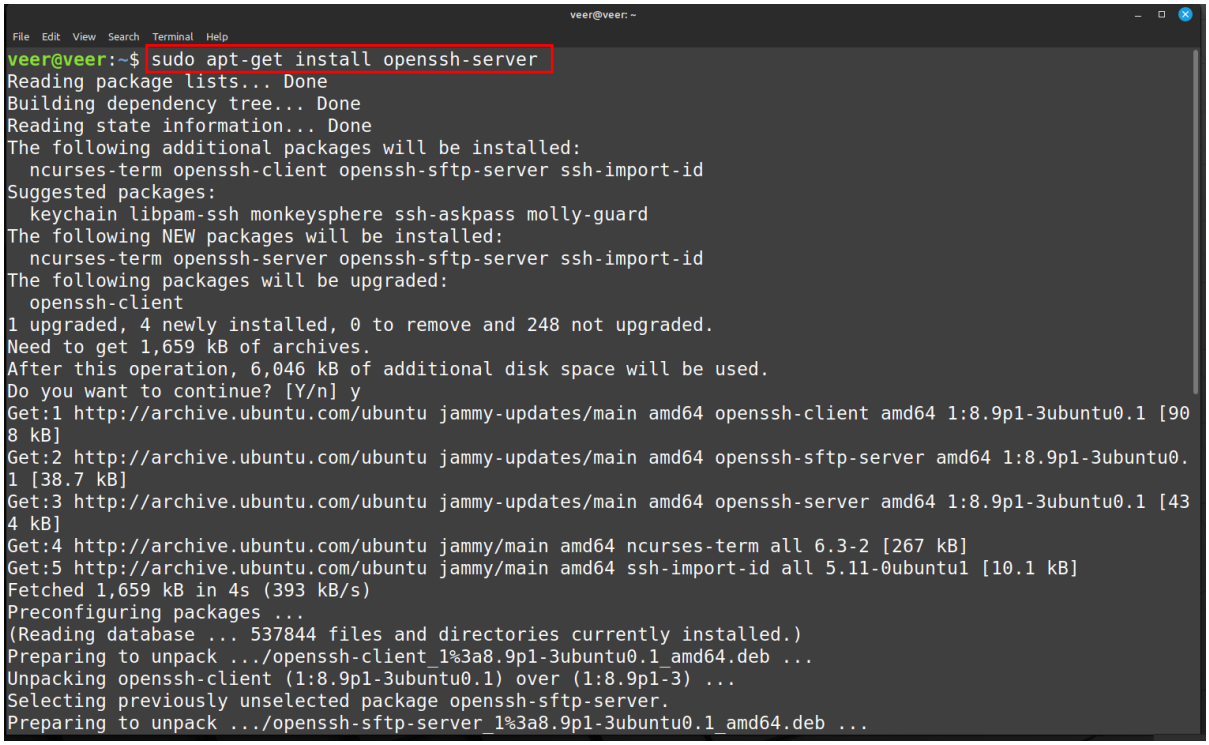
2: Ubuntu (As Client)



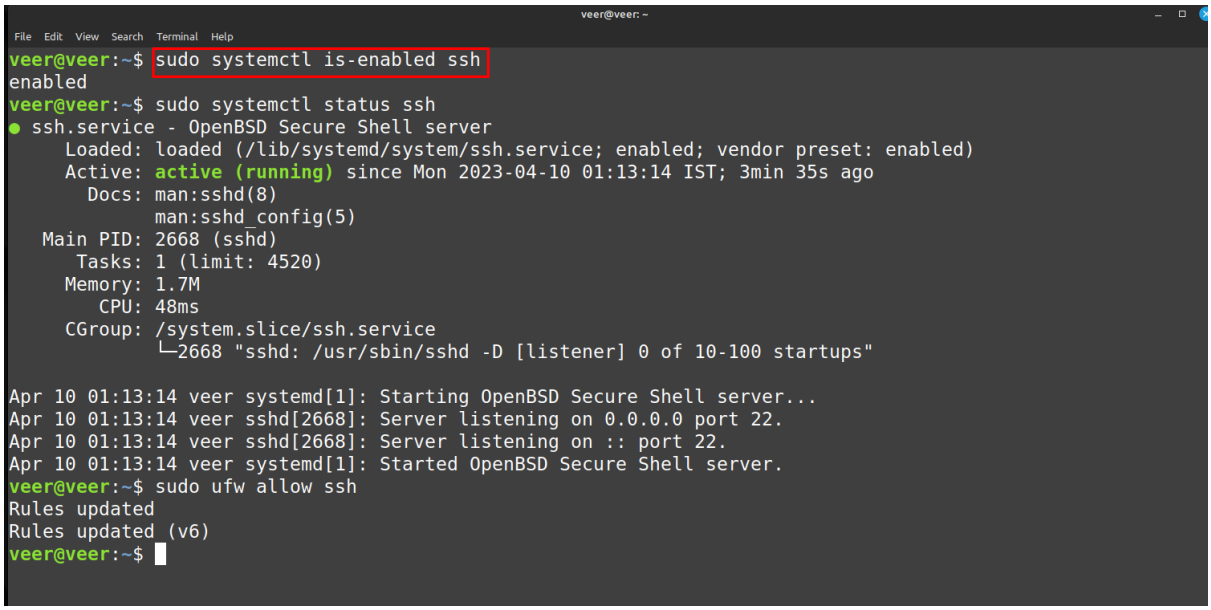
To transfer the files from Linux Mint (server) to Ubuntu (client):

1. Install OpenSSH on Linux Mint




veer@veer: ~
File Edit View Search Terminal Help
veer@veer:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
openssh-client
1 upgraded, 4 newly installed, 0 to remove and 248 not upgraded.
Need to get 1,659 kB of archives.
After this operation, 6,046 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-client amd64 1:8.9p1-3ubuntu0.1 [908 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-server amd64 1:8.9p1-3ubuntu0.1 [38.7 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-server amd64 1:8.9p1-3ubuntu0.1 [434 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy/main amd64 ncurses-term all 6.3-2 [267 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy/main amd64 ssh-import-id all 5.11-0ubuntu1 [10.1 kB]
Fetched 1,659 kB in 4s (393 kB/s)
Preconfiguring packages ...
(Reading database ... 537844 files and directories currently installed.)
Preparing to unpack .../openssh-client_1%3a8.9p1-3ubuntu0.1_amd64.deb ...
Unpacking openssh-client (1:8.9p1-3ubuntu0.1) over (1:8.9p1-3) ...
Selecting previously unselected package openssh-sftp-server.
Preparing to unpack .../openssh-sftp-server_1%3a8.9p1-3ubuntu0.1_amd64.deb ...

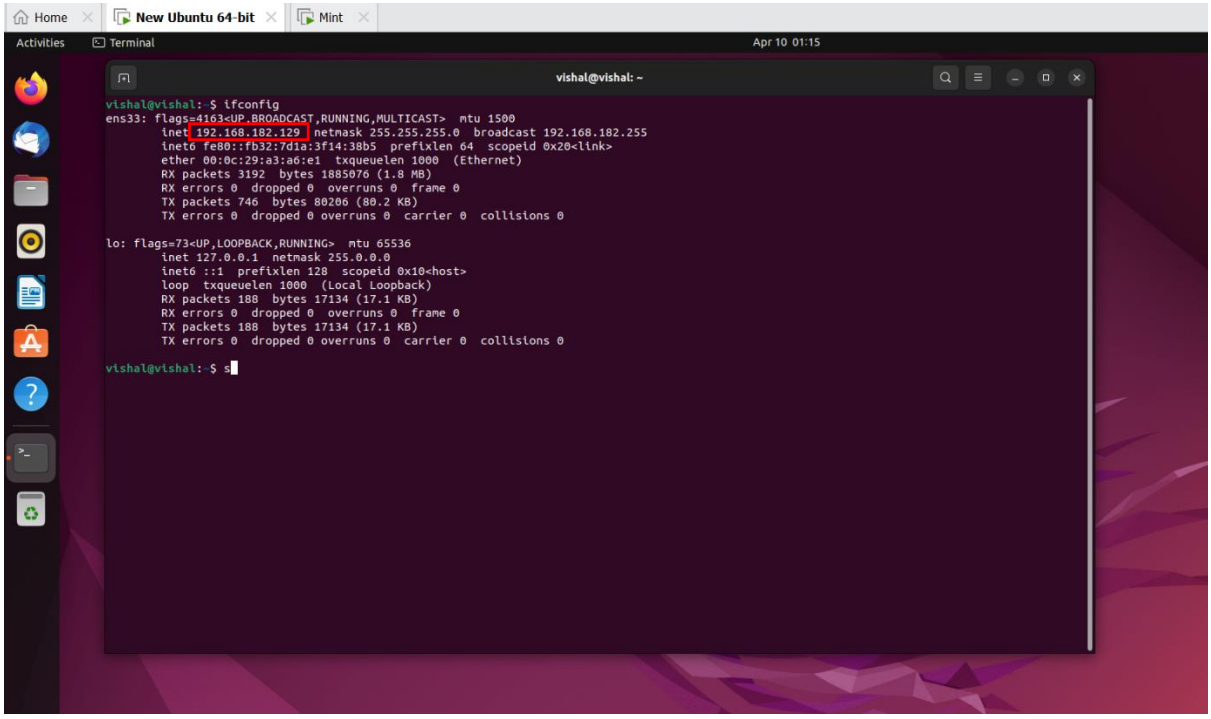
Enable SSH


veer@veer: ~
File Edit View Search Terminal Help
veer@veer:~$ sudo systemctl is-enabled ssh
enabled
veer@veer:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
Active: active (running) since Mon 2023-04-10 01:13:14 IST; 3min 35s ago
Docs: man:sshd(8)
man:sshd_config(5)
Main PID: 2668 (sshd)
Tasks: 1 (limit: 4520)
Memory: 1.7M
CPU: 48ms
CGroup: /system.slice/ssh.service
└─2668 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
Apr 10 01:13:14 veer systemd[1]: Starting OpenBSD Secure Shell server...
Apr 10 01:13:14 veer sshd[2668]: Server listening on 0.0.0.0 port 22.
Apr 10 01:13:14 veer sshd[2668]: Server listening on :: port 22.
Apr 10 01:13:14 veer systemd[1]: Started OpenBSD Secure Shell server.
veer@veer:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
veer@veer:~$

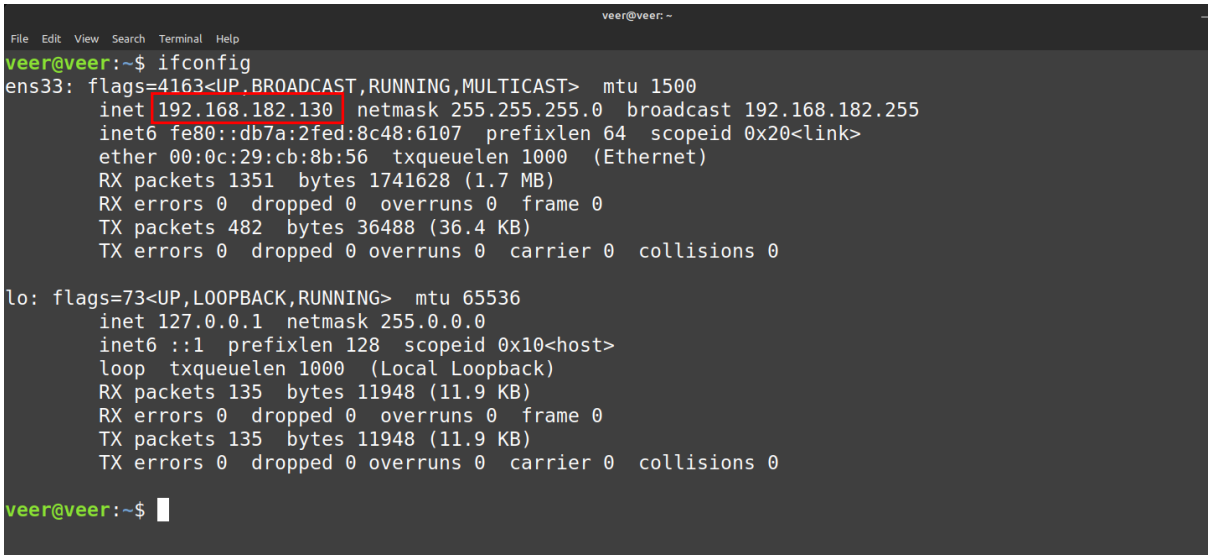
WFW Enable

```
veer@veer: ~
File  Edit  View  Search  Terminal  Help
veer@veer:~$ sudo ufw status verbose
Status: inactive
veer@veer:~$ sudo ufw enable
Firewall is active and enabled on system startup
veer@veer:~$ sudo ufw reload
Firewall reloaded
veer@veer:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)

veer@veer:~$
```

2. Check IP of Ubuntu (Client)

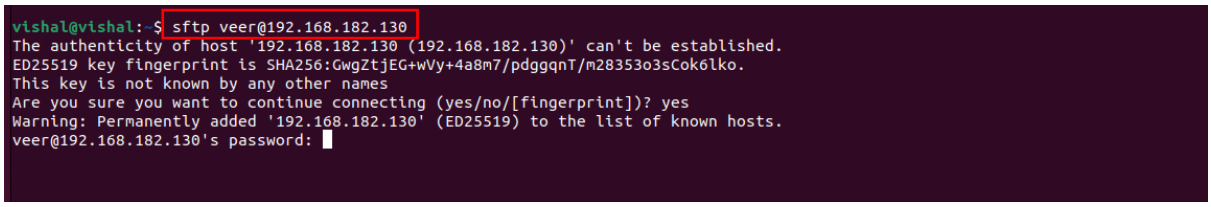


3. Check IP of Linux Mint (Server)



4. On Ubuntu (As Client)

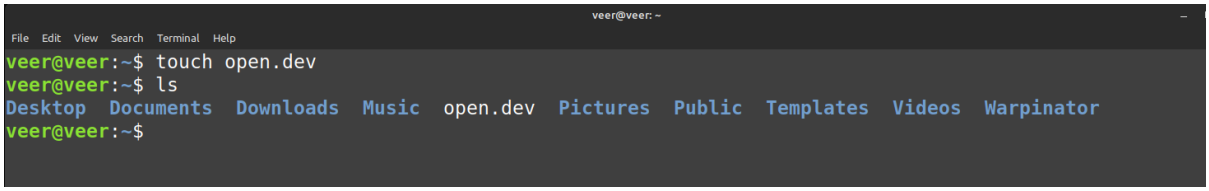
- I want to access the files in Ubuntu from Linux Mint.
- Use following command to get connected Ubuntu to Linux Mint using **sftp**.



5. SMTP Prompt

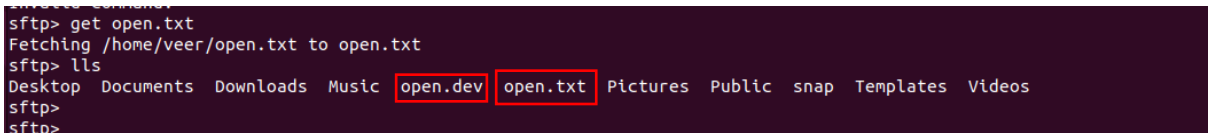
6. Make & See the files on Linux Mint (As Server)

- I have created two files ‘open.dev’ and ‘open.txt’ in Linux Mint (Server) to transfer from this to Ubuntu (Client) using ‘touch’ command.
- You can see both the files using ‘ls’ command.

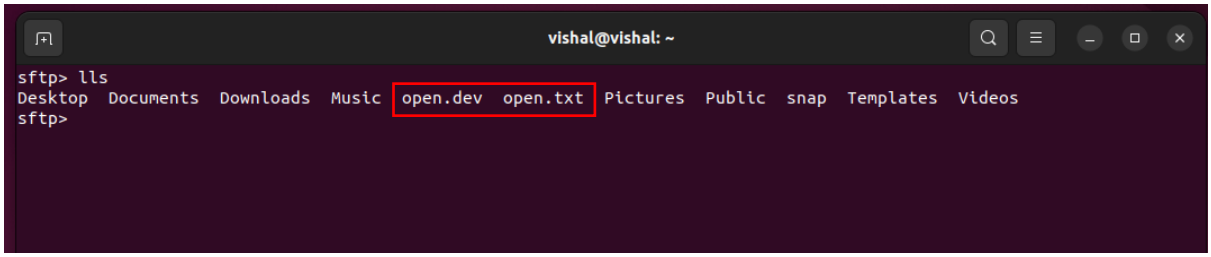


7. See the files in Ubuntu using ‘ls’ command.

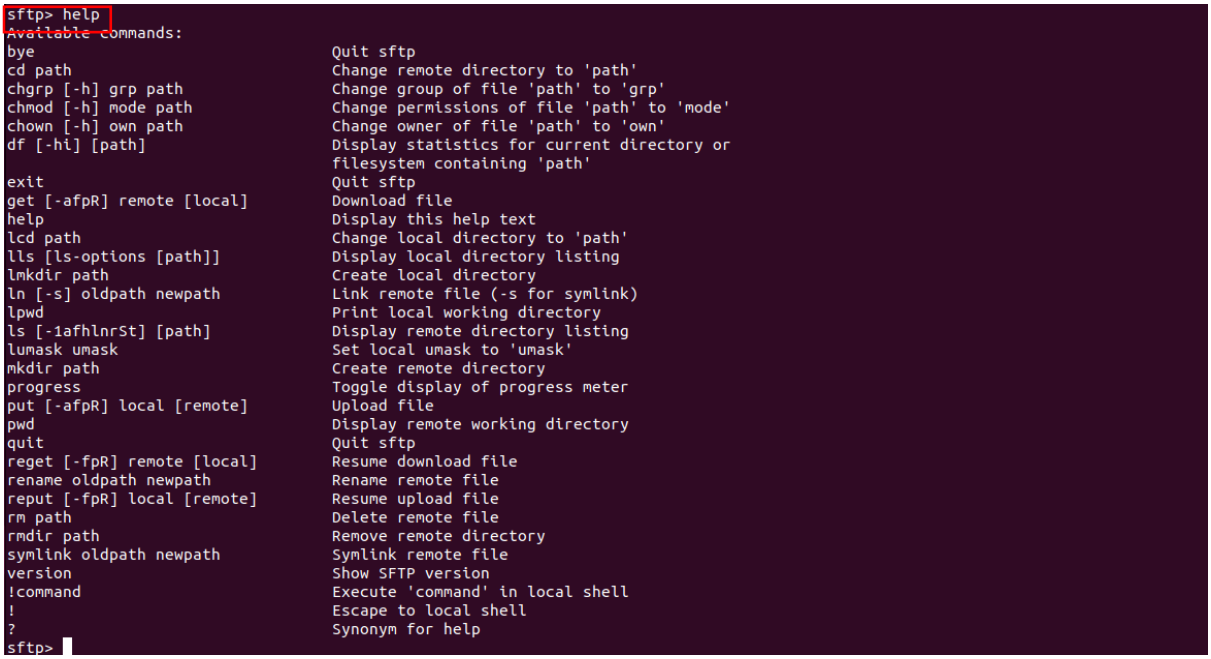
8. Use ‘get’ command to copy file



9. **Now, you can check files have been transferred from Linux Mint (Server) to Ubuntu (Client)**



10. **Check other sftp commands by typing help**

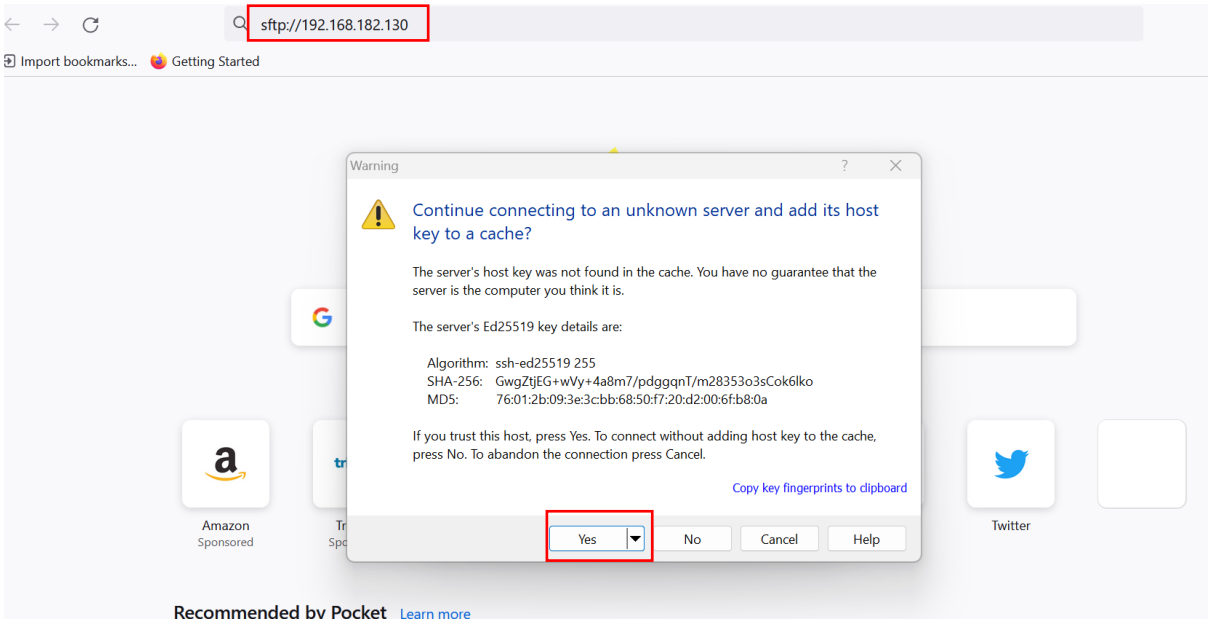


Other ways to copy files

Once authentication is completed and connection is done successfully, we can also use following ways to copy the files.

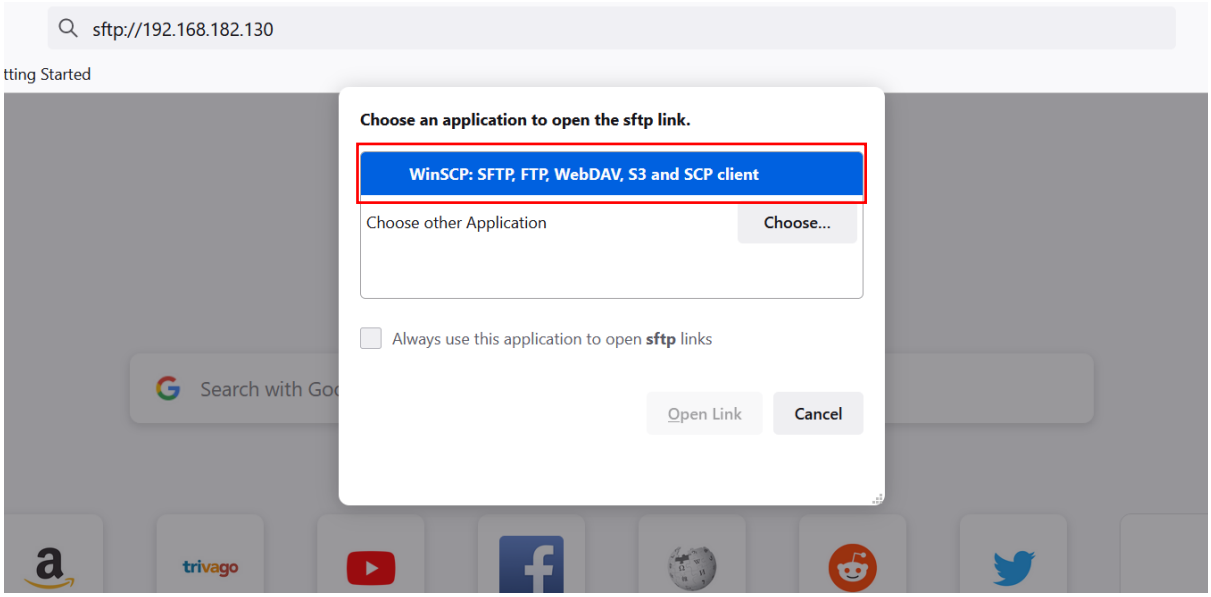
i. Web browser.
ii. File browser.

Use IP of Linux Mint (Server) IP

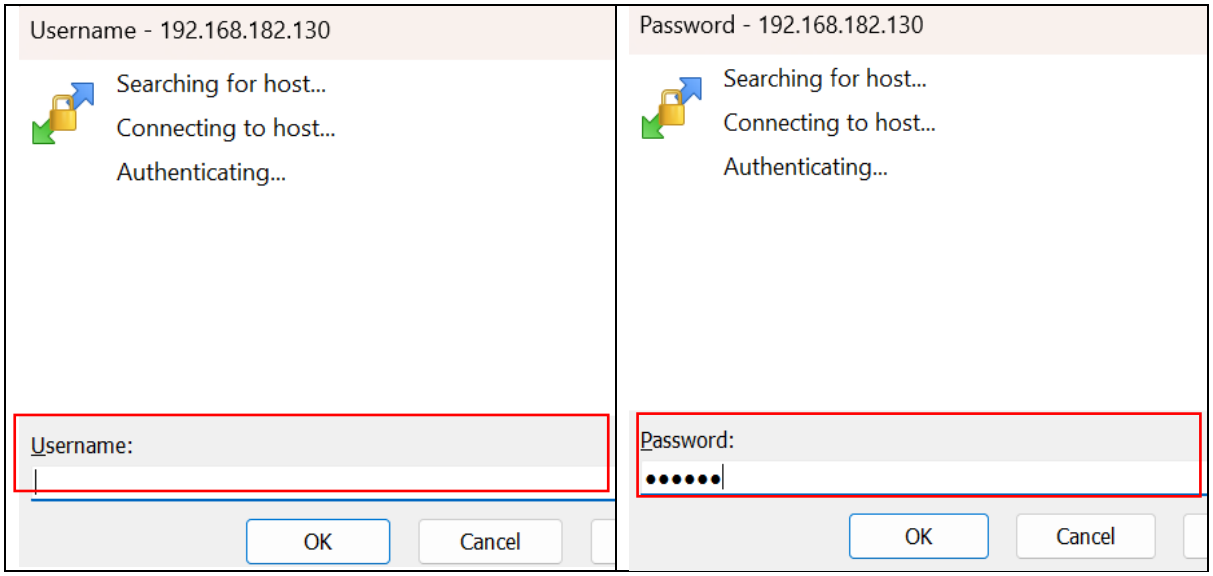


I am using WinSCP application to open the sftp link.

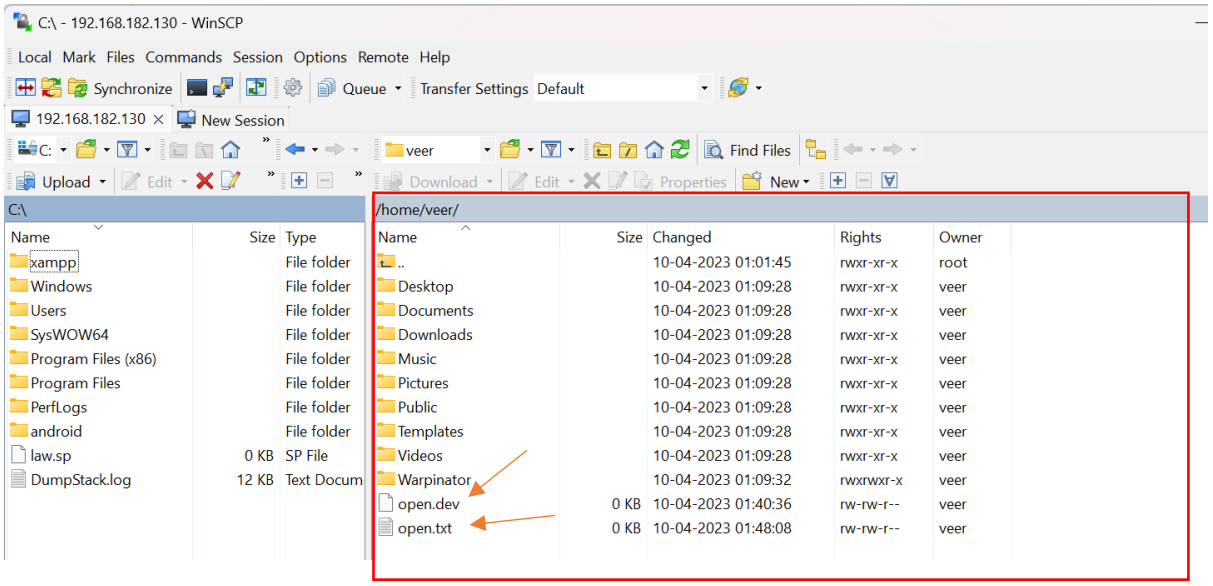
WinSCP is a free and open-source SSH File Transfer Protocol, File Transfer Protocol, WebDAV, Amazon S3, and secure copy protocol client for Microsoft Windows. Its main function is secure file transfer between a local computer and a remote server.



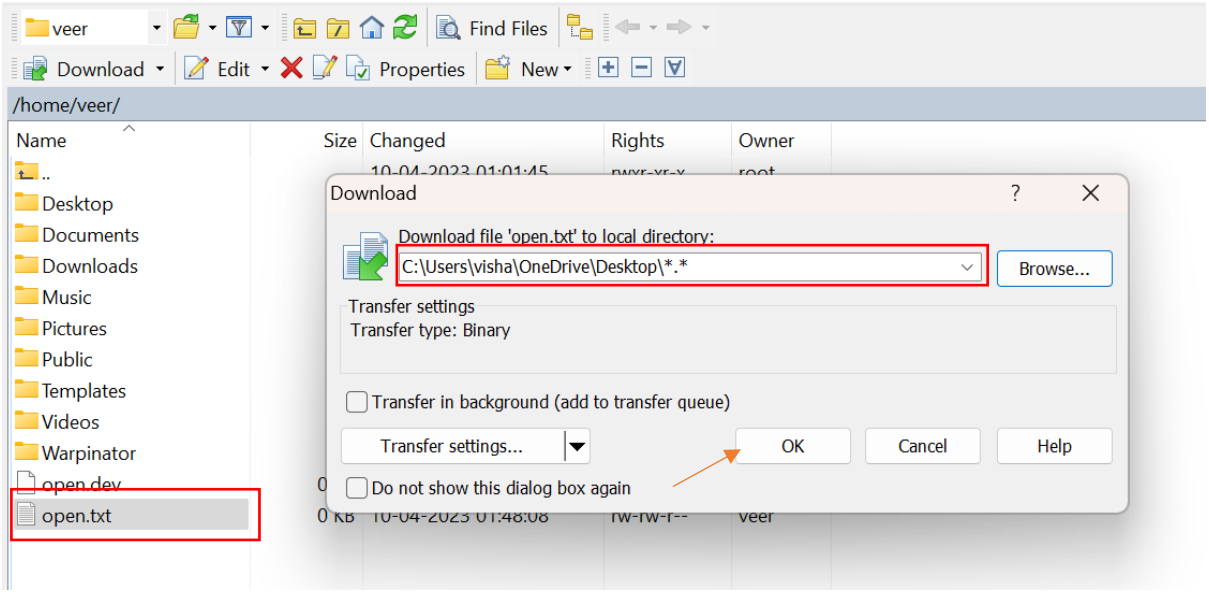
Enter username and password



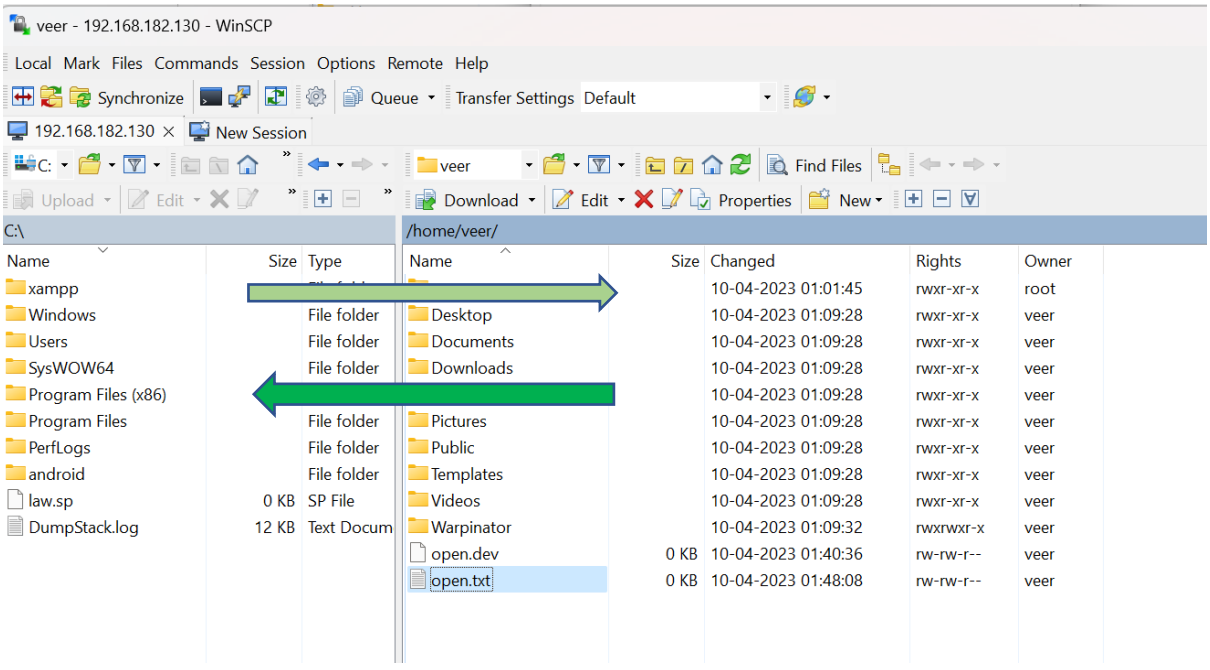
See the files



Click on the filename and download it



You may access the files of Linux Mint directly by WinSCP application and do multiple things according to your requirement.



4. Reference/ Bibliography

1. Wikipedia
2. Google