E

Remote access manual

To facilitate remote access and file transfer, a VNC software and SFTP client are configured.

E.1. Remote access GUI mode; RealVNC

1. Enable SSH and VNC interfaces via **Menu** → **Preferences** → **Raspberry Pi Configuration** → **Interfaces**, selecting **Enabled** for both **SSH** and **VNC**.

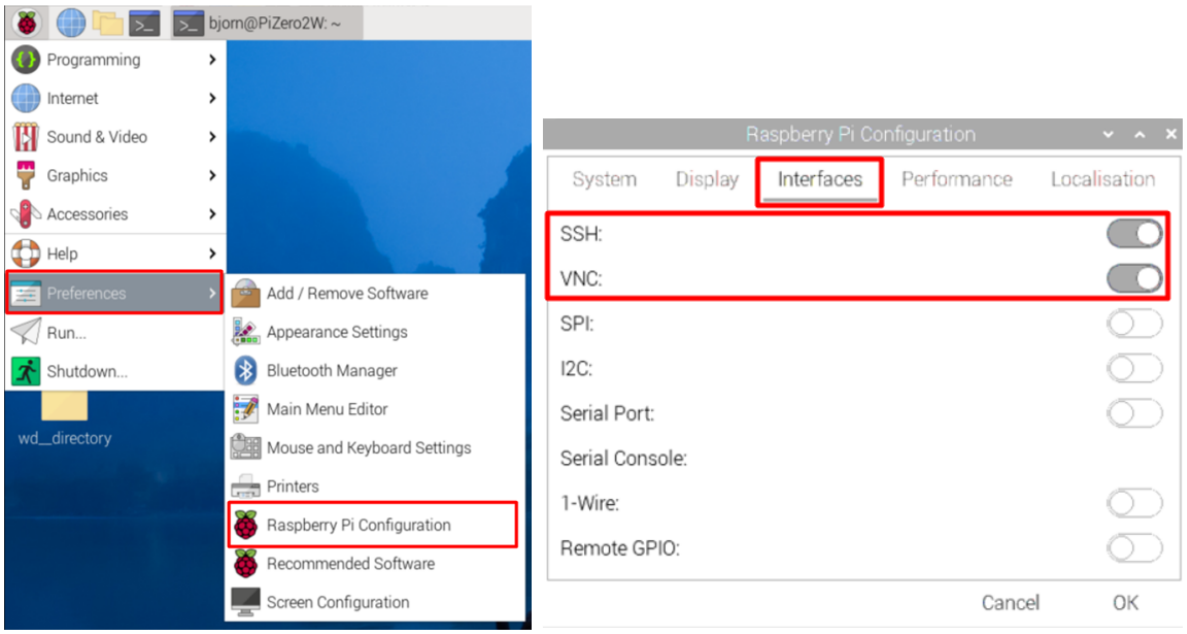

Figure E.1: Enable SSH and VNC settings in RPI environment.

2. From a workstation, download and install RealVNC Viewer (`https://www.realvnc.com/download/`).
3. In VNC Viewer, create a new connection using the Pi's IP address (visible by hovering over the network icon on the RPi desktop) as the VNC Server address.
4. Authenticate with the Pi user credentials configured during OS imaging; upon success, the Pi desktop is displayed for remote control.

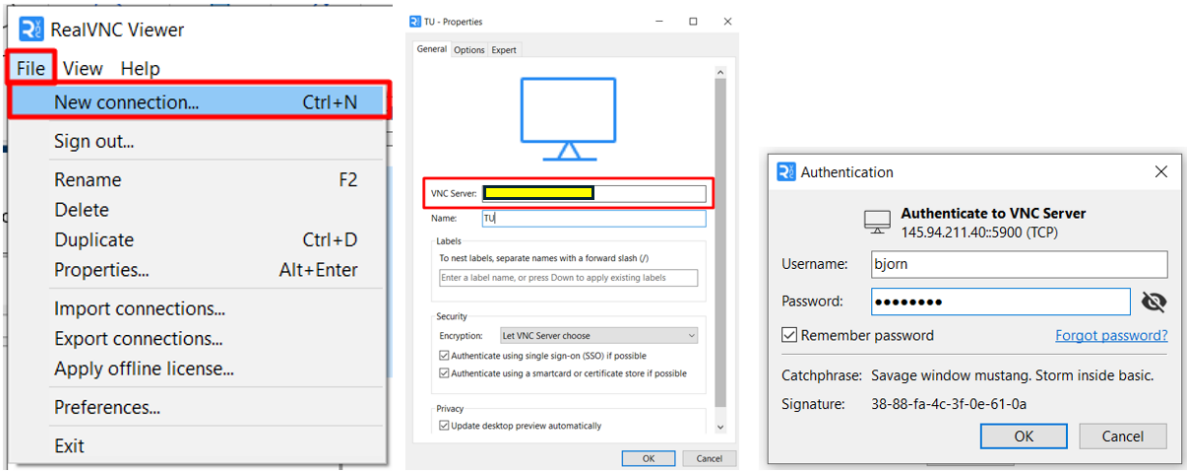

Figure E.2: Setting up a remote connection using RealVNC.

Now the system can be controlled form a pc assuming both systems are using the same internet connection.

E.2. Remote access CLI mode; SSH & PuTTY

In deployments where power savings dictate operating without a monitor or GUI, the Raspberry Pi must be accessed remotely via SSH over Wi-Fi or a mobile hotspot. The following steps describe enabling the SSH server, configuring wireless network credentials, and establishing an SSH connection from a Windows workstation using PuTTY(source PuTTY).

Initial SSH enablement (with monitor & keyboard)

1. Connect the Pi to a monitor and USB keyboard.
2. Open a terminal and run:

   ```
   sudo raspi-config
   ```

3. Navigate to **Interfacing Options** → **SSH**, select **Enable**, then **OK**.

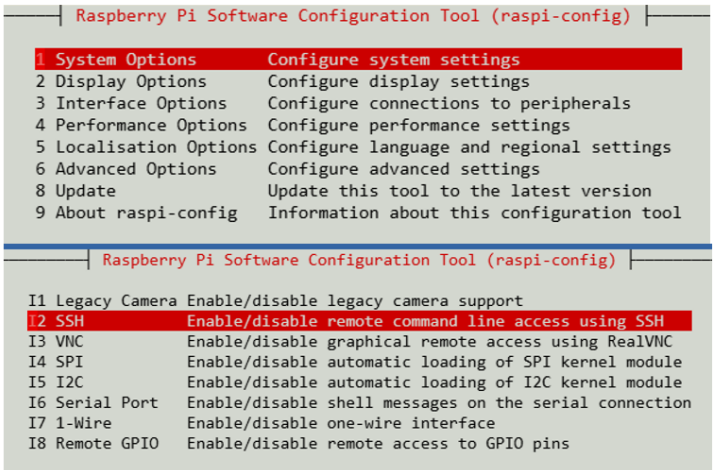

Figure E.3: Set interfacing options.

Configure Wi-Fi credentials:

4. In the same `raspi-config` tool, go to **System Options → Wireless LAN**.

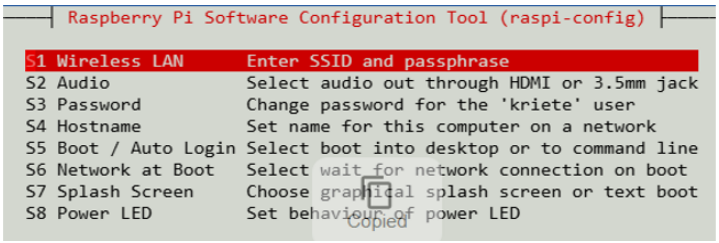

Figure E.4: Configure Wireless LAN connection.

5. Enter your hotspot's SSID and passphrase when prompted.
6. Exit and allow the Pi to reboot (if prompted).

Determine the Pi's IP address on the hotspot:

7. Open a terminal and run:

```
ip a
```

8. Note the address listed under the Wi-Fi interface.

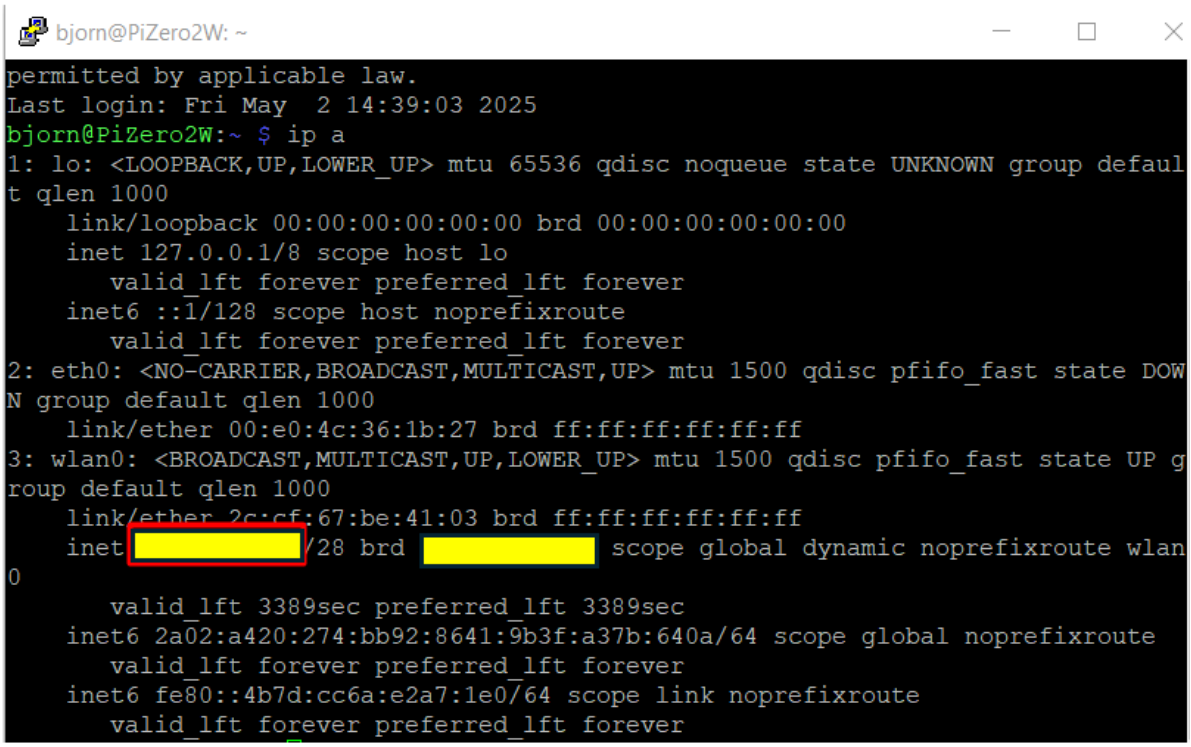

Figure E.5: Location of IP-address

Establish the SSH connection:

9. Download and install PuTTY from `https://www.putty.org/`
10. Launch PuTTY.
11. In **Host Name (or IP address)** enter the Pi's IP from step 8.
12. Ensure **Port** is set to 22 and **Connection type** is SSH.

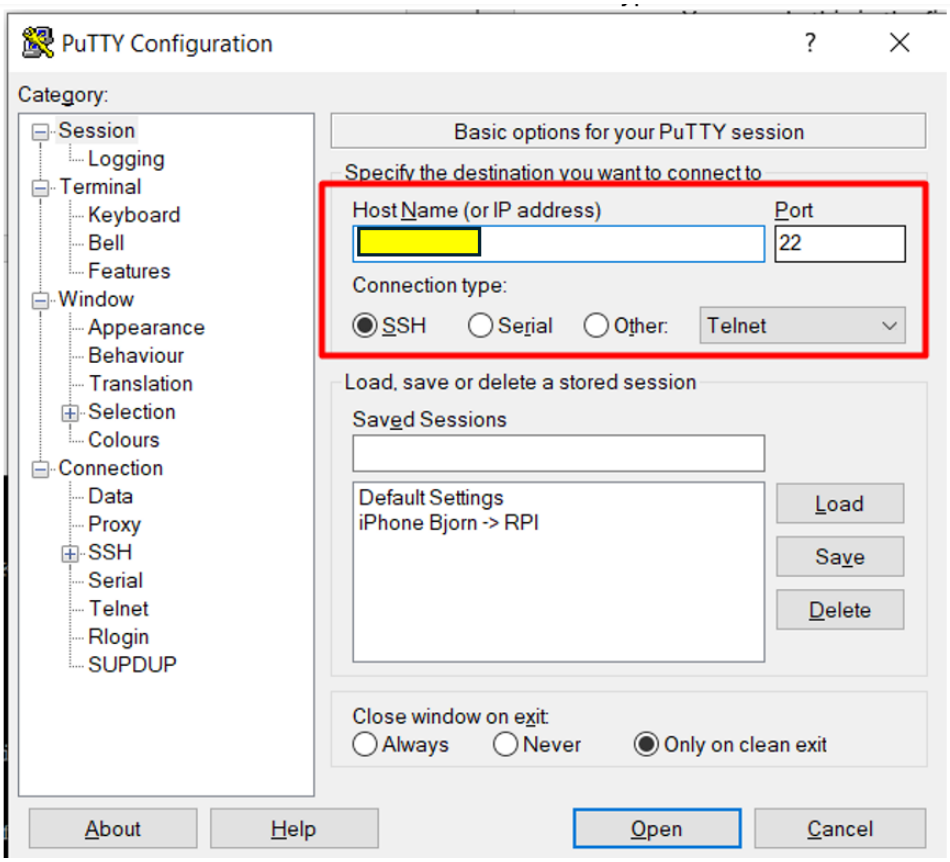

Figure E.6: Insert Host name/ IP-address

13. Click **Open**, then log in with your Raspberry Pi username and password.

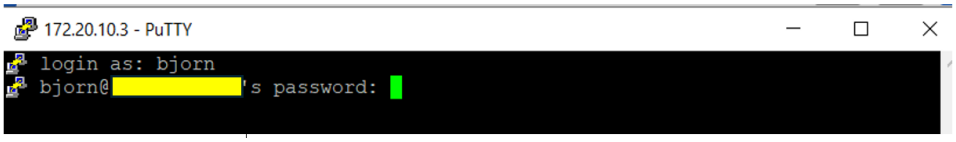

Figure E.7: Login interface for PuTTY

Once connected, you can manage the Pi entirely via the terminal in CLI mode.

E.3. SFTP file transfer via WinSCP

To enable reliable file transfer, the SFTP client WinSCP is configured.

1. Install WinSCP on the workstation (`https://winscp.net/`).
2. Launch WinSCP and configure a New Site with:
   - File protocol: **SFTP**
   - Host name: `Pi IP address`
   - Port number: `<standard>`
   - User name: `<username>` (as set in the OS imager)
   - Password: `<password>` (as set in the OS imager)
3. Save the site and connect; navigate to the project output directory (e.g. `/home/pi/wd_directory/output/`) to upload or download images, logs, and CSV files.

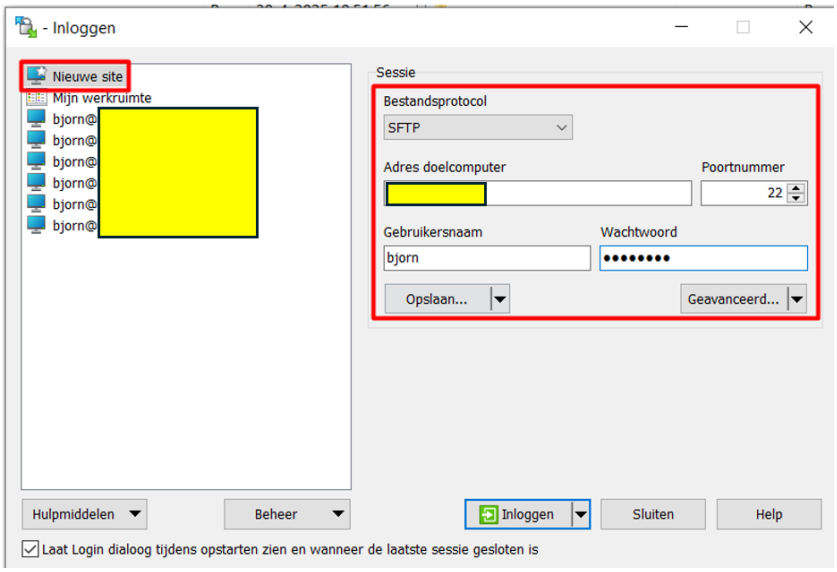

Figure E.8: Setup file transfer configuration.

Once connected, WinSCP can also be used to upload the entire project directory (cloned from the GitHub repository) to the Pi. Simply clone the wd__directory locally on your workstation (e.g. via git clone (GitHub link)), then in WinSCP's local pane navigate to that folder and drag it into /home/pi/ on the remote pane. This transfers all scripts, modules, and configuration files in one step, ready for execution.