

# Welcome to “Clockfile”

## Encryption key management software

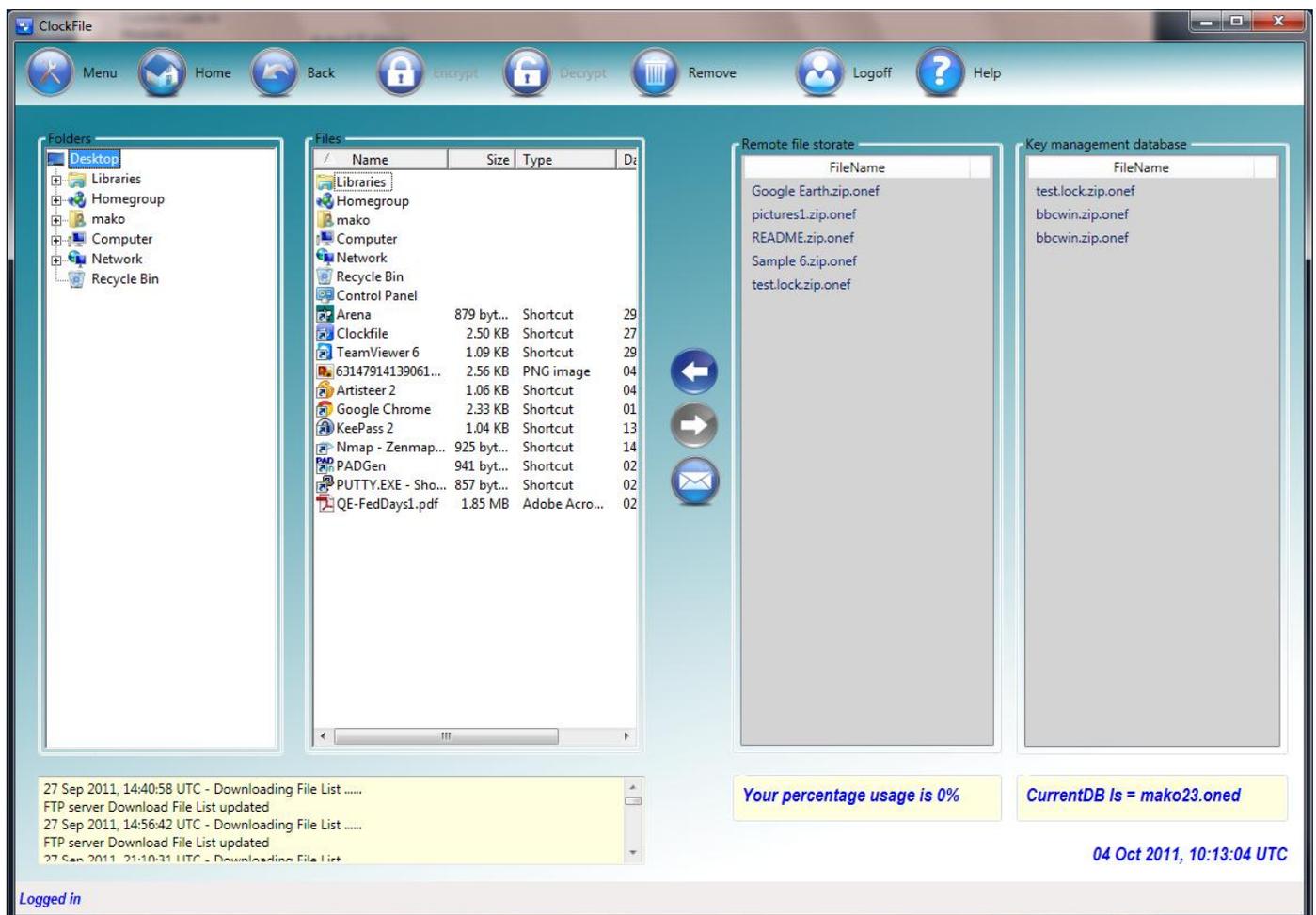
Clockfile was designed to make encryption easy for the user while not sacrificing security. Even though we feel Clockfile is intuitive to use we still strongly suggest that users make the effort to read this small user manual. With any encryption software it is easy for a user to make mistakes that compromise security or lead to a situation where users can't decrypt their own files. Several features are built into Clockfile to enhance a recovery where a user cannot decrypt their files.

In this manual you will see the following word password/key for individuals experienced in encryption the word key will be familiar, to individuals not versed in cryptography the concept password will be more familiar. For the purposes of this manual I have combined both words

## Clockfile main screen explanation

The main screen for Clockfile is listed below in *Figure 1*. There are four main windows in this screen. The first two windows on the left is an inbuilt file explorer that mimics the standard file explorer that comes with windows. For most users it should be intuitive to use. The two windows on the right hand side are the Off-site file storage window and the local database window. The top ribbon provides extra functionality

*Figure 1*



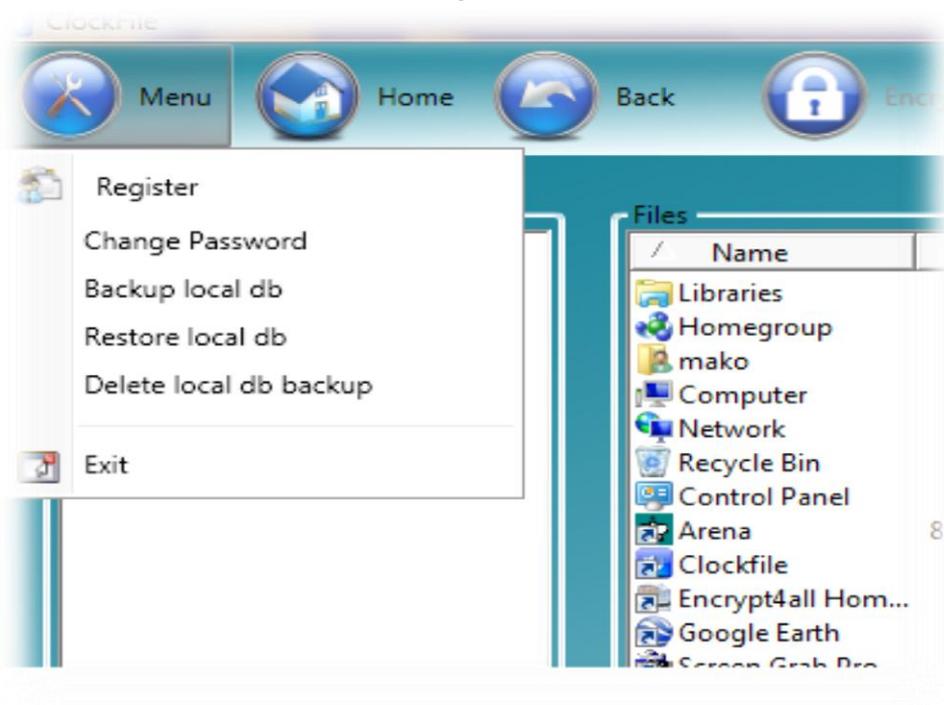
## Menu Ribbon

Figure 2



**Menu icon** allows users to backup and restore their local database plus delete the local database. The saving and deleting of local database backup is of critical importance to the smooth running of Clockfile. We strongly urge all Clockfile users to back up their local database at the end of every day. Backing up your Clockfile encrypted files provides another level of redundancy. Backing up your database and encrypted files also give another level of portability where a user can run Clockfile from any PC which has the software installed.

Figure 3





### Home Icon

Takes users to the Clockfile Home directory. All Encrypted files are stored in this directory when a file is encrypted. Encrypted files have the **.onef** extension to their names. When you encrypt a file click on the home icon to see where your encrypted file is placed. Your encrypted file will have the **.onef** extension. The Home Directory is an important directory because it is were all encrypted and decrypted files are placed. All restored files from the Ftp sever are placed here as well.



### Back Icon

Takes File explorer screen back one step in the file explorer screen. You will find the Back Icon of use when you want to flip back and forth between the Home Directory and any other Directory you are working in.



### Encrypt Icon

256 bit AES encryption of selected file. Select the file you want to encrypt and click on the Encrypt Icon.



### Decryption Icon

Provides decryption of Clockfile encrypted File



### Remove Icon

Trash can for encrypted files, you will not be able to find files in the system trashcan



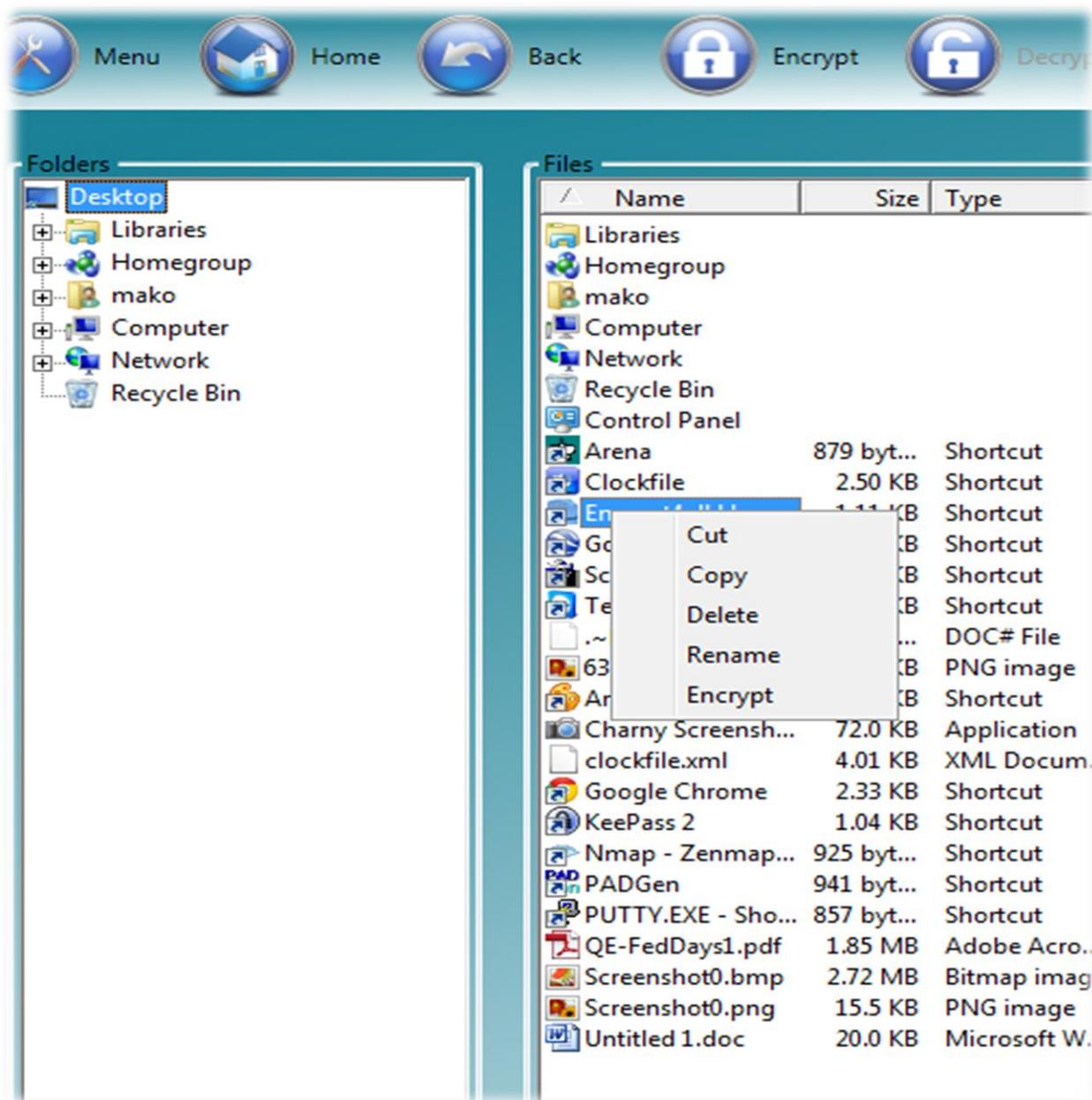
### Log Off Icon

Log off the system to allow another user to sign in

## Integrated File explorer

Explore your Network and Hard disk drive and select what files you want to manage. A lot of the functionality of Clockfile can be found by right clicking on a file. Like windows explorer you can select multiple files to an operation on them. You can select multiple files to have them encrypted into one file.

Figure 4



You can Cut, Paste, and Delete files and Rename them. You can encrypt files or decrypt onef files which are encrypted. If you right click on an encrypted file (has .onef extension) you can also send this file to other Clockfile users. Words of warning, do not rename files that are encrypted if you rename the file you will not be able to decrypt the file until you rename it back to its original name.

## Off-site Storage

Each user is allocated 50 MB Off-site storage for their encrypted files. Clockfile has an integrated FTP client to allow upload and download of files. It is strongly advised that users take advantage of the FTP facility to back up their local database. Also users can back up their encrypted files this allows another advantage that means that Clockfile can be used by any user on any machine that has Clockfile installed. A user can simply restore his local database and files to a new machine.

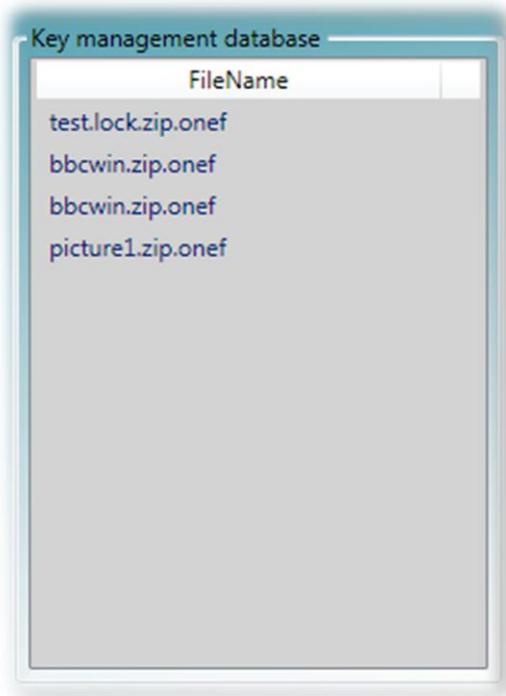
*Fig 5*



## Password/Key Database

Integrated Database to store encrypted file passwords. Every encrypted file has a randomly generated password/key that is stored in the local database. The local database always has the file name extension of .oned. You can find out the name of your database in the Footer display at the bottom of the program. Naming convention is “username”.oned

*Figure 6*



There is no need to remember passwords/keys when decrypting files. When you decrypt a file the Clockfile software looks in the local database for the password/key to decrypt the file. This is of one of the advantages having an integrated database; you never need to remember the password/key.

For security purpose having a unique password/key for each file greatly enhances security. Having the same password/key for every encrypted file is very problematic when sending other users encrypted files. Tell the other user your password/key and they will be able to decrypt any files of yours. However trying to remember to many too many password/keys is also problematic. To get over this problem we have built in the password/key management database which solves this problem.

We have gone to great lengths to ensure the security of this database by encrypting the database itself with 256 bit AES encryption also the records in the database are encrypted with AES 256 using another key/password that provides an extra layer of protection. In essence the database is double encrypted

## Bottom Footer

Figure 7



The bottom footer of the program provides a user log of all transactions which is listed on the left hand side. You can scroll through a list of transactions with the scroll bars

The right hand side displays the name of the [local database](#) which in this example is called [mako23.oned](#). Clockfile stores all key information into this database.

[Your percentage usage is %](#) displays what percentage of the 50 Megabytes each user has been allocated.

All clockfile transactions are listed in standard UTC time so that all users are on the same clock. It also provides a universal standard time for all users in regards to file decryption dates. This ensures that all users get access to protected documents at the same time.

### Things you need to remember

1. Encrypted files have .onef extension
2. The Local Database has .oned extension to its name
3. onef and oned files are stored in the Clockfile home Dir
4. Never delete your database oned files

## How to

### Encrypt a File

Select file in File explorer, right click and select encrypt from drop down menu or highlight file and click Encrypt Icon

### Decrypt a File

Right click on encrypted file and select decrypt from drop down menu or highlight file with left click and click on decrypt Icon

### Delete a File

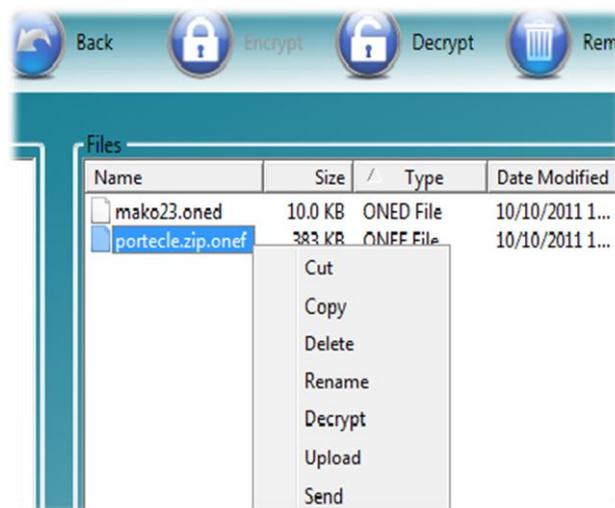
Right click on file and select delete from drop down menu or highlight file with left click and click on delete icon. Or drag file to trash can in first window or drag file to trash can Icon in Top menu.

What's the difference between clockfile trash can or windows trash can. You can easily restore deleted files put into windows trash can you cannot easily restore files placed into the Clockfile trash can.

### Send a File to another user

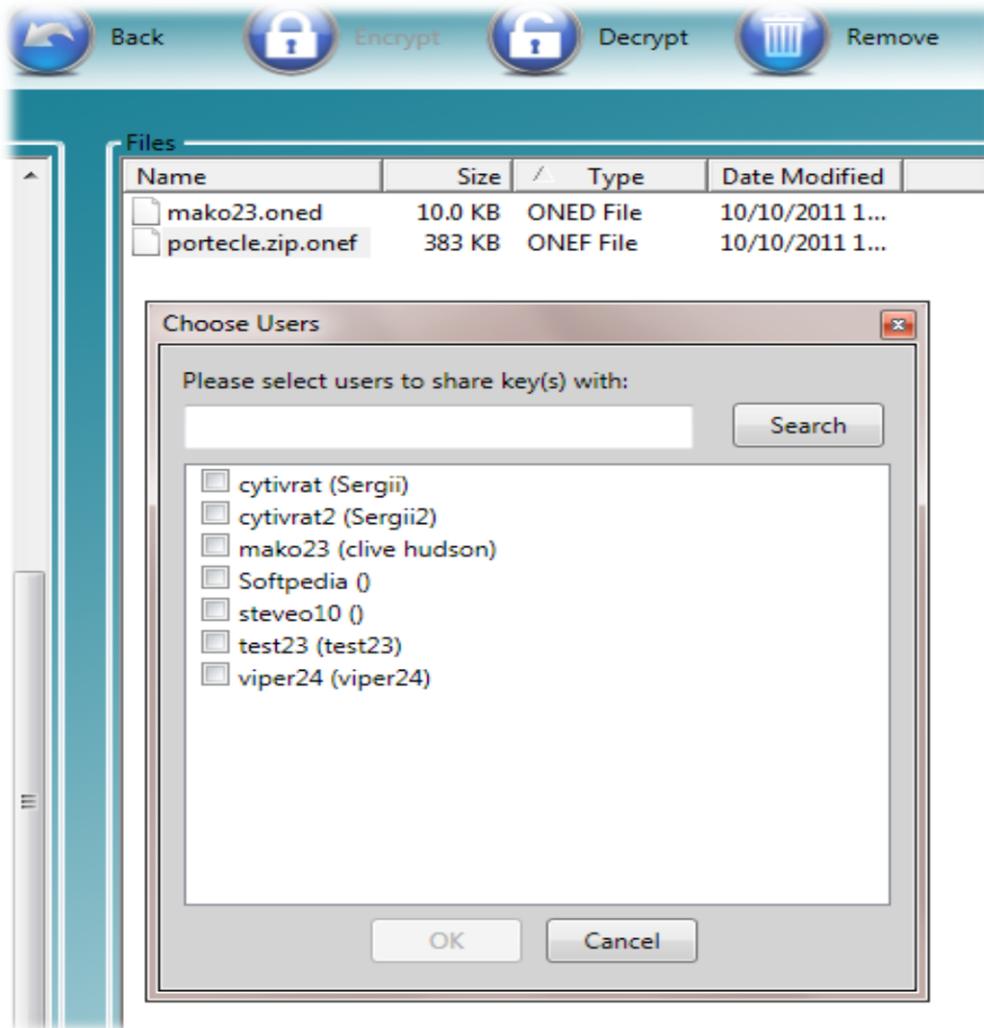
Right click on the encrypted file and select send from the drop down menu and you will see something similar to Fig 9

*Figure 8*



After selecting *Send* the following screen appears

Figure 9



Select the name of the user who you want to send the file too and click on the OK button. At this point the screen in *Figure 11* will appear. This screen allows an important functionality of Clockfile. A time restriction on files provides the ability to ensure at what date a file can be decrypted. For example is can ensure that obsolete files are not decrypted. Inversely setting the decryption time in the future is one way to ensure that all recipients have access to the document at the same time. For some legal documents this can be of particular importance.

Figure 11

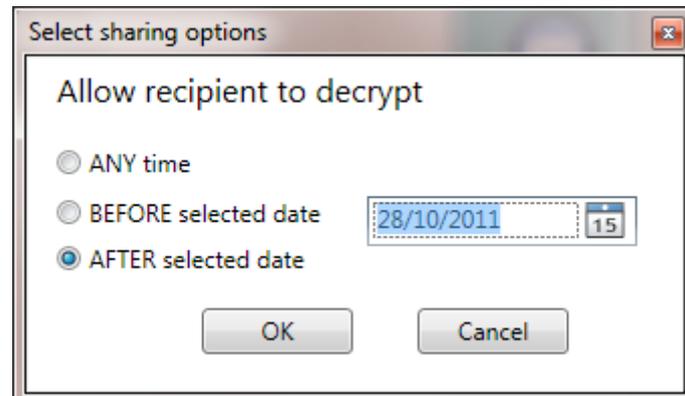


Figure 11 shows the date control screen where a user can select when a file can be decrypted when it is sent to another user. In Figure 11 the file will not be able to be decrypted until after 28/10/2011. The opposite scenario can also be created to deny decryption after the 28/10/2011. This could be achieved by selecting “BEFORE selected date” and the date of 28/10/2011

For most users selecting “ANY time” will be the default taken because this puts no limitations on decryption dates.

You will notice that your file will be uploaded to your Ftp account. This is part of the process involved when sending another user a file of yours. You will need to keep the file in your ftp directory for 5 minutes.

When a user sends a file to another user the following happens. The file is copied over to their personal Ftp account. When the receiver requests the file be sent to them, a copy of your Password/Key is sent to the receivers Clockfile client software. The key is sent securely using RSA encryption which provides seamless security of the user key during the whole transfer process. Once the sender’s password/key is received the file is decrypted and then a new key is generated and the file is encrypted. In the end the sender and receiver have the same file but they are encrypted by different key/password. Any date constraints on the file are inherited from the sender.

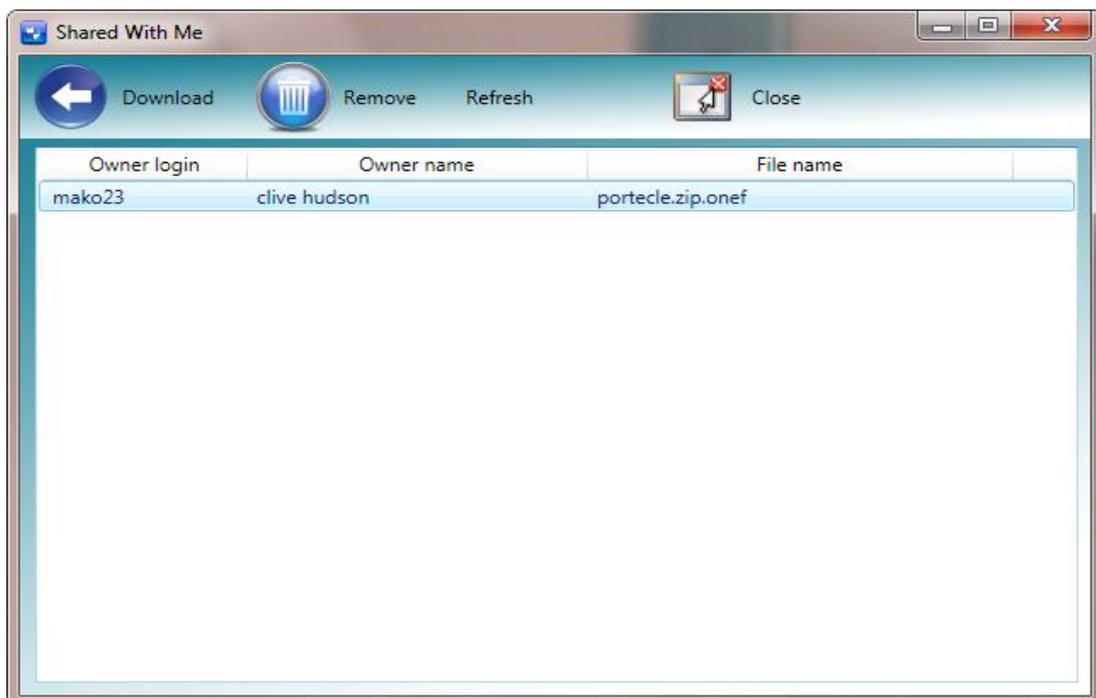
## Receiving Files from another user

When another Clockfile user has sent you a file you will see the mail notification Icon flashing



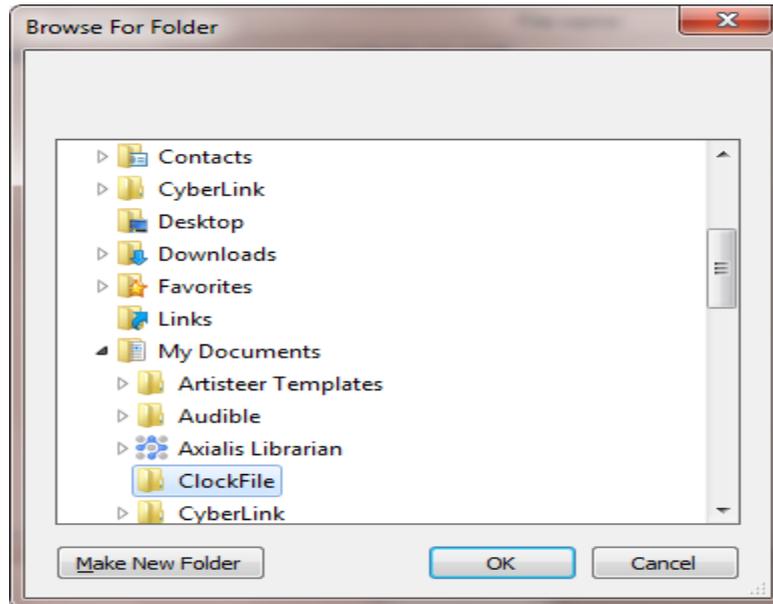
When the Icon starts flashing click on the Icon and the following screen will appear

Figure 11



In this example select file portecle.zip.onef and click on the Download Icon. You will be asked to where you want the file downloaded. The default Directory is the Clockfile Home directory. For most users selecting the default directory will suit most purposes.

Figure 12



After selecting your chosen directory and clicking on the OK button you will see that the file has been downloaded. In most cases this will be the Home Directory. You will also see that a corresponding entry has been made in your local database.

### Changing Password

Clockfile provides two methods of passwords; one is the very traditional username and an alpha numerical password. This system is the most commonly used for access with most computer systems. There is nothing wrong with this method, however we provide a more secure and statistical robust system for those users who ensure the best security that they can.

Clockfile provides a graphical Log on process. This process involves selecting specific areas of a picture which are used to generate a hash from. To enable graphical Log on go to the Menu Icon and select Change Password from the drop down list. You will see Figure 13

Figure 13

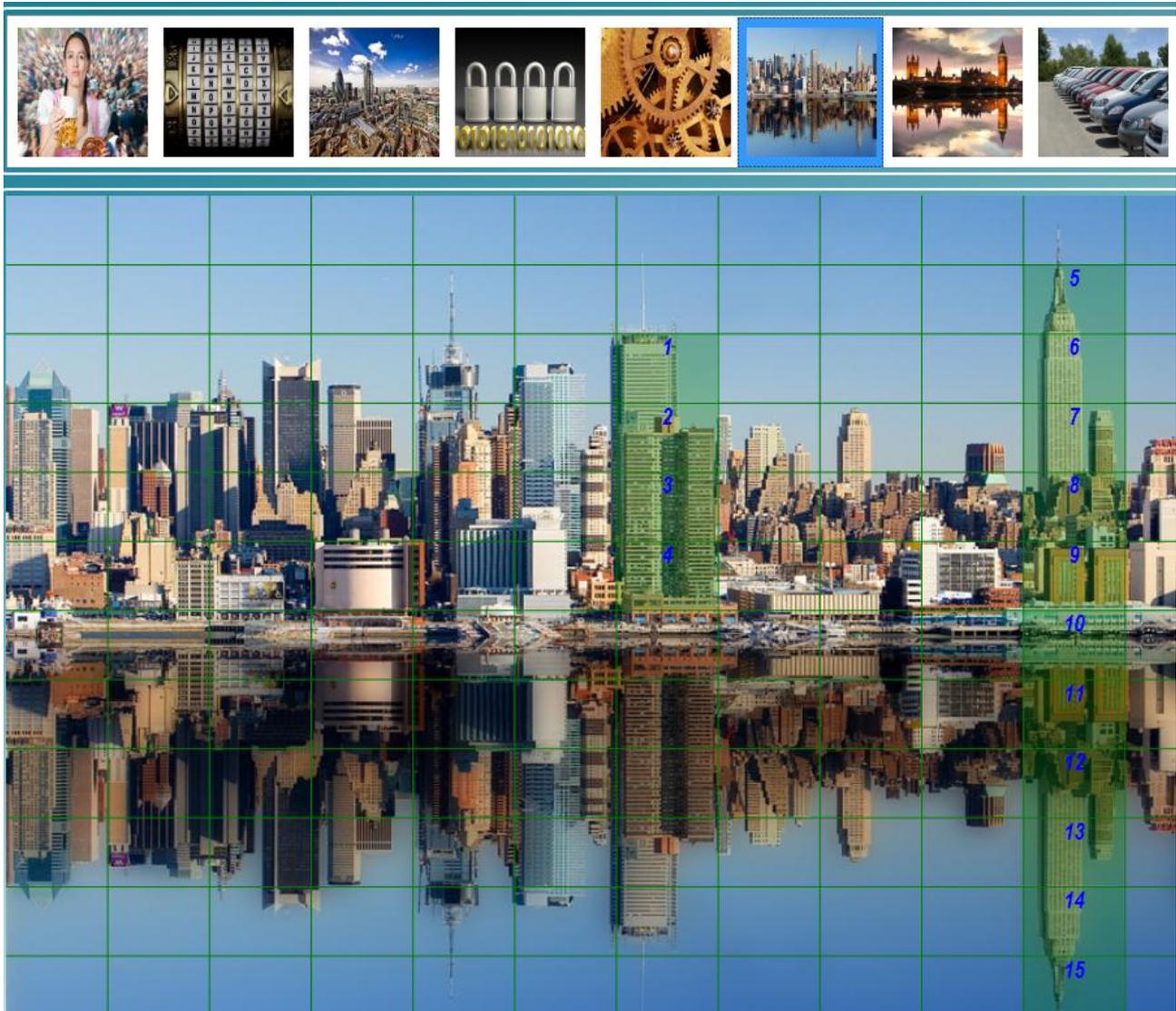


You will notice by the password field a little jigsaw shaped Icon this provides access to the

graphical logon Feature. Clicking on  brings up the graphical Login window

The graphical log on picture provides a mesh of 144 squares. User selects what squares and sequence of squares that they want. Users can select a number of pictures and select squares out of a multitude of pictures.

Figure 14



As long as you select the same number and sequence in the SAME picture or the SAME combination of picture it will generate the same password. A minimum of 10 squares must be selected to generate a password.