

Transcriptome Data Analysis in Non-model Organisms

Ponsit Sathapondecha Jiratchaya Nuanpirom
Prasert Yodsawat

2/28/23

Table of contents

Preface

This is a Quarto book.

To learn more about Quarto books visit <https://quarto.org/docs/books>.

1 + 1

[1] 2

1 Introduction to MobaXterm, Terminal, and SSH

1.1 MobaXterm (for Windows)

MobaXterm is a toolbox for remote computing. In a single Windows application, it provides loads of functions that are tailored for programmers, webmasters, IT administrators and pretty much all users who need to handle their remote jobs in a more simple fashion. MobaXterm provides all the important remote network tools, such as SSH, X11, RDP, VNC, FTP, MOSH, and of course, Unix commands, and many more!

There are many advantages of having an All-In-One network application for your remote tasks, e.g. when you use SSH to connect to a remote server, a graphical SFTP browser will automatically pop up in order to directly edit your remote files.

Visit MobaXterm official website to see a demo: <https://mobaxterm.mobatek.net/demo.html>

1.2 Terminal (for macOS)

Terminal provides a command-line interface to macOS. Each window in Terminal represents an instance of a shell process. The window contains a prompt that indicates you can enter a command. The prompt you see depends on your Terminal and shell settings, but it often includes the name of the host you're logged in to, your current working folder, your user name, and a prompt symbol. For example, if a user named michael is using the default zsh shell, the prompt appears as:

```
michael@MacBook-Pro ~ %
```

This indicates that the user named michael is logged in to a computer named MacBook-Pro, and the current folder is his home folder, indicated by the tilde (~).

MacOS features a built-in SSH client called Terminal which allows you to quickly and easily connect to a server. Starting from open the “terminal” app, and enter the standard SSH command:

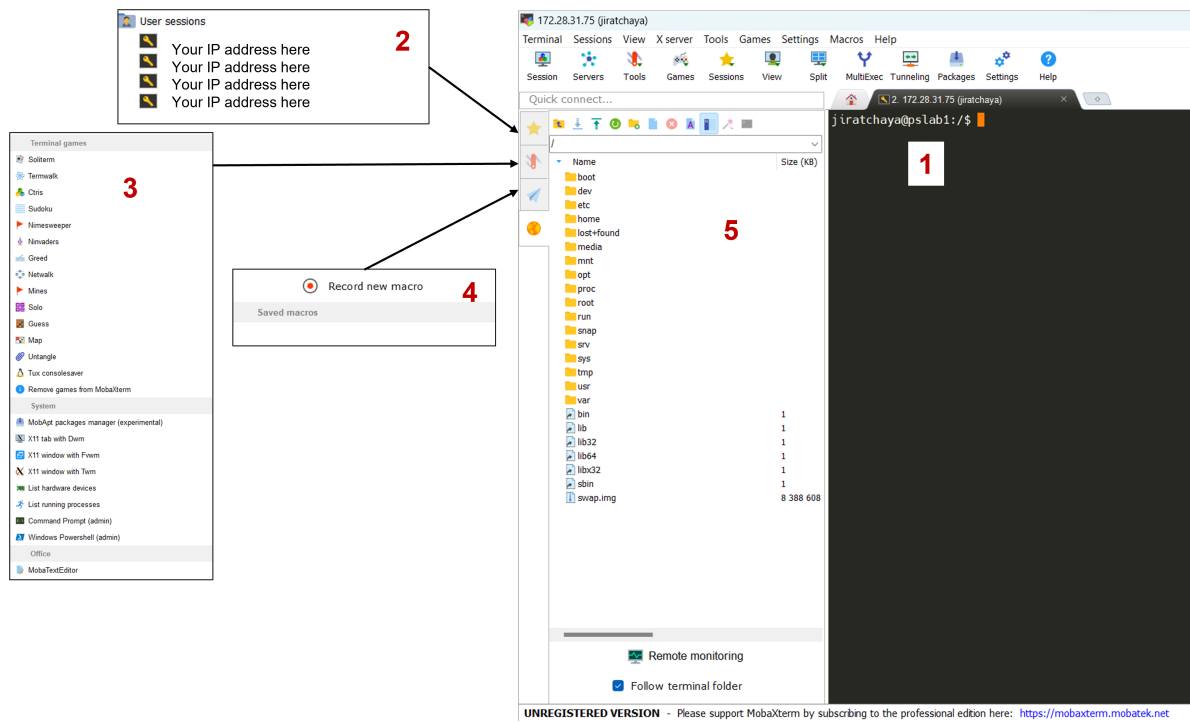


Figure 1.1: MobaXterm user interface. In the context of remote access through SSH and FTP, mobaXterm provides easy-to-access route as (1) a secure shell (SSH) terminal of the remote server, (2) a list of remote server you've accessed, (3) Utilities facilitating remote server access including entertainment, like Swiss army knife!, (4) If you want to reduce redundant typing, just set macro to it, and (5) a files available in the current working directory in the remote server, you can also transfer files from remote server to your local computer using this route!

```
ssh user@IPAddress
```

This will connect to the server via SSH with the username ‘user’ and the default SSH port 22. The connection will look similar to the following:

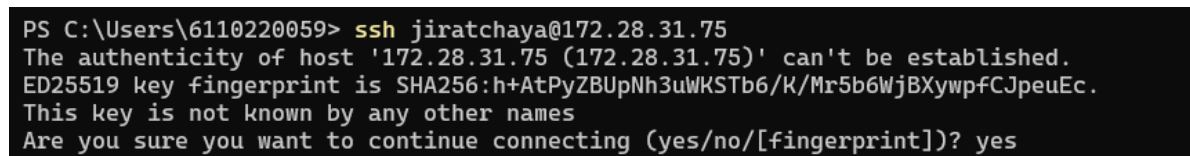
1.3 Connecting to Remote Server

Bioinformatics data processing tasks require more computing power than our laptops, so we need large servers or clusters. It’s likely you’ll work mostly over a network connection with remote machines on some projects. It can be frustrating for beginners to work with a remote machine. So, This part will introduce you to some commonly used bash commands. To make it easier for beginners to manage their remote machines, there are a range of different tools and technologies available, such as SSH, FTP, and terminal commands, which can be used to access and manage the environment of the machine. Additionally, there are a variety of bash commands which can be used to streamline the process of managing the machine.

What you need to know for connecting to a remote server:

1. Your username and password in the remote server
2. IP address of the remote server, and which port to connect to server
3. You should know whether the remote server accessible via local network or a public IP address

By default, SSH uses port 22 but it can be changed to a non-standard port. To securely connect the client to the remote server, SSH uses symmetric encryption, asymmetric encryption, and hashing. If you’re connecting for the first time, you’ll be asked to verify the server’s public key. Whenever you connect to the same server in the future, the client will reference this verified public key. During an SSH connection, the client and server negotiate a session key used to encrypt and decrypt data.

A terminal window with a black background and white text. The prompt is 'PS C:\Users\6110220059>'. The user has entered 'ssh jiratchaya@172.28.31.75'. The output shows a warning about the host's authenticity, the SHA256 fingerprint, and a prompt to confirm the connection.

```
PS C:\Users\6110220059> ssh jiratchaya@172.28.31.75
The authenticity of host '172.28.31.75 (172.28.31.75)' can't be established.
ED25519 key fingerprint is SHA256:h+AtPyZBUph3uWKSTb6/K/Mr5b6WjBXywpfCJpeuEc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Figure 1.2: In order to establish a connection, SSH needs to verify SHA keys once connected for the first time. Once authentication is complete, the SSH connection is secure and can be trusted for future access.

Upon connecting to the remote server, you’ll see a welcome message like this

```

PS C:\Users\6110220059> ssh jiratchaya@172.28.31.75
jiratchaya@172.28.31.75's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-60-generic x86_64)

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

System information as of Mon Feb 27 12:30:54 PM +07 2023

System load: 0.00048828125   Processes:            688
Usage of /:  36.5% of 2.58TB Users logged in:          1
Memory usage: 0%           IPv4 address for docker0: 172.17.0.1
Swap usage:  0%            IPv4 address for eno12399: 172.28.31.173
Temperature: 39.0 C        IPv4 address for eno8303: 172.28.31.75

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

   https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

7 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Mon Feb 27 11:02:32 2023 from 172.28.121.108
jiratchaya@pslab1:~$ |

```

Figure 1.3: An example welcome message of server using Ubuntu, including general software and hardware status, information of the latest connection, as well as a prompt for user command.