



---

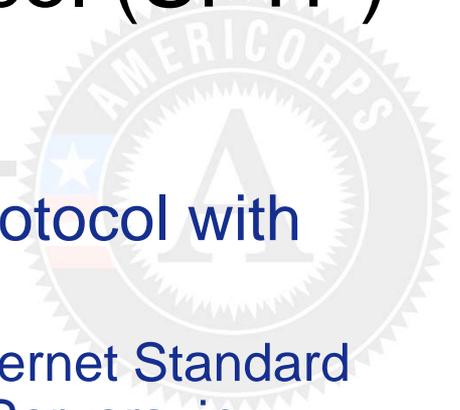
# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)

## What is a Secure File Transfer Protocol with Secure Copy???



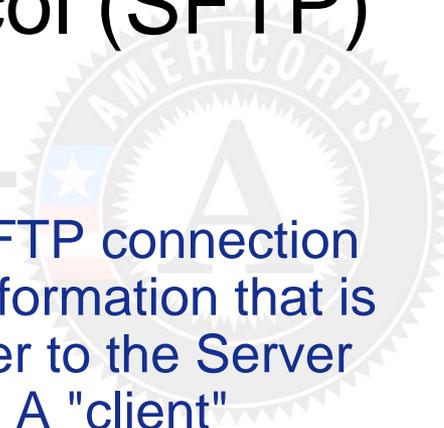
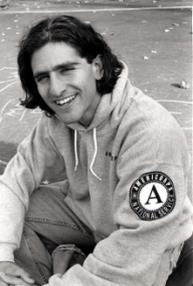
# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)

- What is a Secure File Transfer Protocol with Secure Copy???
- A Secure File Transfer Protocol is an Internet Standard for transferring data between computer Servers; in Delaware's case, between the Host Server within Delaware Health and Social Services (DHSS) and the remote sub-grantee location computers. This protocol basically allows one computer to talk to another. The Secure Copy allows the data to be encrypted so it must be dragged with the mouse from the SFTP into whatever application it has been created in; Word, Excel, Access, etc.

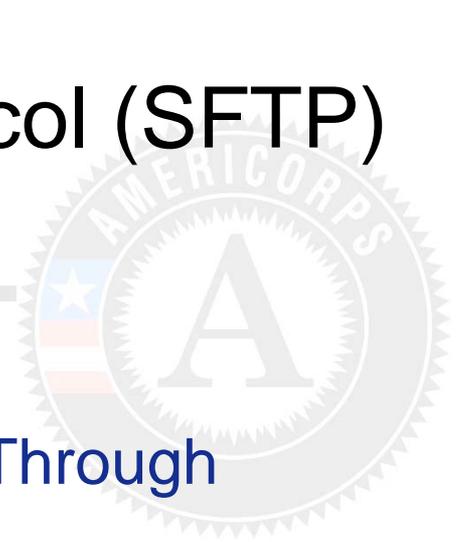


# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)

- Both locations provide a secure client SFTP connection to the DHSS Server by encrypting the information that is sent between the sub-grantee's computer to the Server and back to State office staff computers. A "client" means any program running on one computer that interacts with another program running on a Server).
- In order to input an SFTP with SC, the SFTP software must first be downloaded and established on both the Host Server computers and the remote location computers. This is done through the establishment of Public and Private Keys, which are basically secure recognition programs through each user's login and location set-up.



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)



- So how is this accomplished?? Through working directly with your State's.....



- Information Technology Department



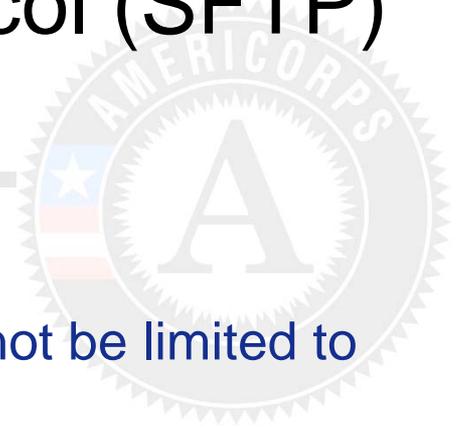
# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)



- My first thought when I contacted the Department's IT folks was to create an icon on our Division's home page. Each sub-grantee could then click the icon, enter a password, and access their own reports. SOV state office staff would then be able to enter a "master" password and retrieve the data.
- This was not a feasible solution, as in talking with the IT personnel, this method would require the remote sub-grantee computers to actually transfer their data into the State's Mainframe system, which raised several issues...



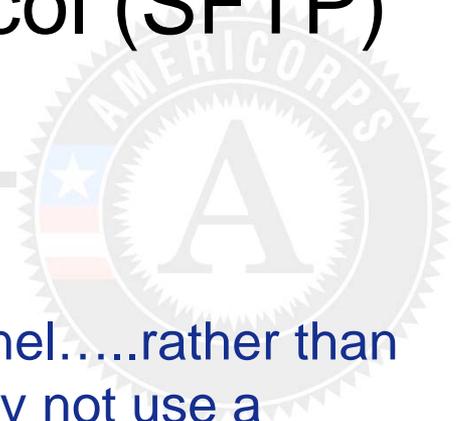
# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)



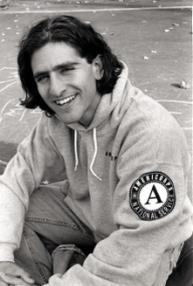
- The submitted sub-grantee data could not be limited to sole access to SOV personnel;
- The data could not be segregated from other data ports within the Server's Main-Fram;
- The data could not be properly protected;
- Because the sub-grantees were not state entities, their systems could not access the State's Firewall.



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)



- The next idea came from the IT personnel.....rather than an icon on the public State Website, why not use a direct-communication type of program that would allow the sub-grantee information to simply filter through our Mainframe and link directly to an external file on chosen state staff computers? After discussions regarding the formats of the reporting data, IT chose an SFTP application.

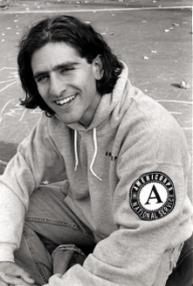


# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)

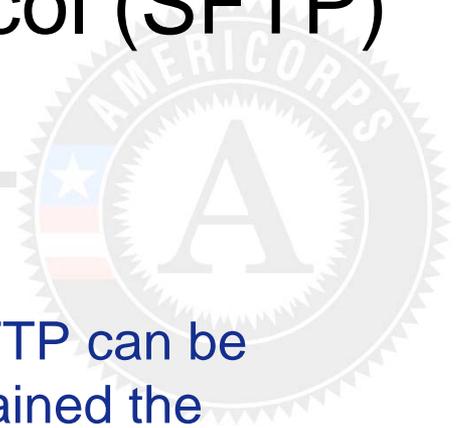


The next steps before downloading this program were:

1. Ensuring the data transmission ports between the remote sub-grantee's computers and the State's mainframe were accessible to each other.
2. Ensuring the sub-grantee's were registered with the state IT Department.
3. Collaboration between IT, SOV, and the sub-grantees throughout the entire process. IT personnel worked closely with the sub-grantees to help them set up the application on their end, pass through our firewall and access into our port, and establish their "Keys" for log-on.



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)



- Although there are several sites that SFTP can be downloaded from, our IT personnel obtained the application from [www.winscp.net](http://www.winscp.net)
- Once all of the sub-grantee registration information was updated, and both SOV staff and authorized sub-grantee staff had downloaded the application, our IT personnel began working in teams with all of us following the same process for installation. The following slides depict the steps necessary for connectivity of this application.



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)

- Once the program is downloaded and installed, the program window will open. In the window, click the *Profiles* button, then select *Add Profile*, as shown below.



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)



- Type a descriptive name for your profile and press the Enter key:

Add Profile

First/Last Name

Add to Profiles

Click the *Profiles* button again and select *Edit Profiles*. The Profiles dialog box will open. On the left side of this box, select the name of the Server for which you wish to create a profile. Then on the right side, in the *Connection* tab, enter the Server's host name in the *Host Name* box and your account's username in the *User Name* box. Select OK.



# Profiles

- Quick Connect
- Profiles
- Your Name

- Colors
- Tunneling
- File Transfer
- Favorite Folders
- Connection
- Cipher List
- Authentication
- Keyboard

Configure protocol settings for the connection. New settings will take effect upon next login.

Specify \* as the host name or the user name to be prompted for the information when the profile is chosen for connecting.

Host name:

User name:

Port number:

Encryption algorithm:

MAC algorithm:

Compression:

Terminal answerback:

Connect through firewall

Request tunnels only (disable terminal)

OK

Cancel



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)



## Connecting to a Server

To connect to a Server (for which you have already defined a profile, as previously described), click the *Profiles* button and select the profile name for that Server, as below:



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)

- The first time you connect to a Server, you will be asked to save a new host key in the local database. Select Yes. In the future when you connect to this Server, you will (usually) not be asked this again.
- You will then be prompted for your password, as shown below:



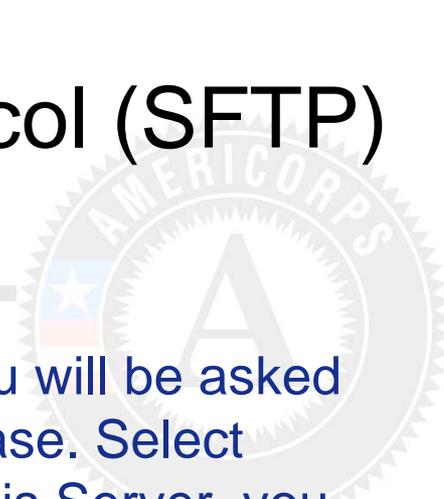
Enter Password

Password: xxxxxxxx

OK

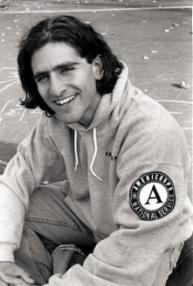
Cancel

Type your password and press Enter. This will connect you to the Server, and you will receive a command prompt for your account on the Server.



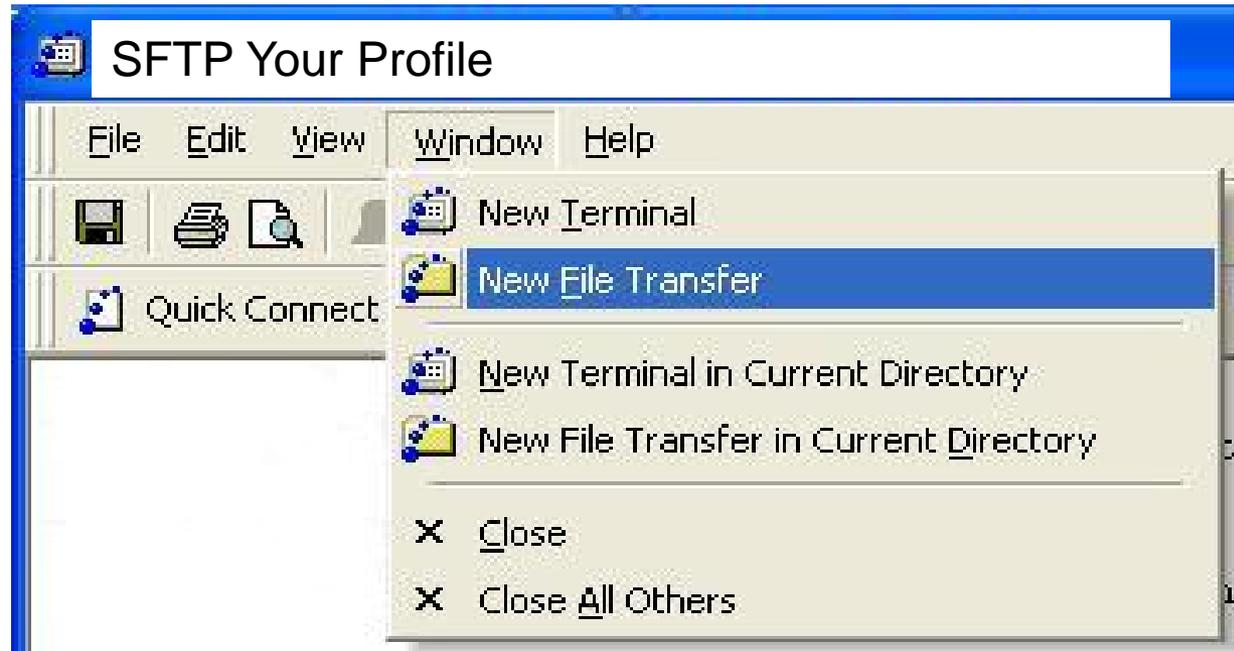
# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)

- **Transferring Files**
- We are now ready to transfer files, as all locations have now established a Profile for the main Server, and can now connect to the Server. NOW WHAT???



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)

- You need to open the SFTP client window by displaying the *Window* menu and selecting *New File Transfer*.



### 3:hubert.vcu.edu - Hubert - SSH Secure File Transfer

File Edit View Operation Window Help



Quick Connect Profiles

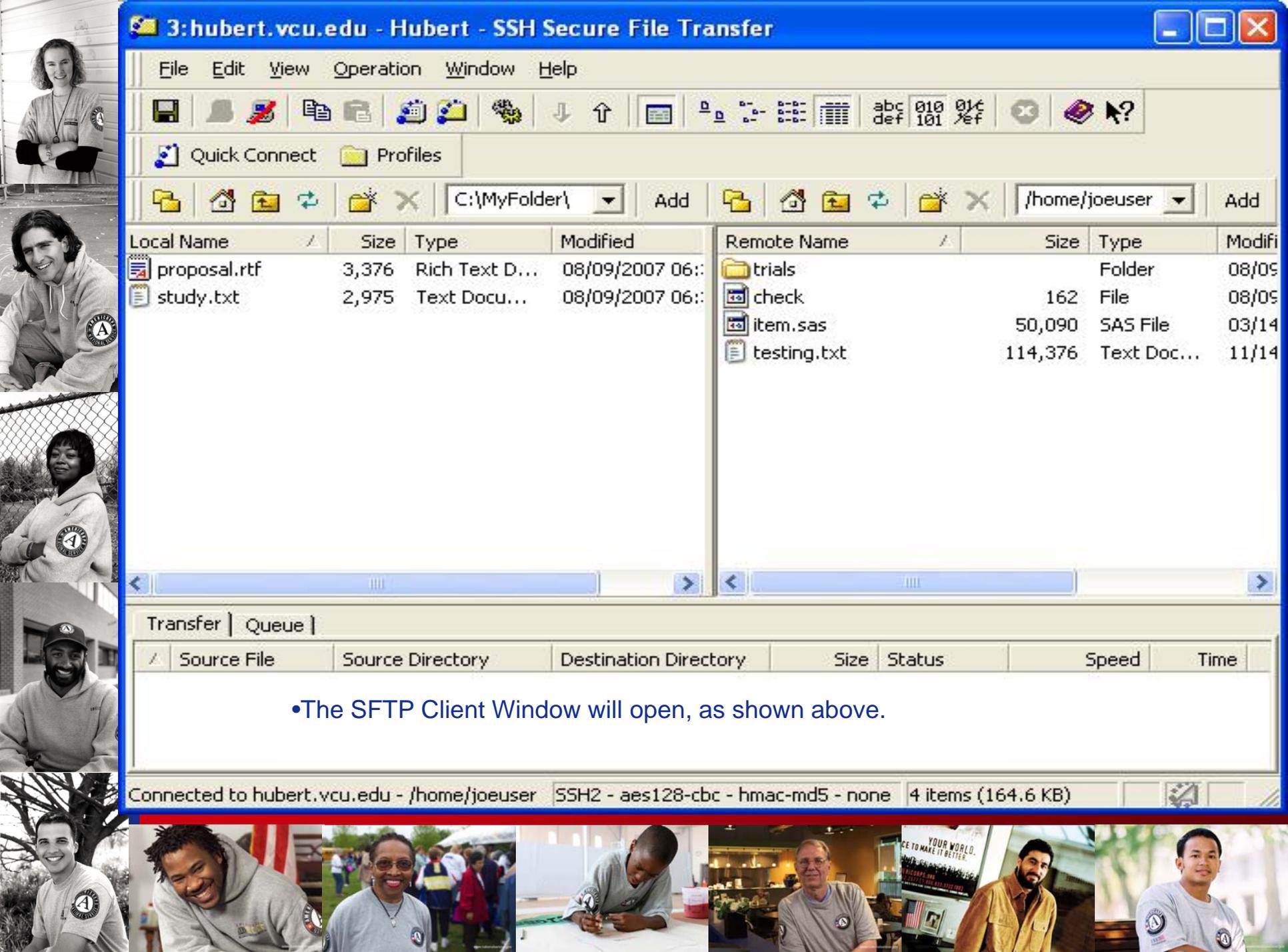
C:\MyFolder\ Add /home/joeuser Add

Local Name	Size	Type	Modified	Remote Name	Size	Type	Modified
proposal.rtf	3,376	Rich Text D...	08/09/2007 06:00	trials		Folder	08/09/2007 06:00
study.txt	2,975	Text Docu...	08/09/2007 06:00	check	162	File	08/09/2007 06:00
				item.sas	50,090	SAS File	03/14/2007 06:00
				testing.txt	114,376	Text Doc...	11/14/2007 06:00

Transfer | Queue |

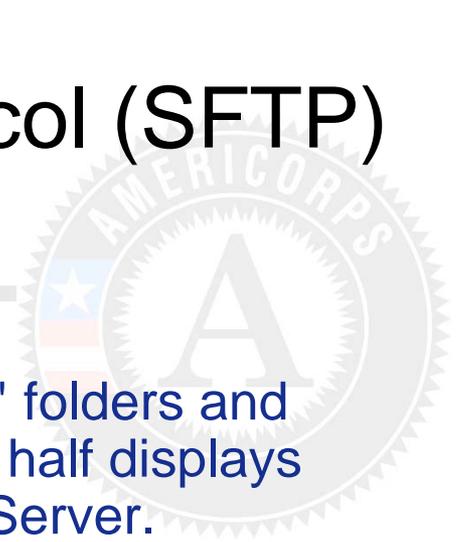
Source File	Source Directory	Destination Directory	Size	Status	Speed	Time
•The SFTP Client Window will open, as shown above.						

Connected to hubert.vcu.edu - /home/joeuser SSH2 - aes128-cbc - hmac-md5 - none 4 items (164.6 KB)



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)

- The left half of the window displays "local" folders and files that are on your computer. The right half displays "remote" folders and files that are on the Server.
- To copy a file from your computer to the Server, or vice-versa, simply use your mouse to "drag" the file from one side and "drop" it on the other side in whatever format your file is in; Word, Excel, etc. The file transfer will begin immediately. A summary of the transfer progress will be displayed in the area at the bottom of the window. Note that you are *copying* the file and not moving it (i.e., the original file will remain in place).



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)

- Before you copy a file, you should set the proper *transfer mode*, using the three toolbar buttons as shown:

```
abc 010 01c  
def 101 1ef
```

Select the left, middle, or right button to set the transfer mode to ASCII, binary, or automatic, respectively:

ASCII mode is appropriate for copying plain text files.

Binary mode is appropriate for image, zip, and program files.

Automatic mode will select the mode according to the file's filename extension, if the extension is any of the following.....



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)



.txt  
.html  
.htm  
.bat

then ASCII mode will be used; otherwise binary mode will be used. If desired, the above list of extensions can be altered by displaying the *Edit* menu and selecting *Settings* and then *Global Settings*, then *File Transfer*, then *Mode*.



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)

So, what exactly makes the data secure?????

Why, the Public and Private.....



The Private Key is the protective login dialog stored in each remote computer location within the SFTP application; just as when you log into your computer with that login and password data.

The Public Key is what allows the Host Mainframe computers to access each remote user's data. One remote user cannot access another remote users data; only the Mainframe remote user has that capability.

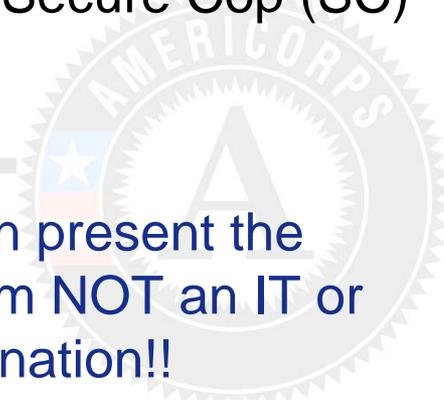


# Secure File Transfer Protocol (SFTP) With Secure Cop (SC)

## CONCLUSION:

Let me conclude by saying that while I can present the principles of the SFTP/SC application, I am NOT an IT or computer guru by any stretch of the imagination!!

To input this application took the efforts of several of our IT folks working both from the State's mainframe end and working extensively with each of the sub-grantees on their end. The entire process from conception, to testing, to verification took approximately four months. It is important to test this application with all remote sites and with all data formats you will be collecting to ensure there are no bugs. However, it is a compatible, Web-based, and user friendly system, and is free to download and utilize.



# Secure File Transfer Protocol (SFTP) With Secure Copy (SC)

- Questions???????

