HOW TO SET UP AN SFTP CONNECTION AND UPLOAD AN ENCRYPTED FILE (WINDOWS)

WARNING: ONLY CONNECT TO TRUSTED REMOTE SERVERS AND NEVER SHARE SENSITIVE DATA WITH SOURCES THAT YOU DO NOT KNOW AND TRUST THOROUGHLY.

INTRODUCTION: *The use of the Secure File Transfer Protocol (SFTP) is a common industry standard for technical analysts in a variety of fields. Any person that is expected to send files with sensitive data (e.g., Personally Identifiable Information) will need to know how to encrypt files using a key and utilize an SFTP file-sharing service to communicate necessary information. This process helps to reduce the risk of data leakage while communicating crucial information about finances, health coverage, and more.*

REQUIRED MATERIALS: You'll need a computer (Windows) with an operable web browser and a reliable internet connection. Any fully-updated web browser will work.

STEP 1: CHECK YOUR SYSTEM DETAILS

It's important to verify that your system can handle running the recommended software.

Press the Windows key and select the gear on the left of the menu. In the window that populates, click the "system" icon, and then scroll down to "About," an option on the left-hand side of the menu. Clicking this will reveal your system details. Verify that you're using Windows 7 or above, a 64-bit processor (or above), at least 2GB of RAM, and at least 3GB available disk space for installation (Shown in Figure 1).

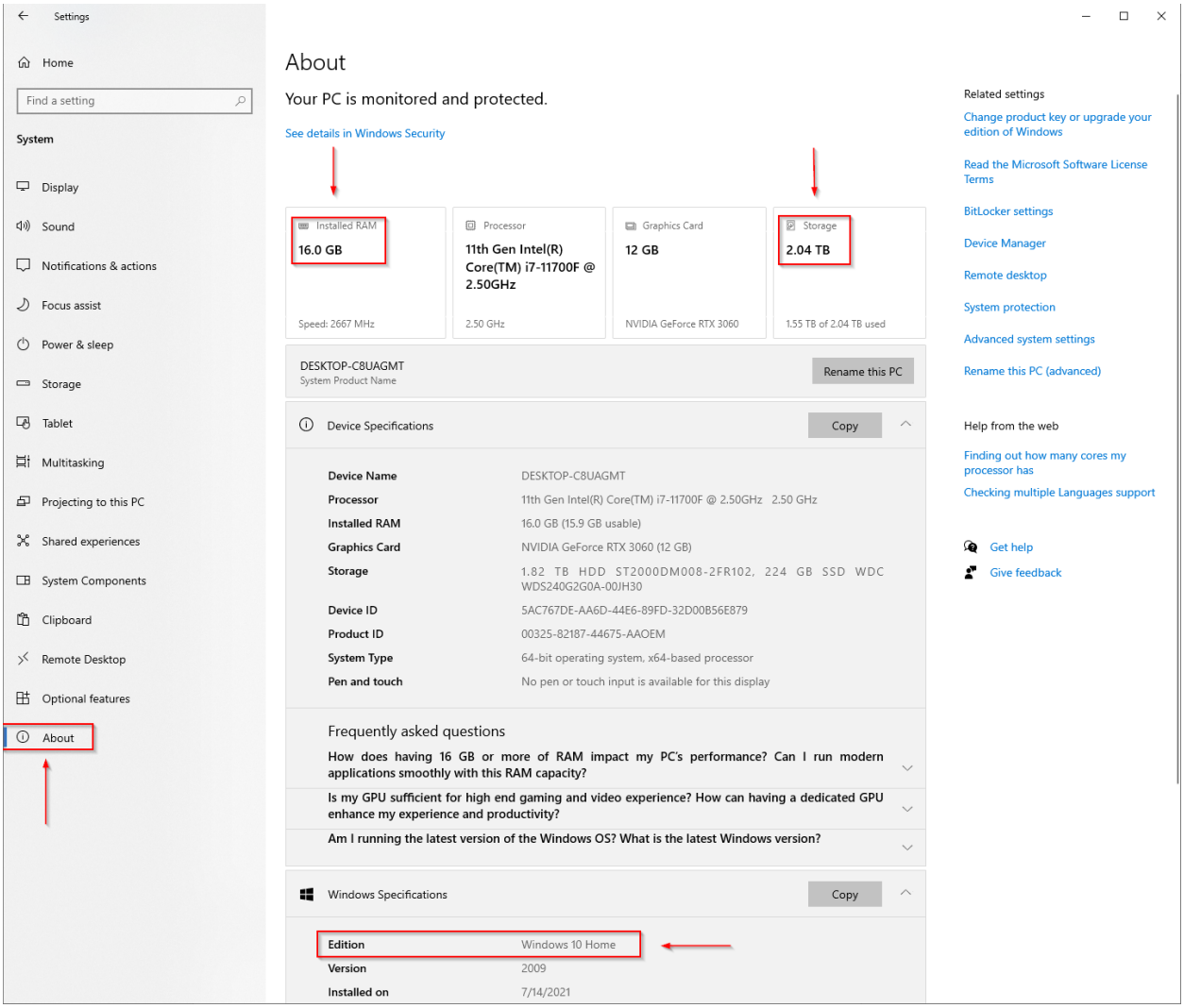
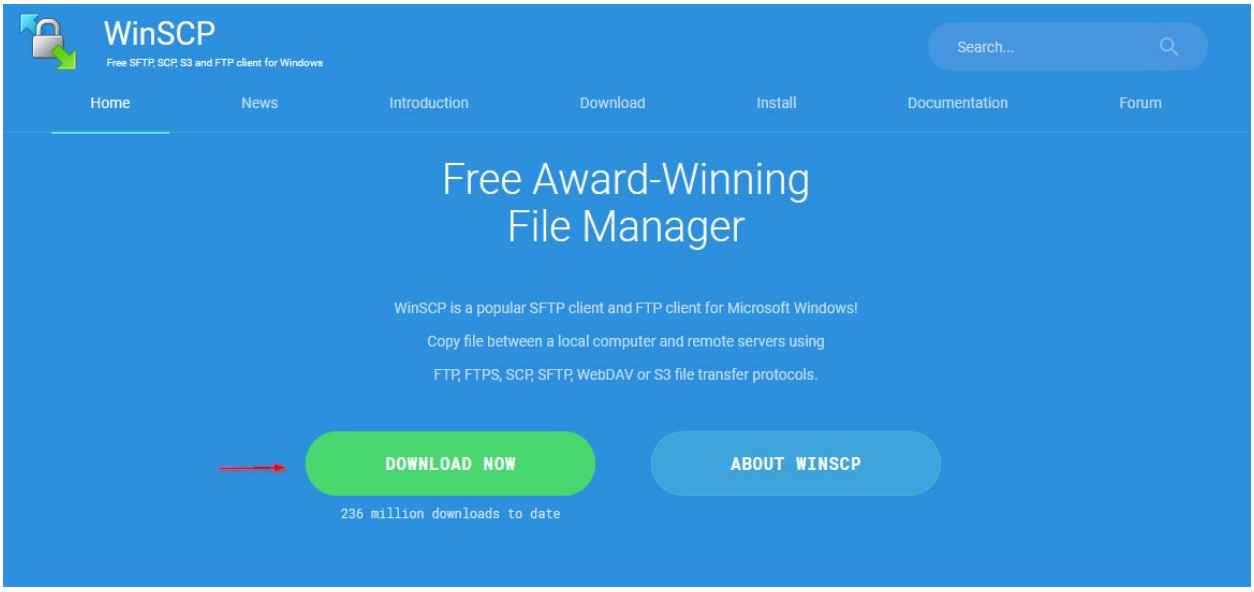


Figure 1

STEP 2: DOWNLOAD THE REQUIRED SOFTWARE

Now that we know your system can run the recommended software, you'll have to download it!

- Open your browser and navigate to https://winscp.net/eng/index.php (Figure 2)
- Download the software and run the installation wizard. Accept the license agreement and select the "Express Installation" option.
- Navigate to https://gpg4win.de/get-gpg4win.html and press the download button. (Figure 3)
- Run the installation wizard. Select the "Kleopatra" component and select an installation location.



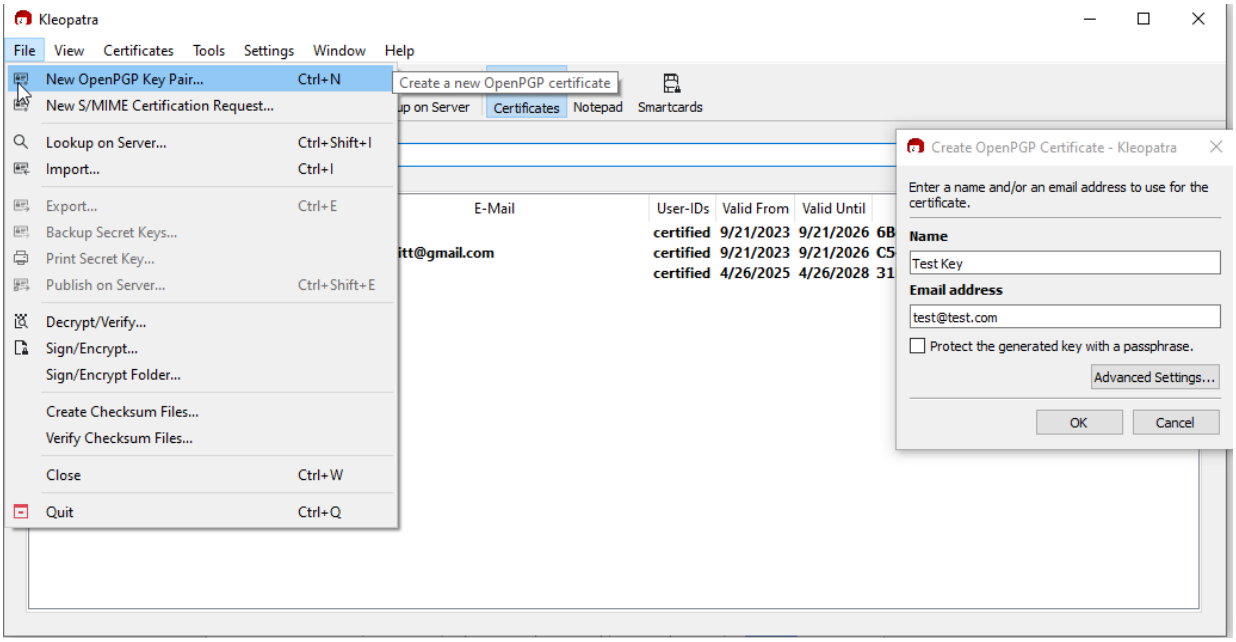
(Figure 2 above)

(Figure 3 above)

STEP 3: DETERMINE THE ENCRYPTION KEY THAT YOU WANT TO USE

Encryption keys can be public or private and may be in any file format – though they are often in .asc format. In a professional setting, the entity you are sending files to will usually provide the key that they want you to use. In this exercise, we'll create our own key! Alternatively, if you already have a key, just verify that it is the correct key for use with regard to the file you'll be sending.

- With Kleopatra open, click "File" > "New OpenPGP Key Pair." (Figure 4)
- Enter an associated name and email address in the designated fields.
- Press OK.



(Figure 4)

STEP 4: IMPORT THE KEY AND ENCRYPT YOUR FILE

There are two parts to this step. If you created your own key pair, the key is already in Kleopatra, and you can jump to part two.

PART 1

- Drag the key file into Kleopatra and select "Import Certificate" on the option box that populates.

PART 2

- Drag your file into Kleopatra and select "Sign/Encrypt" on the option box that populates. (Figure 5)
- Ensure that your key is shown and selected at the top. (Figure 6)
- Select "OK" > "Finish" to complete the encryption dialogue box flow. (Shown in Fig. 7)

Your encrypted file should now be shown in the folder containing its unencrypted counterpart.

Figure 5 above.

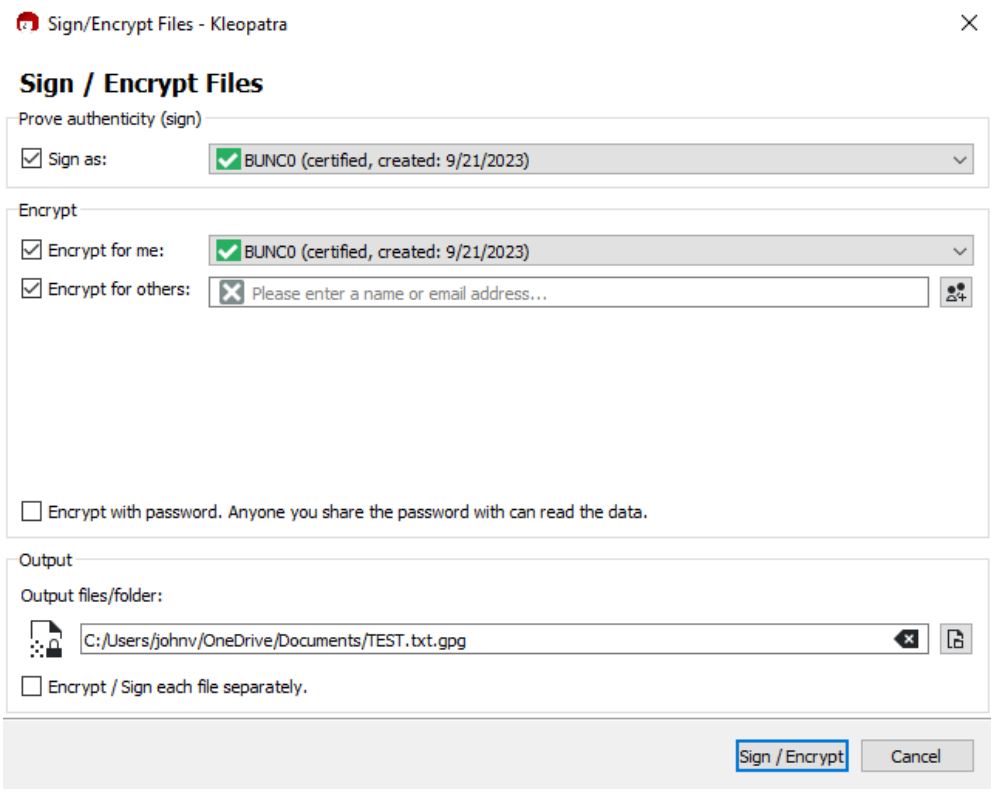


Figure 6 above.

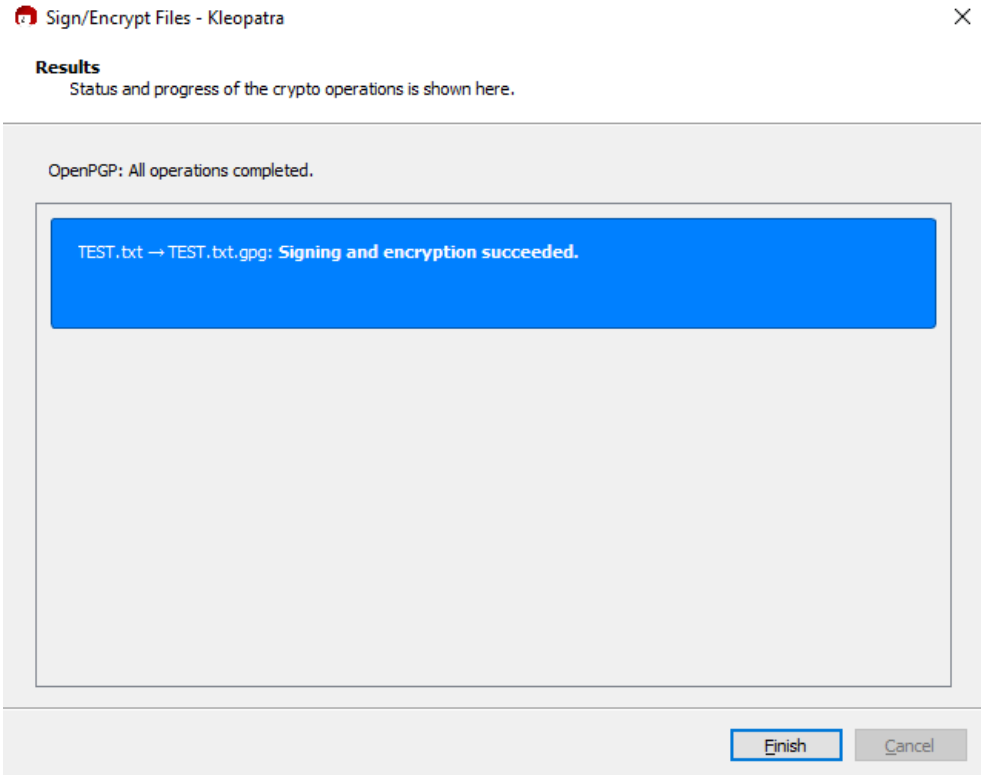


Figure 7 above.

STEP 5: ENTER SFTP LOGIN CREDENTIALS AND TEST THE CONNECTION

WinSCP is the tool you'll use to access the remote SFTP location. For this, the organization will have to provide you with connection details. This often includes a username, a password, a host URL, and a port number.

- Open WinSCP
- Click "New Connection," and enter the information in the designated fields.
- Press connect to test the connection.

If you are unable to connect using the information provided, you'll have to consult with the organization that will be receiving the file to obtain updated login credentials.

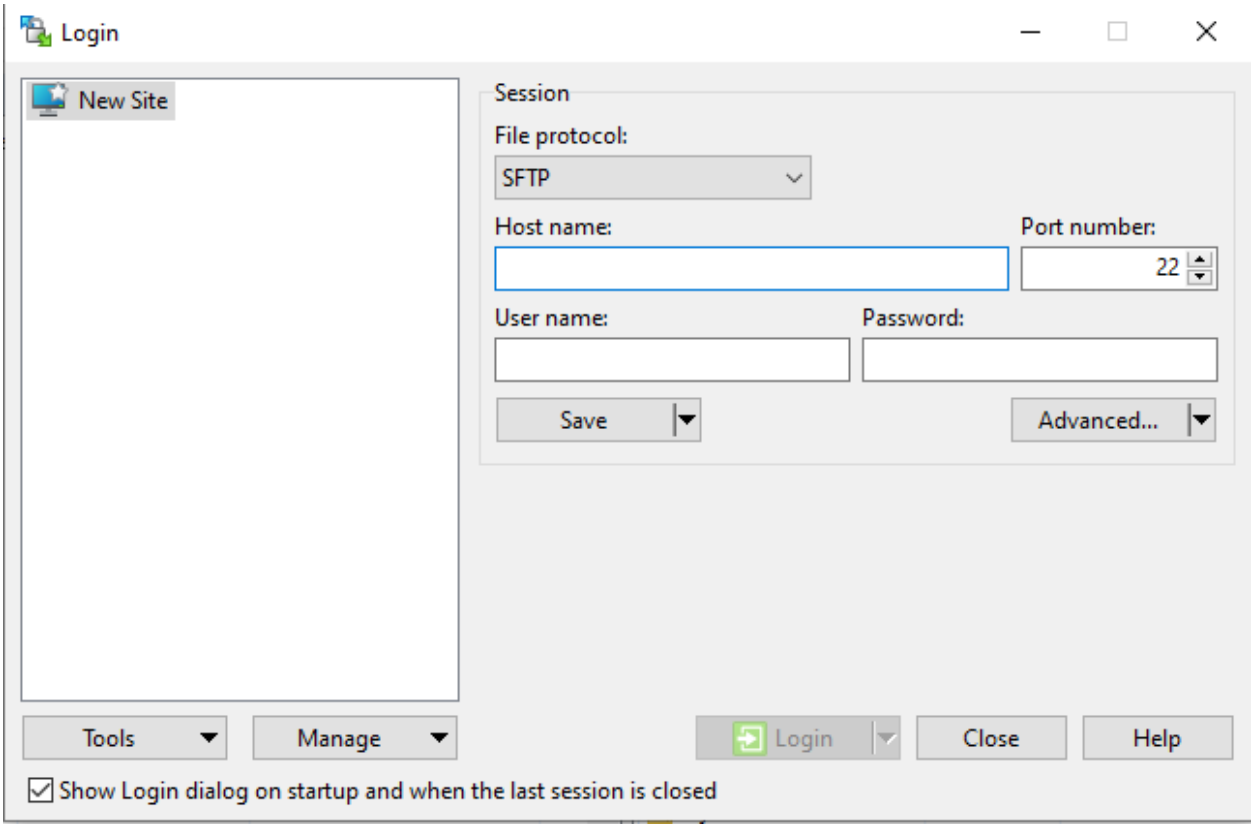


Figure 8 above shows the SFTP login screen within WinSCP.

STEP 6: SAVE THE CONNECTION FOR FUTURE USE

After you have verified that the connection details are valid, you'll want to save them for convenient access later.

- Press "New Connection."
- Type the connection details into the designated fields.
- Press "Save Connection."
- Enter the name you want the connection to have. Make it something you'll recognize!
- Press "Save."

STEP 7: NAVIGATE TO THE REQUIRED FILEPATH WITHIN THE SERVER

Many organizations will not want files placed into the root location. This is the location that you typically first see while accessing an SFTP location and is referenced as "/." A normal file destination will often look like "/Files/incoming/".

- To enter the required filepath, you may navigate to it as you would in a normal folder.
- (For hidden destinations) You can type the filepath in at the top left of the connection window.

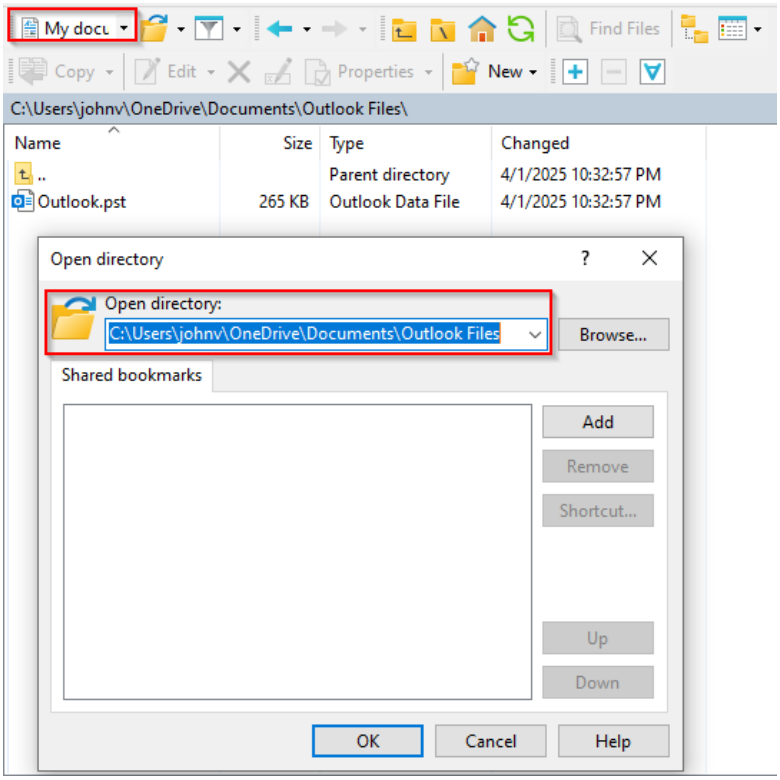


Figure 9 above shows where a user can enter a filepath.

STEP 8: DROP THE ENCRYPTED FILE INTO THE OPEN FOLDER

This step requires attention to detail. Ensure that you are moving the correct file. It is easy to accidentally move the unencrypted file, which is not what you want!

- Carefully click the encrypted file and drag it into the connection window at the desired file destination. (Shown in Fig. 10)

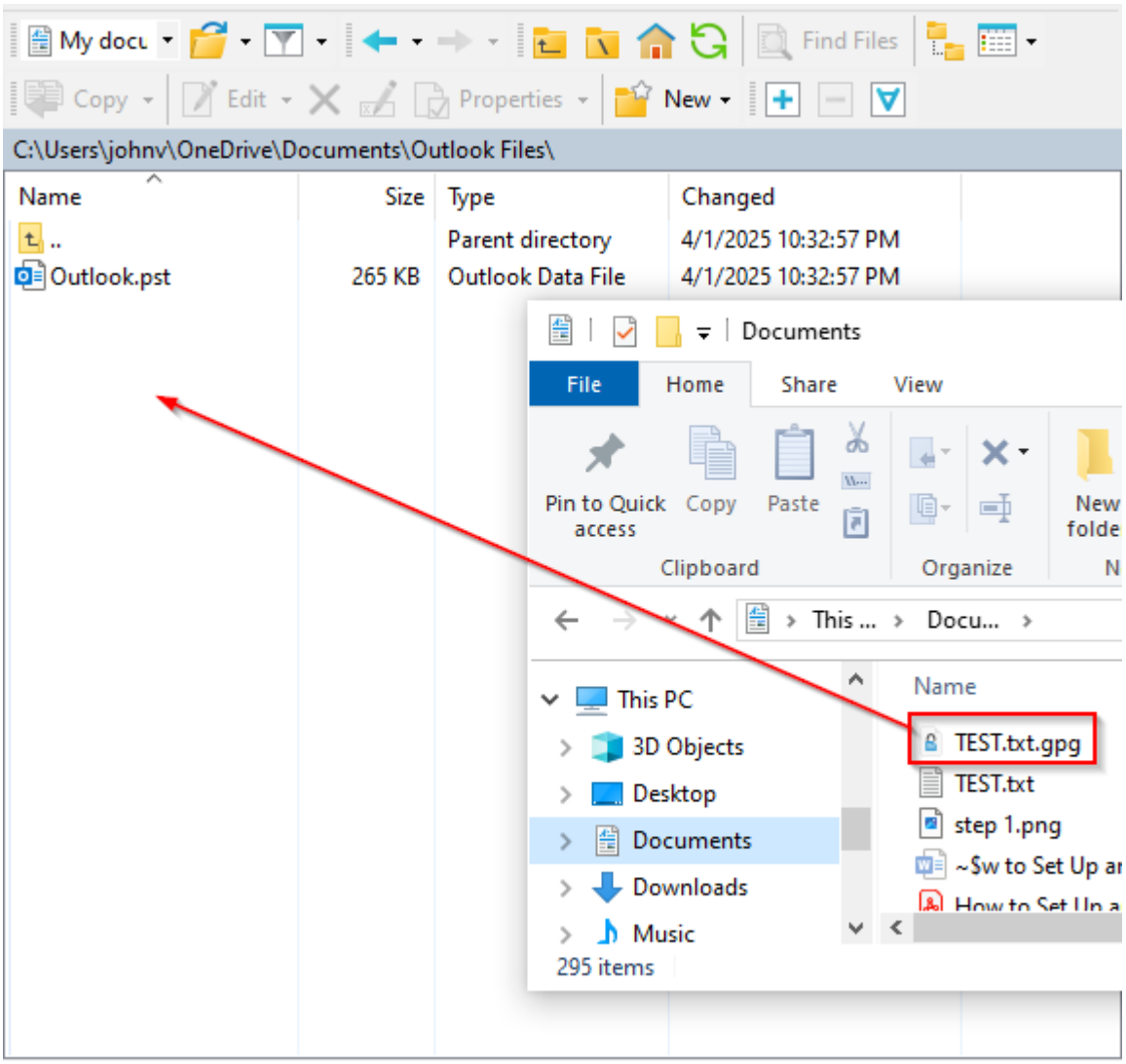


Figure 10 above.

STEP 9: CLOSE THE CONNECTION TAB IN WINSCP

If the connection is not closed after your business is concluded, it may cause problems for others who need to access the server. It is also an important safety step!

- Close the connection window

STEP 10: [OPTIONAL] KEEP A LOCAL COPY OF FILES THAT ARE SENT.

This step is optional but recommended. Keep a local record of what you've sent and where by placing a copy of all the files you send into a folder. If they are files associated with a client, name the folder after that client. This extra step will be important in the event that you must perform a data audit. You will have the ability to resend past files, as well as ensure that the data included on those files was accurate and complete. Many companies have record-retention requirements, so make sure you're in compliance if this is the case for you!


Great Work! You successfully encrypted and transferred a file via SFTP.