



MULTIMEDIA TOOLBOX

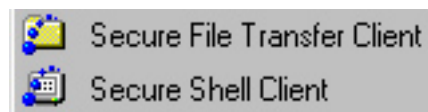
Using Multimedia Tools for Education

FROM FTP TO SSH SECURE SHELL: TRANSFERRING FILES ON THE NETWORK

Ruth Dahl, Centre for Innovation in Teaching and Learning

A lot of academics need to transfer files from their computer to various servers or they may need to download files from a server. Sometimes this server is our server, sometimes it is on a remote site. We are used to using FTP (File Transfer Protocol), a program that makes it easy to connect a computer to a server for uploading and downloading files, to accomplish this task. To enable us to do this smoothly, the University has made the WS FTP program freely available in the past.

Those of us on campus who have received a new Dell computer in the last few weeks will soon realize that the WS FTP program we are all so used to using is no longer part of the loaded software. It has been replaced by the SSH Secure Shell Client for network communications between users and the University servers. This was done for security reasons. Network security is a huge concern for the University. The software is designed to protect network communications against security hazards. It provides secure network sessions by utilizing secure encryption. It is used for all FTP and Telnet communications. The program consists of 2 small applications; SSH Secure Shell Client and the SSH Secure File Transfer Client.



The Secure Shell Client opens a terminal window. All functions and tasks one normally carries out in Telnet can be done in the Secure Shell Client. Secure File Transfer Client opens a file transfer window. All uploading, downloading, and other FTP functions that have been done in WS FTP or any other FTP program can be carried out in the Secure File Transfer Client.

If the SSH Secure Shell software is already installed on your computer, it can be accessed through the Start menu (Start > Programs > SSH Secure Shell > Secure File Transfer Client or Secure Shell Client) or by double clicking on the short cut icon on the desktop. Those on campus with a new Dell computer, you will find the program icons in the U of W Apps folder > SSH Communications folder. For those who do not have this program installed on their computers and would like to start using it, you can download it from

<http://commerce.ssh.com/index.html>

Secure Shell Client

Starting the Secure Shell Client application opens up the following program interface, see Figure 1.

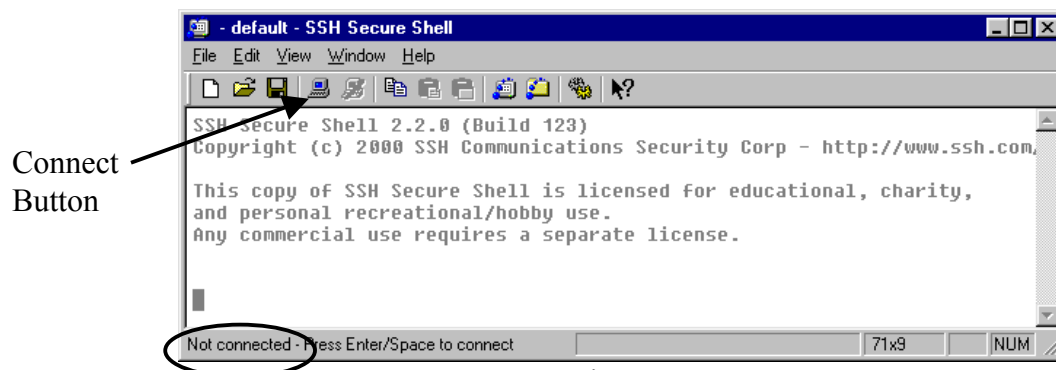


Figure 1

At this point there is no connection to a server. To connect to a server, select Connect under the File menu, or click the Connect button on the toolbar. A dialog box will appear where the user enters the appropriate Host Name (the server you wish to connect to), User Name, and Password. Click OK to connect. See Figure 2.

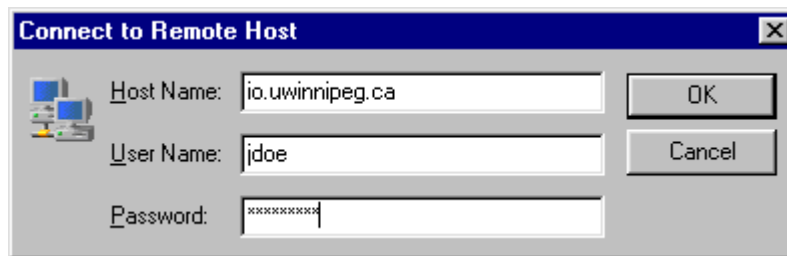


Figure 2

The Host Identification dialog box appears. See Figure 3. When you connect to a host (server) for the first time, the server will provide your computer with a "host public key". This key identifies the server that you are connecting to. Saving this key by clicking Yes will store this key on your computer. If you regularly connect to this server, saving the key will allow you to bypass this Host Identification step the next time you login. It is not necessary to save it.

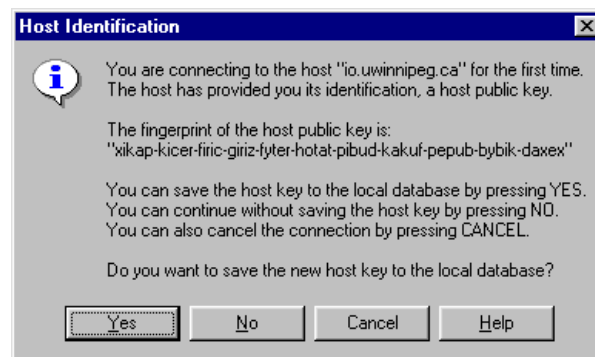


Figure 3

As stated previously, the terminal window is a secure replacement for Telnet connections. All functions normally carried out through Telnet can be carried out in this window through the command line interface. See Figure 4. Select Disconnect under the File menu to terminate the connection.



Figure 4

Starting the Secure File Transfer Client application opens up the following program interface, see Figure 5. To connect to the server, select Connect under the File menu or click the Connect button on the toolbar. The Connect to Remote Host dialog box appears followed by the Host identification box as described previously (Figures 2 and 3).

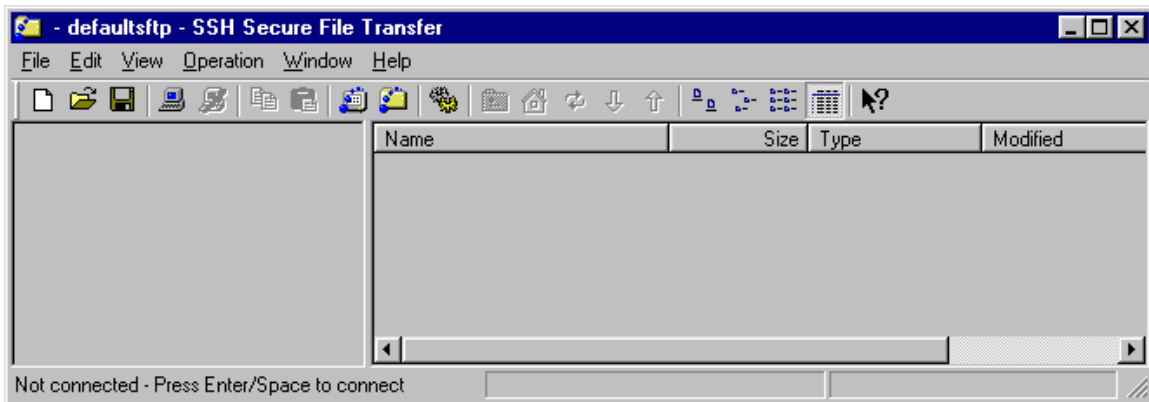


Figure 5

Once the user has successfully logged on to the server, all folders/files in the user's directory become visible. See Figure 6.

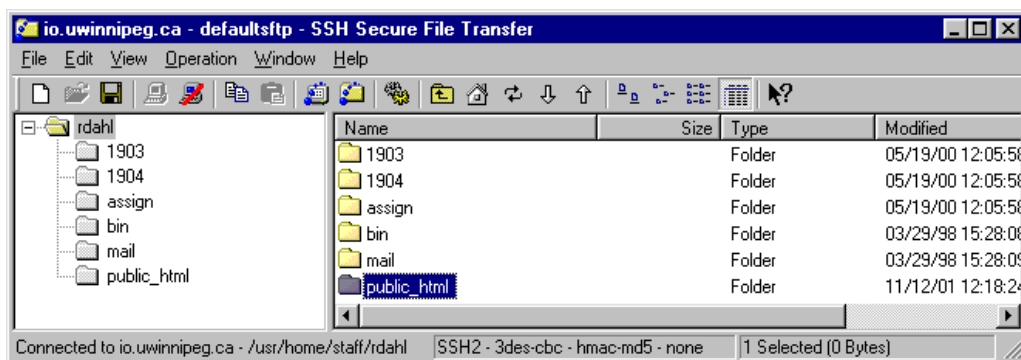


Figure 6

The Secure File Transfer interface is similar in functionality to Windows Explorer. Files or folders can be copied or moved to and from the server using familiar “drag and drop” mouse actions. Simply click and drag files from your computer into the appropriate folder within the Secure File Transfer interface. Drag and drop operations can be made easier by displaying all your computer files - Windows Explorer can be opened up directly from this application by selecting New Explorer from the Window menu. This way, all files on your computer as well as all files on the server to which you have access can be seen and accessed from your computer.

Files can be uploaded or downloaded by accessing the toolbar icons as well. Select the file to download off the server (from the Secure File Transfer Interface) and click the download button on the toolbar. You will be prompted to select a folder on your local hard drive into which the file will be downloaded. To upload a file, first highlight the folder within the Secure File Transfer window you wish to upload to. Click the Upload button on the tool bar. You will be prompted to select the folder/files on your local computer that you wish to upload to the server.

Uploading, downloading, as well as renaming files, deleting files, opening files, and creating new folders can also be done by accessing the Operation menu. Simply select the appropriate file/folder within the Secure File Transfer window, and select the desired action from the Operation menu. See Figure 7.

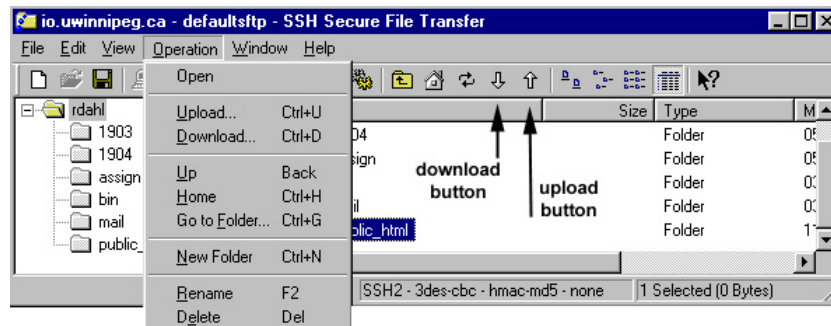


Figure 7

Please note that it is not possible to delete a remote folder that is not empty. First delete the files and all subfolders residing in the folder. Select Disconnect under the File menu to terminate the connection.

SSH Secure Shell Client is an easy to use, intuitive, secure means of network communication. Consider using it for all your Telnet and FTP operations through the University server(s). If you are logging in to the University from home, install the SSH Secure Shell Client on your home computer to ensure secure network communications.

Note: You cannot use the software to login to **any** remote server – the SSH software must be running on the remote server as well as on the local computer. If the remote server does not have the software, any attempt to log on with the SSH client will be unsuccessful. If logging on is a necessity, another type of FTP program (such as WS FTP) must be used.