Introduction

CryptoExpert is a real-time encryption system providing secure storage for documents, commercial data and private files.

It uses the following encryption world-known algorithms: Blowfish, CAST, DES, 3DES, and it provides excellent protection against unauthorized data access.

CryptoExpert is easy to use and install, and totally transparent for all Windows applications, thus providing secure virtual drives to store your important files.

Main Features
Requirements
Limitations

CryptoExpert Features
Easy in Use

Once the <u>virtual drive</u> drive is loaded, you can copy, move, delete files and folders as if you worked with any other hard disk. Once unloaded, the virtual drive is disappeared from your system and you are to enter the password to mount it again. When it is unloaded, CryptoExpert' high security encryption technology ensures that your data is safe (it is stored in encrypted form inside the encrypted container file).

Military grade Security

Once written to the CryptoExpert's container file, your data is never stored in the 'open' state. CryptoExpert uses published strong encryption methods to make sure no one can open, copy or read your important files.

It is very important for a trusted security system to use open published encryption methods to allow experts to verify its reliability.

CryptoExpert Pro utilizes the following encryption algorithms:

·   the Blowfish algorithm with 256 bit key length (was designed by Bruce Schneier in 1983 and is is very popular now)
·   the CAST algorithm with 128 bit key length (was developed by Carlisle Adams. Its description can be found in [rfc2144](rfc2144))
·   The DES algorithm with 56 bit key length (USA Data Encryption standard FIPS 46).
·   TRIPLEDES with 168 bit key length (It is approved by NIST as an encryption standard. Its description can be found in FIPS 46-3)

No "back door" in the software
No access possible under any circumstances. If you do not remember the password you cannot access the encrypted contents. There is no special procedure, secret code, or hidden entry method to fall back on.

Using in Network

It is possible to use any network drive to create and access file containers:

• Mount remote containers
• Share virtual drives between the network users in the same way as other logical hard drives on your computer

CryptoExpert Requirements

CryptoExpert requires the following minimum computer configuration:

Hardware

·   IBM or compatible
·   Minimum 5 MBytes of free HDD space to install and run the CryptoExpert software.

Software

·   Microsoft Windows NT version 4.0 (Workstation or Server), or Windows 2000, or Windows XP

CryptoExpert Limitations
Local hard drives and External drives

There are no limitations in the number or type of Local and External Drives used as storage media for CryptoExpert's encrypted containers. SCSI and IDE hard drives, removable media drives, magneto-optical devices, RAM drives, CD-ROM drives and others may be used.

Virtual drives

You can use any number of virtual drives in the current release of CryptoExpert simultaneously.

Maximum Size Of CryptoExpert's container

Windows NT/2000/XP: Maximum size of encrypted drive mapped to a correspondent container file is 2 Gbytes

Minimum Size Of CryptoExpert container

Minimum size of CrypotExpert encrypted drive is 19 Kb.

CryptoExpert Versions

CryptoExpert has two release types: Personal (**PE**) and **Professional**.

CryptoExpert 2004 PE

PE version can be used at home only, **not in business**
PE version has **1 encryption algorithm** to protect your files on virtual drive on the fly
PE version able to mount **only one container** as virtual drive at the time (but it does not mean that you cannot have many other containers in unmounted state).
It is impossible to use PE version in network environment
One copy costs US$39.95

CryptoExpert 2004 Professional

Professional version can be used in **business environment** and/or at home
Professional version has **3 encryption algorithms** to protect your files on virtual drive on the fly
Professional version able to mount **unlimited number of containers** as virtual drive at the time
It is possible to use PRO version in the **network** environment: share virtual drive between network users and load containers from other network drives.
One copy costs US$59.95
Volume discounts available

Why encrypt?

There are a number of sophisticated methods and a wide range of equipment by which all your data is accessible if your PC is not protected specially. Encryption is the only way to protect your important files.

Hence, encryption, using **CryptoExpert** software, is a good choice to protect your privacy.

What is encryption?

Encrypting data means getting it transformed into a string of characters undecipherable by others.

What actually happens is that by using a secret-key i.e. the equivalent of a code (see glossary), the cryptography system transforms your data into gibberish. If the scrambling of the data is done properly, the original file can only be unscrambled and read by someone who knows the secret key i.e. the code used to encrypt the file.

Encrypting a file ensures that even if someone gets access to your computers/he would not be able to read the data stored there. Encrypted files can safely be sent by e-mail or placed on a network with the assurance that the data can be read only by those who were meant to have it.

Basic encryption systems have been used to protect secrets for many centuries. But today's encryption methods are far more sophisticated and reliable than ever before because the encryption code itself is a very complex computational transformation that is only feasible with desktop machines in the early 1990s

How does encryption work?

When you use encryption, your data gets converted into meaningless symbols by using a key, which is nothing but the code that helps you to encrypt or decrypt data.

The more random the method of key conversion, the stronger the encryption will be. A pass phrase generally needs to be easy to remember, so it has significantly less randomness than its length suggests. For example, a 20-letter English phrase, rather than having 20 x 8 = 160 bits of randomness, only has about 20 x 2 = 40 bits of randomness.

So, cryptographic software converts a pass phrase into a key through a process called ``hashing'' or ``key initialization.'' (see glossary)

At the heart of the process is the algorithm (see glossary), which is devised so as to make deciphering the encrypted file impossible without using the secret key. Some of the popular encryption algorithms include Blowfish, DES, Diffie-Hellman, IDEA, RC4, RSA and Skipjack. Many of these use 64 and 128 bit encryption systems i.e. devise keys of 2*64 or 2*128
length.

The Blowfish encryption algorithm on which CrypotExpert is based was specially designed to encrypt data on 32-bit microprocessor. It is significantly faster than DES and GOST when implemented on 32-bit microprocessors, such as
the Pentium or Power PC.

CryptoExpert software uses the Blowfish in Cipher Block Chaining Mode with 256-bit key length.

Is encryption safe?

An ordinary user may find it difficult to unscramble even a simple algorithm. However, experts using sophisticated methods can employ a number of means to break an algorithm. The most common of these is "brute force" wherein   a number of computers are simultaneously employed to break the code by a "trial and error" system which physically checks all possible combinations.

However, a well developed encryption system can withstand even such brutal attacks. Encryption based on the algorithms mentioned above are generally

immune to these kinds of attack assuming that no backdoors exist in the programme. Calculations show that the period of time required to crack them through brute force is gigantic. This table will give an idea of the dimensions.

2 to power of	Approximates to	
30	Age of planet earth (in years)	
33	Probability of being killed by a lightning (per	day)
61	Lifetime of universe in seconds	
170	Amount of atoms on our planet	
223	Amount of atoms in our galaxy	
446	Amount of possible keys used by CryptoExpert	
2048	Amount of possible keys	

The probability of being killed by a lightning is 2^{33} to 1, this is about 8.5 billion to 1.
Note: 128 bit keys generally provide maximum security. For most private and commercial applications 60 bit key length is sufficient. Only 56 bit and below keys can theoretically be broken by the "brute force" method.

To see how difficult this is let us look at estimates of the time required using brute force to break symmetric ciphers assuming that:
i.	Every single computer (estimated at 3*108) on the earth is used full time.
ii.	Every computer has the processing power of a PII 450Mhz. Then a single (3DES) key can be brute forced in an average of 457,351,814,728 years.

The table below shows how long the various types of keys remain secure for. A number of assumptions are made:

i.	The number of computers in the world is equal to 100 Billion (that's ten for every single person on earth in the year 2014 - there are expected to be 10 billion people alive in 2014).
ii.	Each of the computers obey Moore's law (the power and speed of computers doubles approximately every 18 months) for the entire period of cracking. (NOTE: this assumption may break current theories on speed of light, quantum physics etc). In reality, Moore's Law is predicted to become
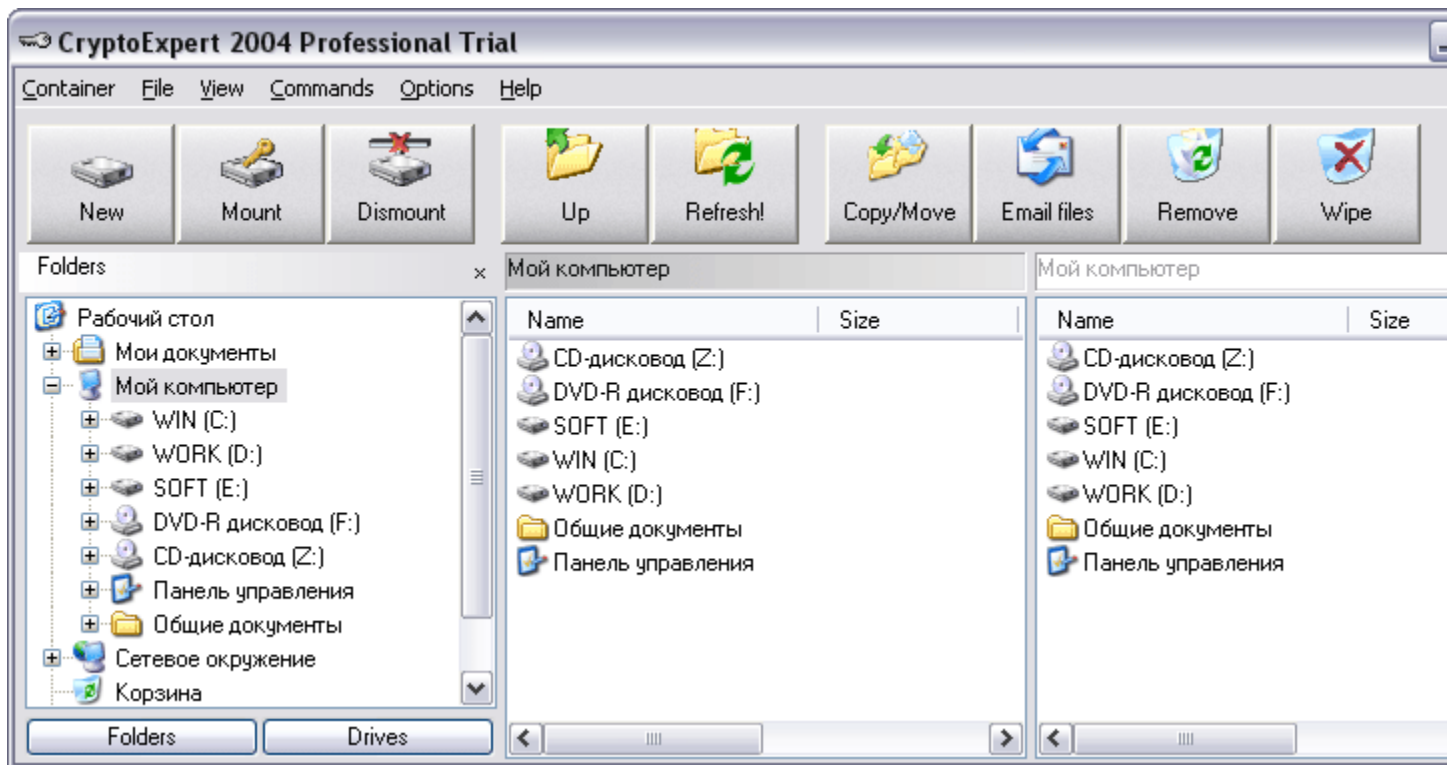
infeasible within 10 years or so.

Cipher	Effective	Years until break
	Key Size	feasible with

		500 Supercomputers	10 Billion	100,000 Deep Crack computers (PII 450)	machines
3DES	112	61		44	45
CAST	128	85		65	69
IDEA	128	85		66	69

Quick start

When you run CryptoExpert, the following window will appear:

Picture 1. *Usual program window*

There are three panes in the CryptoExpert main window - 'Folders' on the left and two file panes on the right.

First of all, you are to create a container file - the secure storage of your confidential information. Choose the "Container->New container..." menu command or just click the "New" button on the main toolbar.

Read How to create container

When you have created a container(s), you can see all your containers in the **"Encrypted Containers"** pane. Click the **"Drives"** button. Then click the **"Containers"** icon.
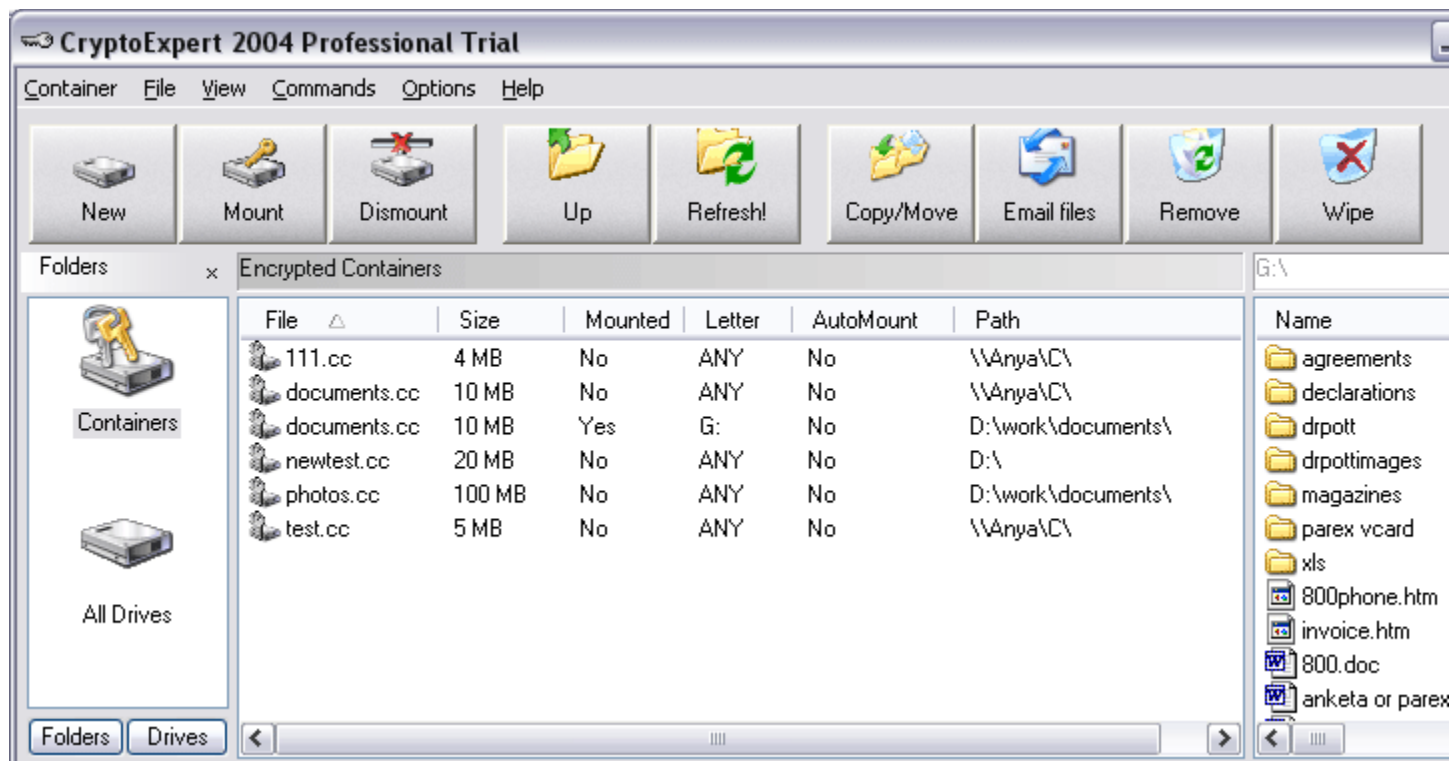
Picture 2. *Activated "Encrypted Containers" pane.*

In this pane you can see the containers and their state.

Now, find a newly created container file in this pane. If you cannot locate this container here, read
Then, have a look if this container is already mounted. In the "Mounted" column you will see the container
mount state. If it is not mounted, just double click the container and enter the password to mount it.

See also:
How to delete a container(s) from the "Encrypted Containers" pane

Basic Concepts of Program Interface

CryptoExpert main window has three panes: **Folders** pane, **First Pane** and **Second Pane**.
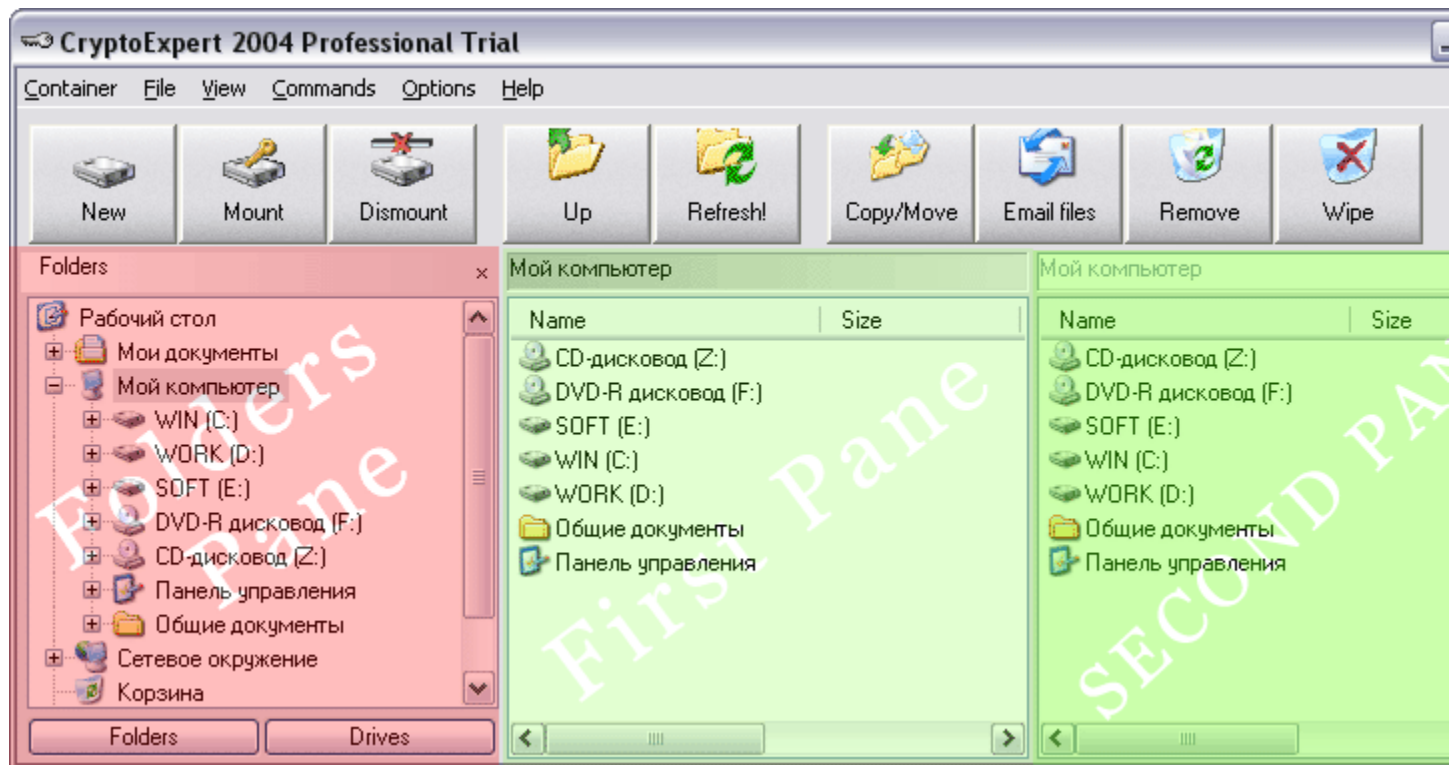
Picture 1. *Usual program window*

Folders Pane is used for navigation through folders, drives, and network drives. It has two modes:
Folders Mode and *Drives Mode*.
Read more about Folders Pane

There are also two other panes: **First Pane** and **Second Pane**.

Both First and Second Pane have two modes: *Files mode* and *"Encrypted Containers"* mode.
Read more about Files Pane /   Pane

First Pane or **Second Pane** can be active or inactive. To make it active, just click this pane. The Active files/"Encrypted containers" pane receives all commands from the folders pane. For example, when the Folders Pane is in the Folders Mode, you can click any folder in this pane and change the root folder for the active files pane.
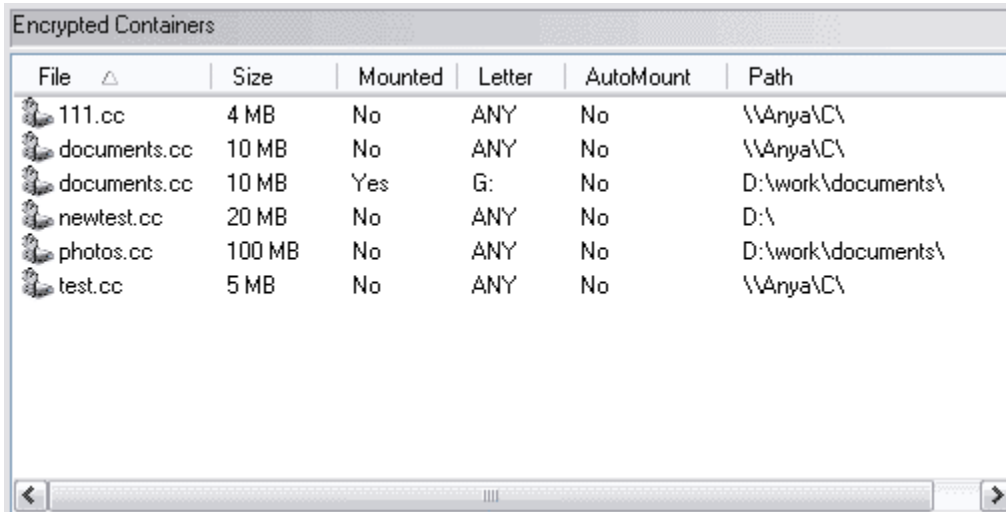
You can set different root folders for all two files panes (*for ex. FirstPane: c:\windows, and SecondPane: d:\mydocuments)*   and copy/move files from one pane to another.

Another Example: You can copy files from one pane (folder on your hard drive) to another pane (CryptoExpert virtual drive).

About "Encrypted Containers" pane

Each files pane has two modes: "Encrypted Containers" and "Files".

When you activate the containers mode, you will see the list of your favourite containers in the active pane.

File △	Size	Mounted	Letter	AutoMount	Path
111.cc	4 MB	No	ANY	No	\\Anya\C\
documents.cc	10 MB	No	ANY	No	\\Anya\C\
documents.cc	10 MB	Yes	G:	No	D:\work\documents\
newtest.cc	20 MB	No	ANY	No	D:\
photos.cc	100 MB	No	ANY	No	D:\work\documents\
test.cc	5 MB	No	ANY	No	\\Anya\C\

Picture 1. *"Encrypted Containers" mode in files pane.*

This pane has several columns.

- The **File** column has the name of the file container.
- The **Size** column has the file container size in Megabytes
- The **Mounted** column shows the container's state if it is mounted as the virtual drive or not
- The **Letter** column has the virtual drive letter. If the container is already mounted as the virtual drive, this column shows the drive letter of this mounted drive. If the container is not mounted, this column shows the drive letter which will be assigned to the container when mounted.
- The **AutoMount** column shows the automount settings for the container. If "Yes", the container will be mounted at the next Windows Start-Up. To change the state, right click the container and select "Properties".
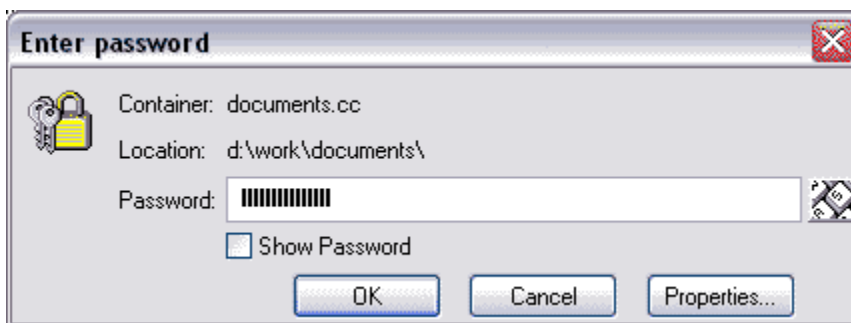- **Path** column has the full path of the container. It can be local or network path.

How to mount a container

To mount a container, just double click it (make sure that active files pane is in the "Encrypted Containers" mode)

Or right click it and select the **"Mount"** command in the popup menu
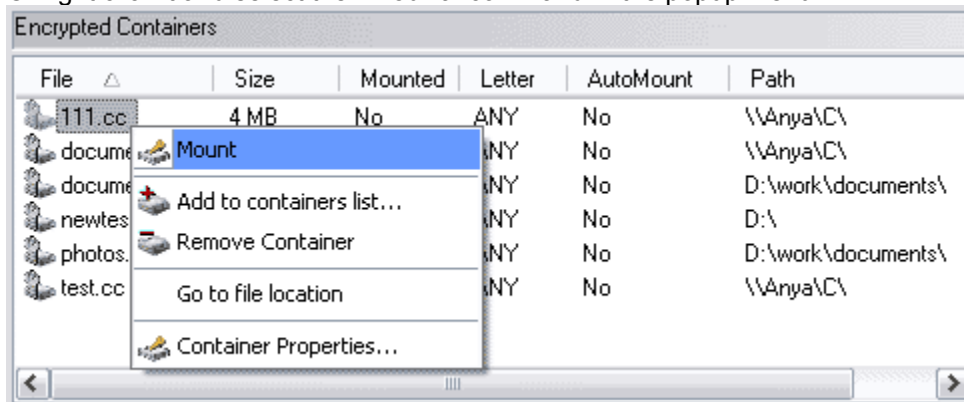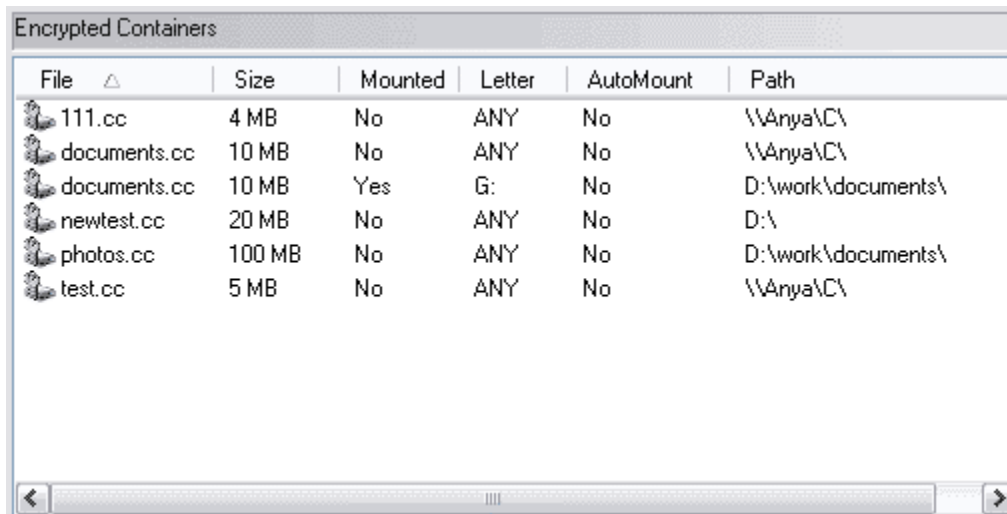

Then enter the password in the password dialog:



See Also

Read more about <u>Password Dialog</u>

How to dismount a container

To dismount a <u>virtual drive</u>, find the mounted container in the "Encrypted Containers" pane. Make sure it is mounted ("Yes" in the **Mounted** column) and double click it.

Picture 1. *"Encrypted Containers" mode in files pane.*

You can also dismount a container from the popup menu. Right click on this container and select the **Dismount** command in the popup menu.
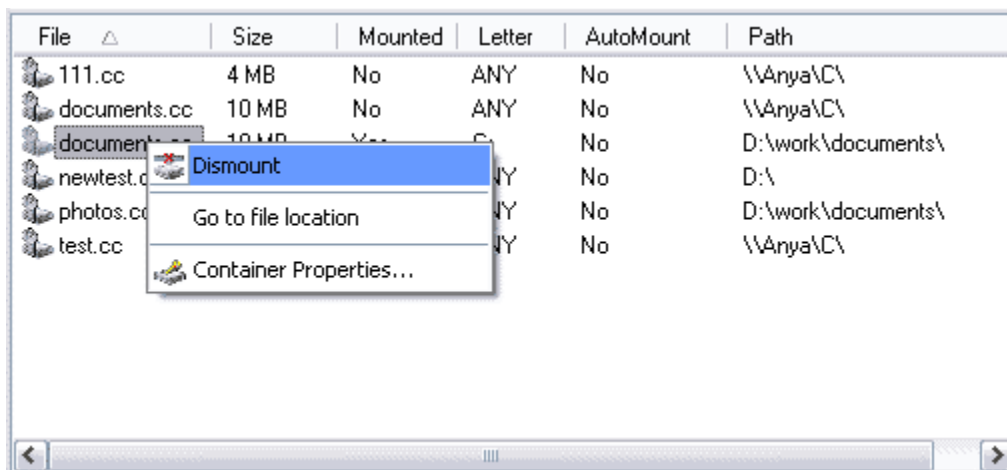
Picture 2. *How to dismount drive from context menu*

How to add containers here

File △	Size	Mounted	Letter	AutoMount	Path
111.cc	4 MB	No	ANY	No	\\Anya\C\
documents.cc	10 MB	No	ANY	No	\\Anya\C\
documents.cc	10 MB	Yes	G:	No	D:\work\documents\
newtest.cc	20 MB	No	ANY	No	D:\
photos.cc	100 MB	No	ANY	No	D:\work\documents\
test.cc	5 MB	No	ANY	No	\\Anya\C\

Picture 1. *"Encrypted Containers" mode in files pane.*

If you want to add a container to the "encrypted containers" list, right click on the white space and select the **"Add container here"** command in the popup menu.

File △	Size	Mounted	Letter	AutoMount	Path
111.cc	4 MB	No	ANY	No	\\Anya\C\
documents.cc	10 MB	No	ANY	No	\\Anya\C\
documents.cc	10 MB	Yes	G:	No	D:\work\documents\
newtest.cc	20 MB	No	ANY	No	D:\
photos.cc	100 MB	No	ANY	No	D:\work\documents\
test.cc	5 MB	No	ANY	No	\\Anya\C\

Add Container Here...
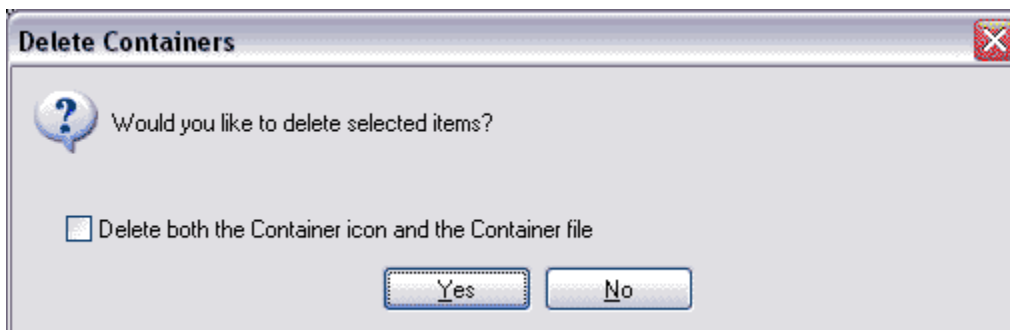
Picture 2. Adding container to the containers list

How to add remove containers

To remove a container from the container list, select it, then right click it and select the **"Remove container"** command in the popup menu.
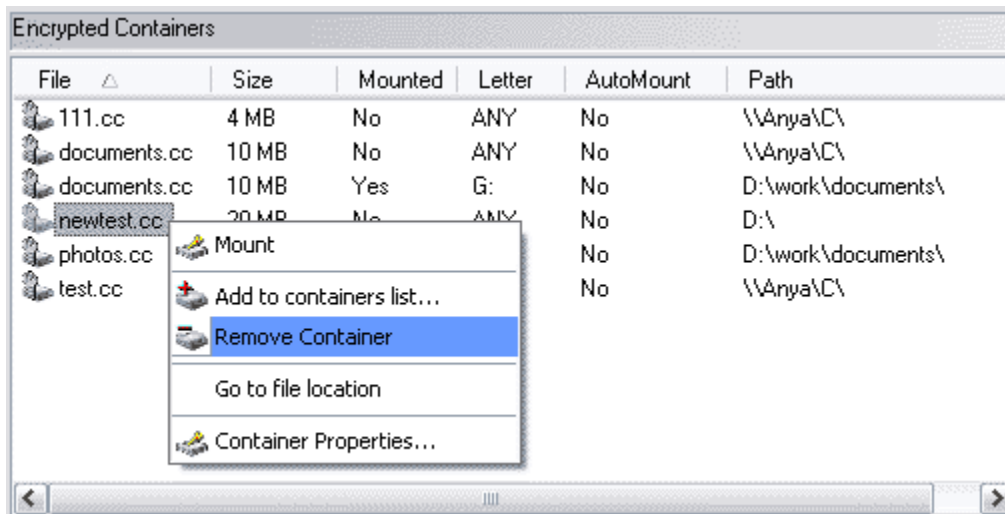
Picture 1. *Removing container from the the containers list*
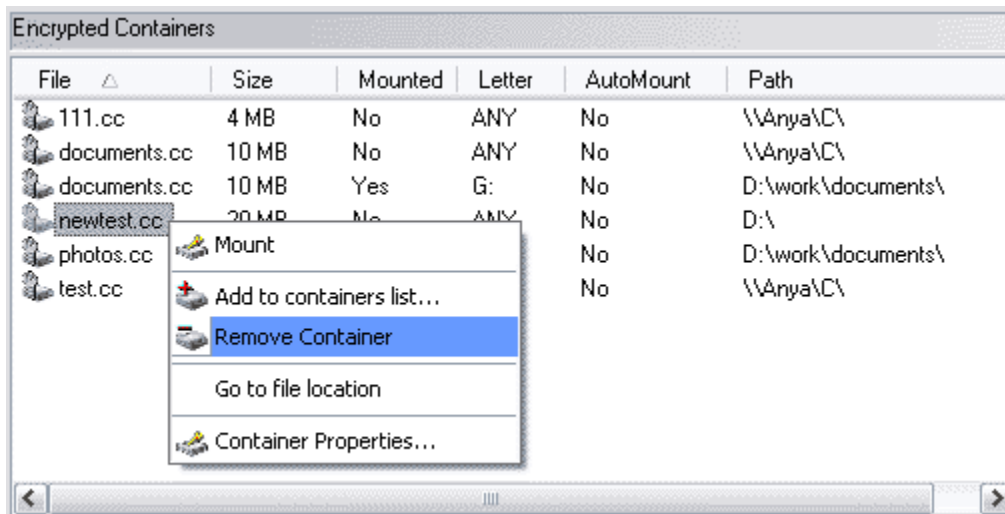
Then you are to confirm the container deleting:

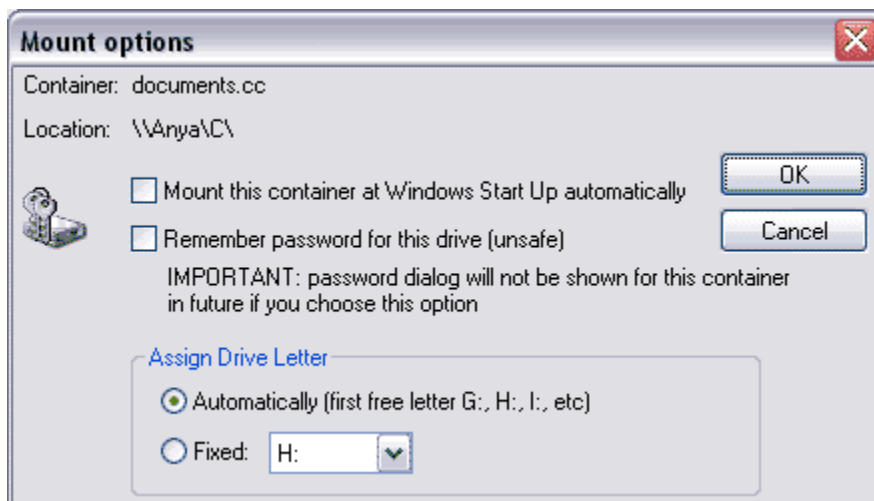Check the box, if you want to delete the container file as well as the container from the list.

How to change container's properties

To change the container properties, select it, then right click it and select the **"Container Properties"** command in the popup menu.

Picture 1. *Changing container properties*

Now you can change the container properties:

Picture 2. *Container Properties Dialog*

Check the **"Mount this container at Windows Start Up Automatically"** option to mount this container at every windows start up.

Check the **"Remember password for this drive"** option if you do not want to enter the password every time to mount the container. It is unsafe, because anyone can mount this container without your permission. It is also unsafe, because the password is stored in the registry of your computer and can be read. When you uncheck this option, all the password records are removed from the registry.
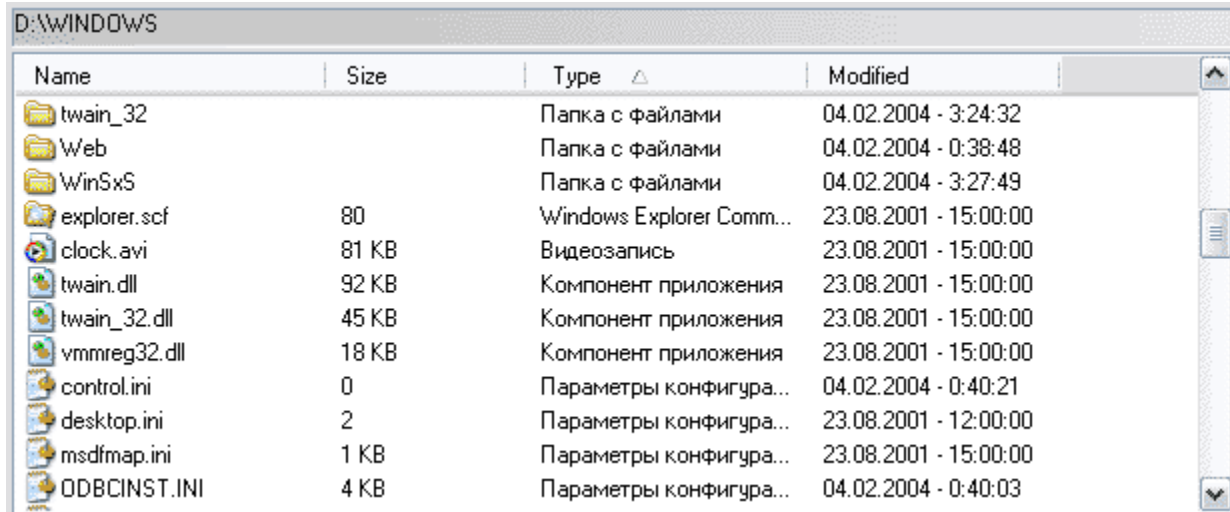
Assign Drive Letter
Check the **"Automatically"** option if you want any free drive letter to be assigned to the <u>virtual drive</u> on mount.
Check the **"Fixed"** option if you want to assign the specified drive letter only to the <u>virtual drive</u> on mount.

Please mind, that the error message will be shown, if the drive letter is already used by another storage device.

About file panes

Picture 1. *Files pane. Detailed View*
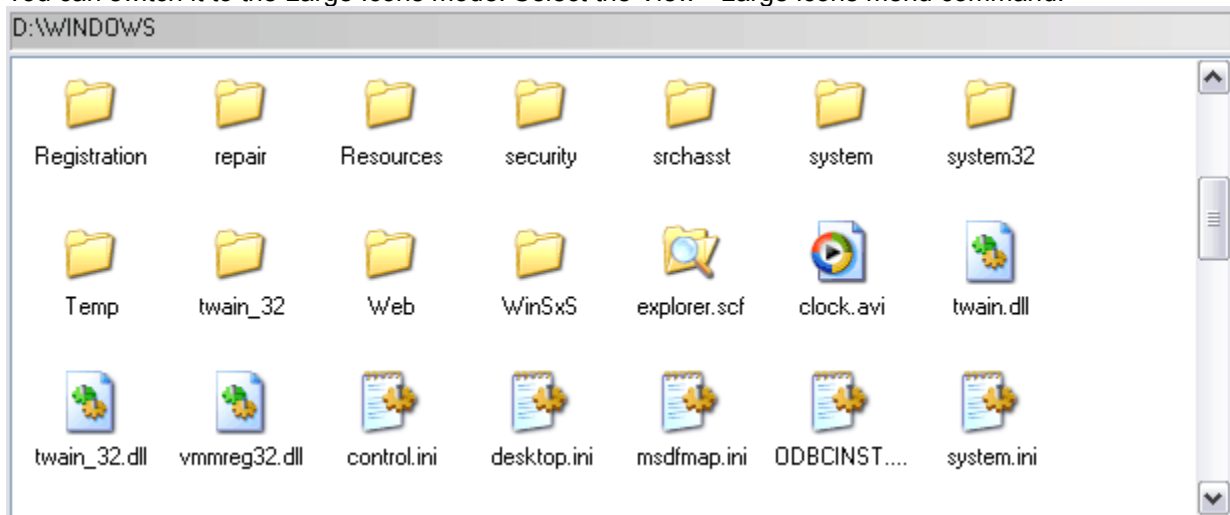
This pane has several columns.

The **Name** column contains the file or folder name
The **Size** column contains the file size
The **Type** column contains file type
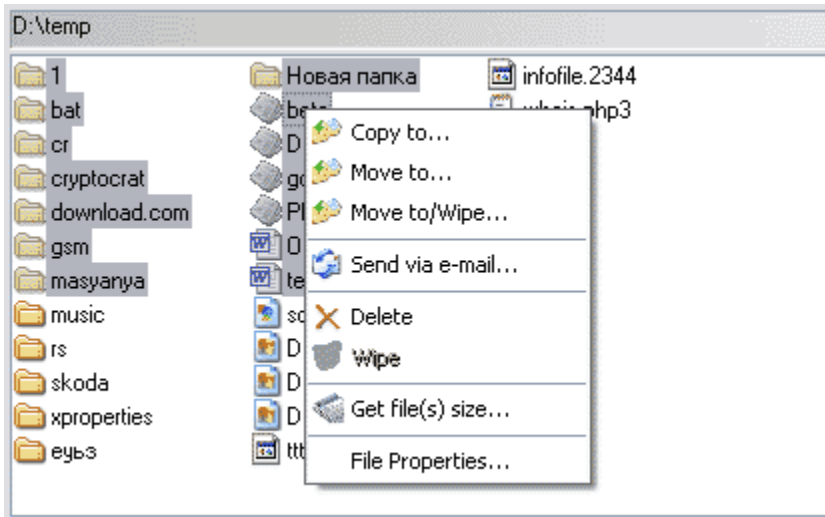The **Modified** column contains the file creation date and time

You can switch it to the Large Icons mode. Select the View->Large icons menu command.

Picture 2. *Files pane. Large Icons View*

How to remove files

To delete a file or several files or folders, select it with the mouse:
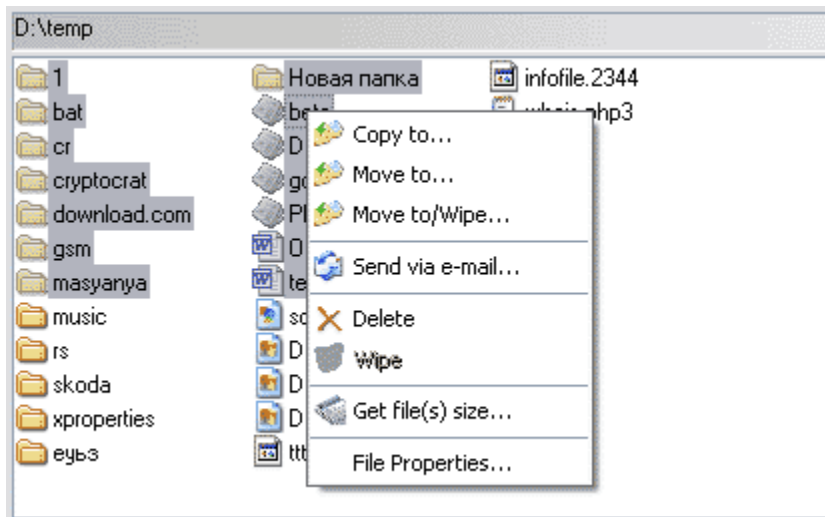

Picture 1. *Files pane. Selected files*

Then right click the selected files and select the **"Delete"** command in the popup menu. You can also click the **Delete** button on the main toolbar menu

How to securely delete files

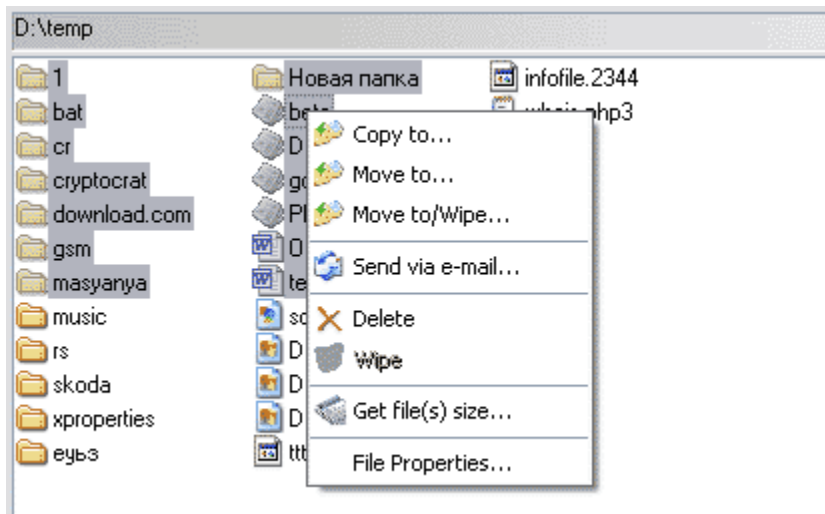To <u>wipe file</u> or several files or folders, select it with the mouse:

Picture 1. *Files pane. Selected files*

Then right click the selected files and select the **"Wipe"** command in the popup menu. You can also click the **Wipe** button on the main toolbar menu

How to send files via email

To send file or several files via email, select it with the mouse:

Picture 1. *Files pane. Selected files*

Then right click the selected files and select the **"Send via Email"** command in the popup menu. You can also click the **Email** button on the main toolbar menu

A new email will be instantly created in your email client and selected files will be attached to this mail.

How to copy files between the panes
CryptoExpert has a two file panes interface to allow you to copy/move files between the panes.
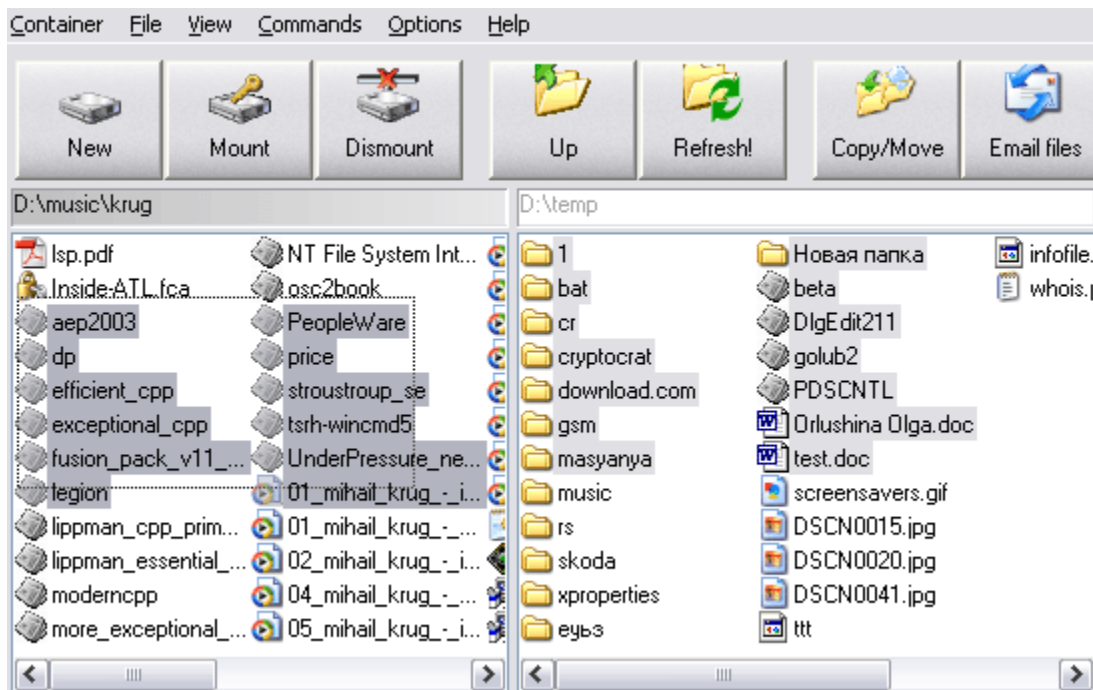
Picture 1. *Two files panes. Selected files in the active pane*

For example, you can copy/move files from your hard drive to the <u>virtual drive</u>.
Read <u>how to change the folder in the pane using the Folders pane</u>

To copy files from the file active pane to the inactive pane, select files in the active pane with the mouse
and click the **Copy/Move** button on the main toolbar or just press **Ctrl-C:**
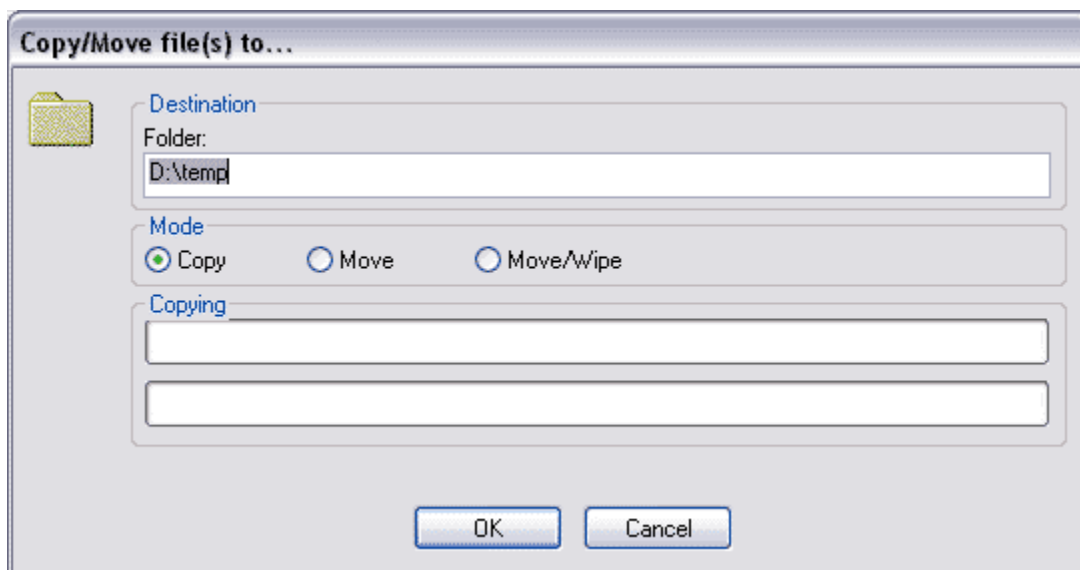
Picture 2. *File copy dialog*

In this dialog choose the copying mode: Copy, Move or Move/Wipe.

Please mind, that files will not be deleted when in the Move/Wipe mode, if the source and destination drives are the same. In this case files will just be moved.

About Folders Pane

Folders pane has two modes: Folders and Drives
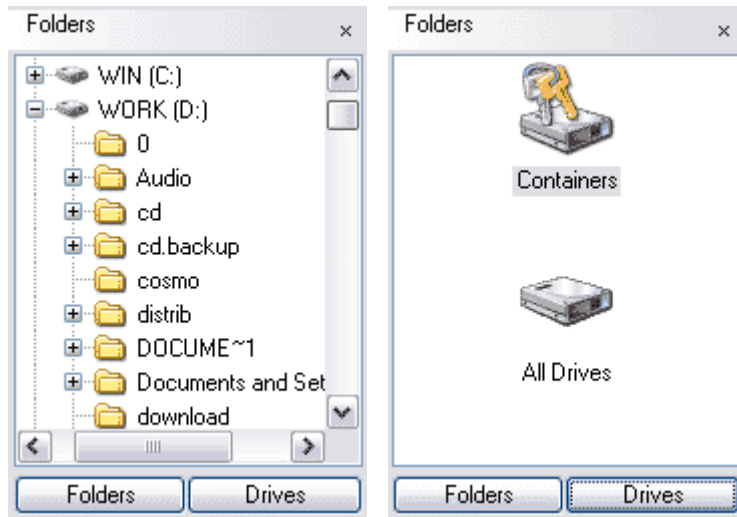
Folders mode   Drives mode

Picture 1. *Folders pane*

To activate the Folders mode click the **Folders** button.
To activate the Drives mode click the **Drives** button.

When you change anything in the folders pane, it sends commands to the active files pane.

For example, when you click any folder, the active files pane changes its root files folder
When you click the Containers icon, the active files pane changes its mode to **"Encrypted Containers"**.

You can close the Folders Pane, selecting the **View / Show - Hide Folders Pane** menu command, or pressing the ` (apostrophe) key

Password Dialog

Every time, when you mount a <u>virtual drive</u>, you are to enter the password.
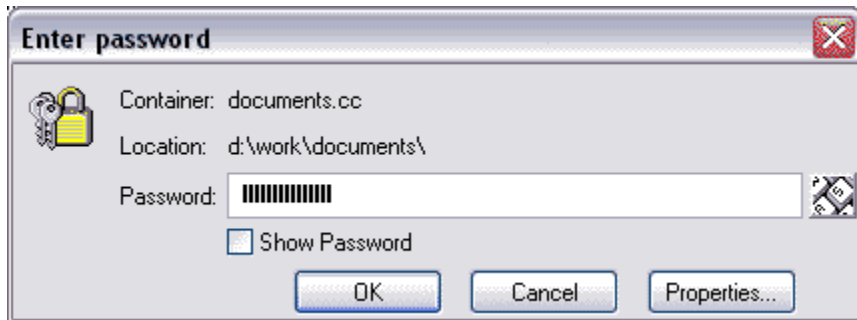
**Picture 1.** *Password dialog*

Check the **Show Password** box if you want to see your password.

Press the **Properties...** button to change the <u>Container Properties.</u>

Click the button right to the password field to type the password using virtual keyboard, to make sure no password characters will be intercepted by the keyloggers of any kind.

How to copy files from one pane to another
CryptoExpert has a two file panes interface to allow you to copy/move files between the panes.
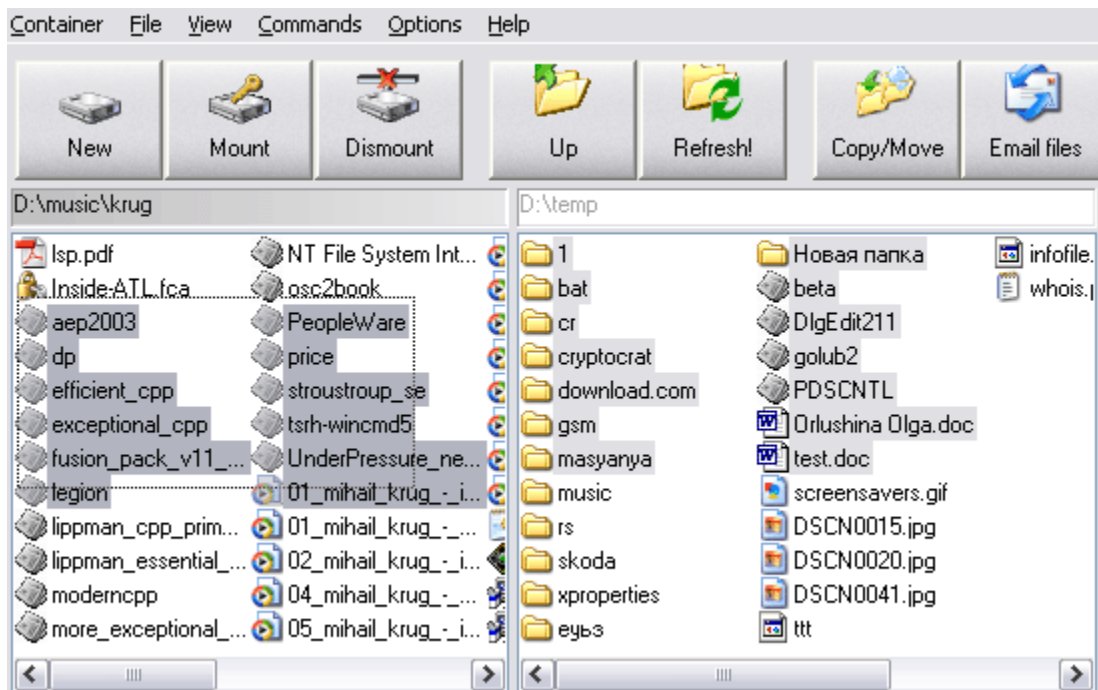
Picture 1. *Two files panes. Selected files in the active pane*

For example, you can copy/move files from your hard drive to the <u>virtual drive</u>.
Read

To copy files from the file active pane to the inactive pane, select files in the active pane with the mouse and click the **Copy/Move** button on the main toolbar or just press **Ctrl-C:**
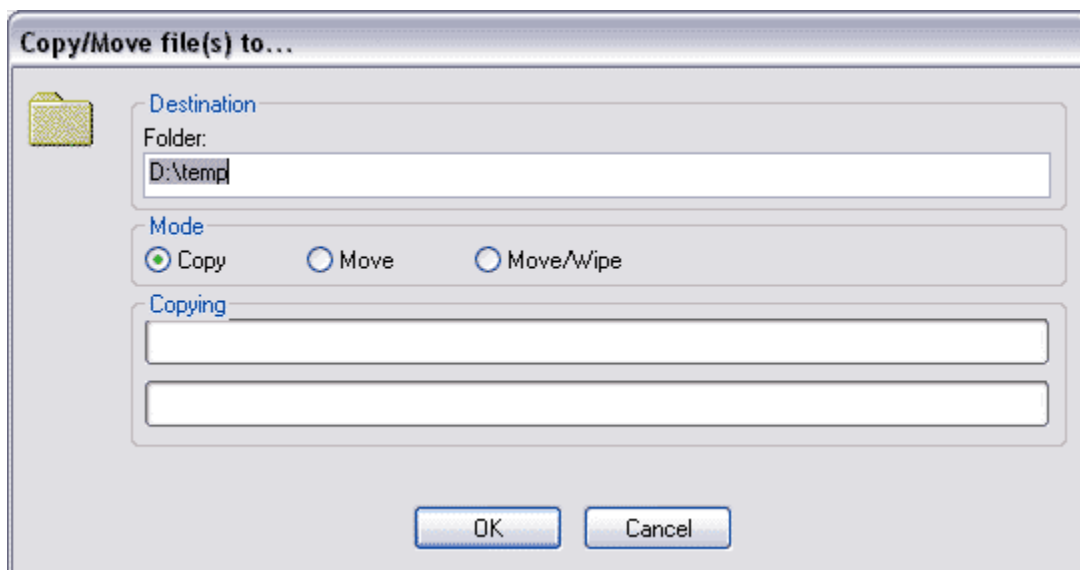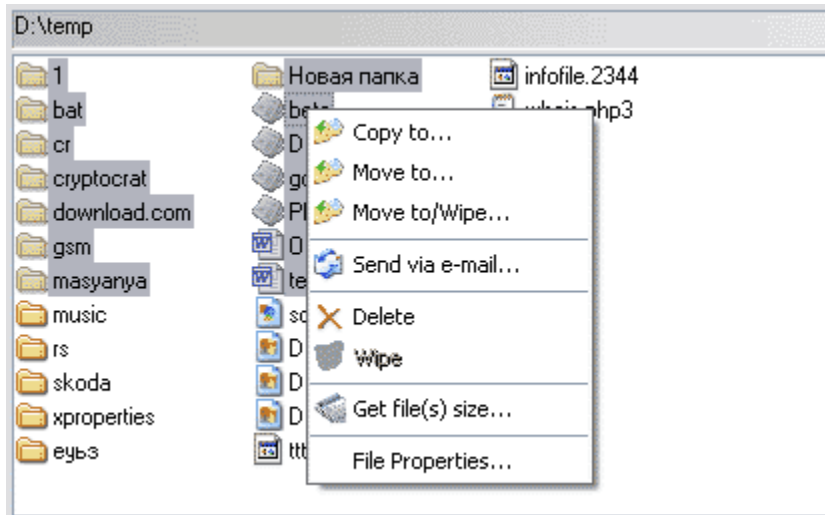

Picture 2. *File copy dialog*

In this dialog choose the copying mode: Copy, Move or Move/Wipe.

Please mind, that files will not be deleted when in the Move/Wipe mode, if the source and destination drives are the same. In this case files will just be moved.

How to remove files

To delete a file or several files or folders, select it with the mouse:

Picture 1. *Files pane. Selected files*

Then right click the selected files and select the **"Delete"** command in the popup menu. You can also click the **Delete** button on the main toolbar menu

How to securely delete files

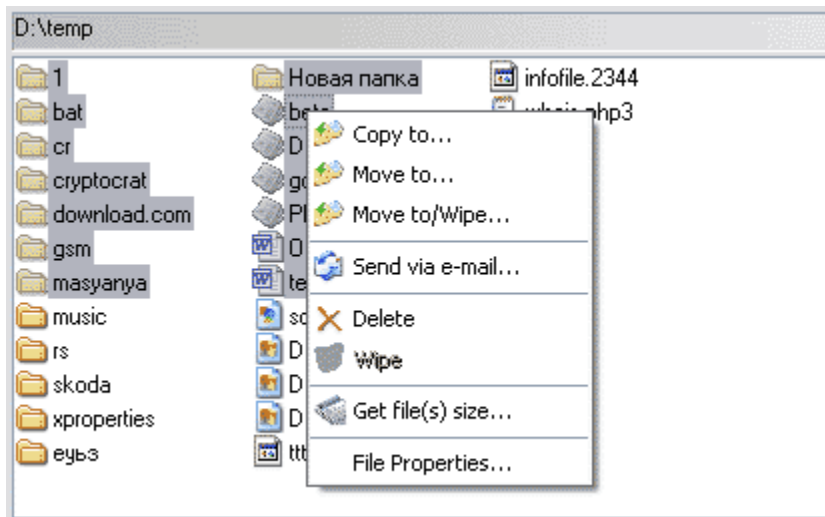To <u>wipe file</u> or several files or folders, select it with the mouse:

Picture 1. *Files pane. Selected files*

Then right click the selected files and select the **"Wipe"** command in the popup menu. You can also click the **Wipe** button on the main toolbar menu

How to create container

To create a new container select the "Container->New" menu command or just click the "New" button on the main toolbar.

Picture 1. *Where to create a container file*

Click the "Browse" button and select the folder to create the file. Also type the file name for the container. You can create the container in a usual folder or in a network folder. For example, "d:\data\newcontainer.cc", "\\comp2\mydata\documents.cc"

Press the "Next>" button to set encryption options for this container file

Picture 2. *How to encrypt data in container*

In the **"Encryption mode"** field you can choose the encryption algorithm for you to use to encrypt your data.
In the **"Hash function"** field you can choose the algorithm for you to use to convert your password to the random binary encryption key.
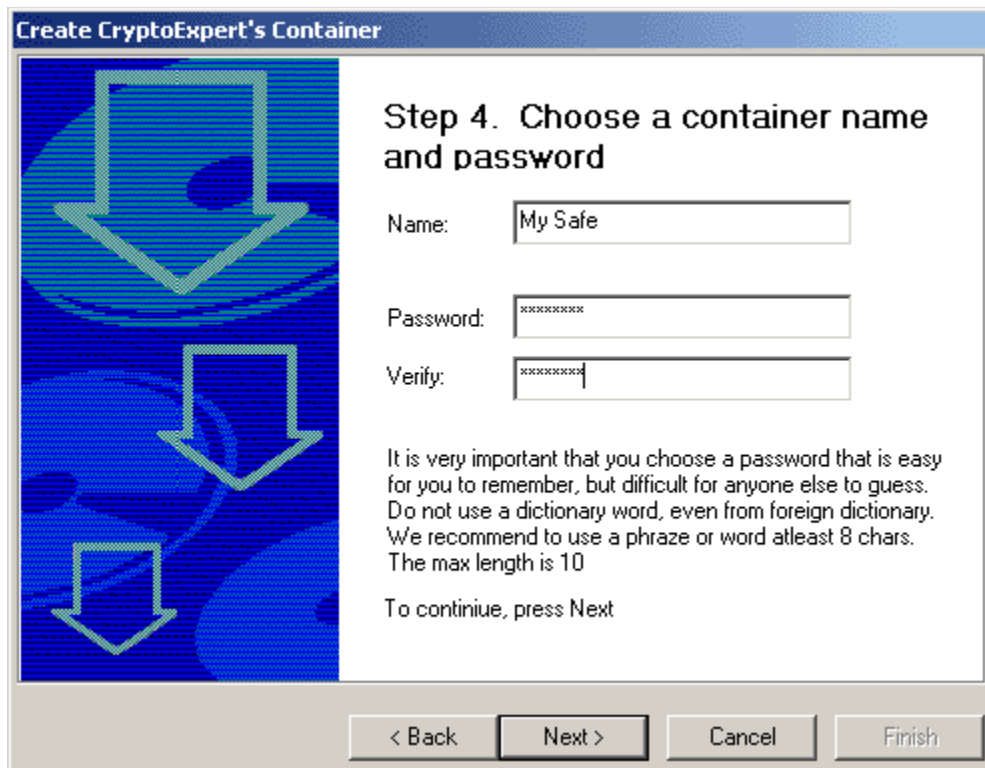
Press the **"Next>"** button to specify the container size

Picture 3. *How to set container's size*

On this page type your container size. For example, the 15 Mb value in the Size field means that you are going to create a container that will be able to store 15 Megabytes of data.

Press the **"Next>"** button to specify the container password:

Picture 4. *How to set container's password*

In the **"Name"** field type the drive label. It will be visible for all applications.
In the **"Password"** and **"Verify"** fields type the password used to encrypt the data inside the container file. This password will be used in the future to mount the container.

Press the **"Next>"** button to finish the container creation

**Picture 5.** *The latest page of this wizard*

It is the last page of this wizard. Check the **"Mount container as drive after creation"** box to mount the container after creation. Press the Finish button and wait until the container is created.

From Program Menu

Now, select the **Container / Mount...** menu command or click the Mount button on the main toolbar.

If no container file is selected in the active files pane you will be asked to find the container file.

Then enter the password to the mount container.
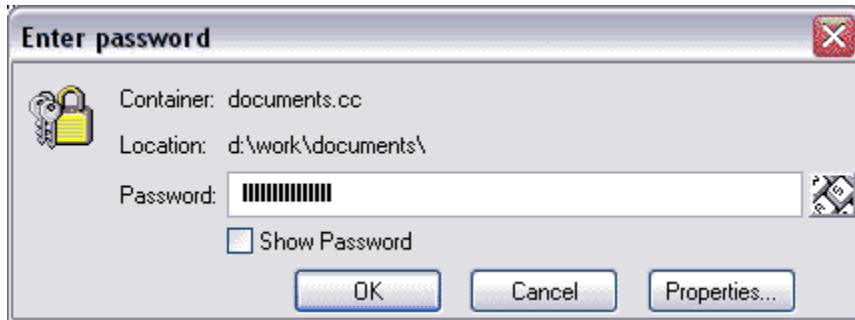
Picture 1. *Password dialog*

Read more about Password Dialog

Now, you can copy files to this virtual drive using any favourite program, like Windows Explorer, Windows Commander, Norton Commander or any other (or use the CryptoExpert program to copy/explore files).

From "Encrypted Containers" Pane

To mount a container, just double click it (make sure that active files pane is in the "Encrypted Containers" mode)

Or right click it and select the **"Mount"** command in the popup menu
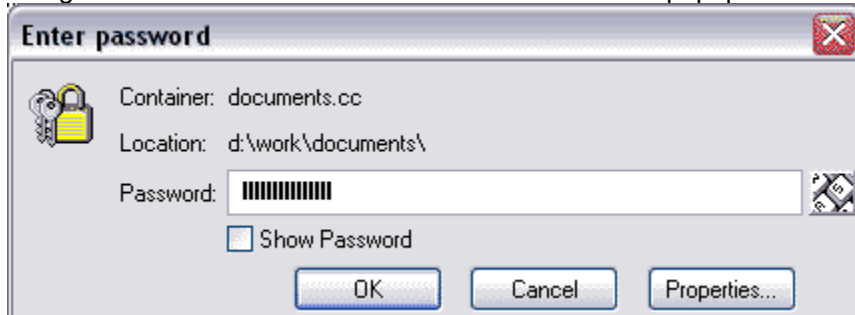
Then enter the password in the password dialog:
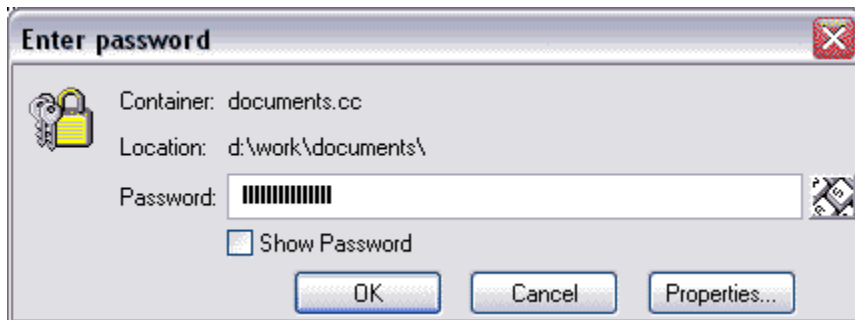
See Also

Read more about

From Tray Menu

When you click the program tray icon, the menu will appear.
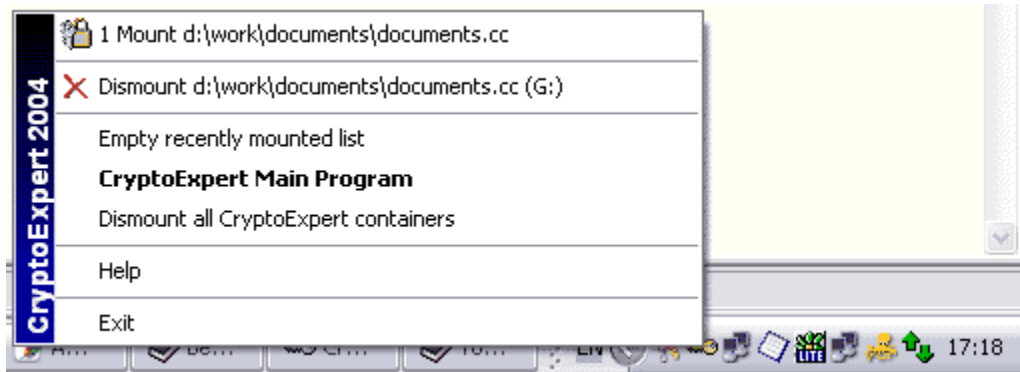
Picture 1. *Tray menu*

This menu has the recently mounted containers.

So, to mount a container, select this container in the list

From Command Line

To mount the existing container execute the following command:

**cexpert.exe /MOUNT="d:\path\container.cc" [/LETTER="D:"] [/AUTOMOUNT>]
[/PASSWORD="password"] [/REMEMBER]**

Where:

/MOUNT or /M - command to mount specified container file
/LETTER or /L - command to specify what drive letter should be assigned with the container. If the letter is not free, CryptoExpert will choose the first free drive letter for this container
/AUTOMOUNT or /AM - marks the container to be mounted at Windows start up
/PASSWORD or /PWD - the password to mount container. If this switch is not specified - the password will be asked
/REMEMBER or /RP - the password for the container will be remembered (on the computer) and will not be asked in future.

Examples:

a) mount the d:\secret\mycontainer.cc file which was encrypted by the password "mydog". Assign "Z:" drive letter for this container.

cexpert.exe /m="d:\secret\mycontainer.cc" /l="z:" /pwd="mydog"

b) mount the d:\file.cc container . The password will be asked. Assign any free drive letter for the container.

cexpert.exe /m="d:\file.cc"

c)) mount the d:\file.cc container . The password will be asked and then it will be remembered and will not be asked again in future

cexpert.exe /m="d:\file.cc" /remember (password will be asked)
then you can use command **cexpert.exe /m="d:\file.cc"** (password will not be asked, because it is remembered)

d)) mount the d:\file.cc container. And make it mounted at every Windows start up automatically (password will be asked at every windows start up. Specify/remember the switch to enter the password for the first time only)

cexpert.exe /m="d:\file.cc" /automount

e) mount the d:\file.cc container. Specify the password "secret". Remember this password. Make the container mounted at every windows start up automatically without asking the password. Mount it as drive T: every time (at every windows start up)

cexpert.exe /m="d:\file.cc" /pwd="secret" /remember /automount /L="T:"

From "Encrypted Containers" Pane

To dismount a <u>virtual drive</u>, find the mounted container in the "Encrypted Containers" pane. Make sure it is mounted ("Yes" in the **Mounted** column) and double click it.
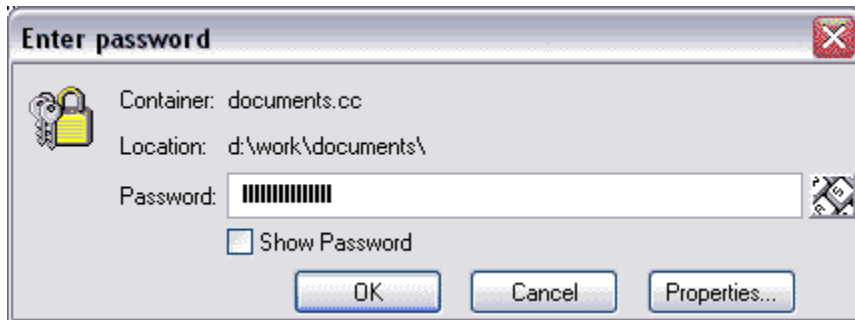
Picture 1. *"Encrypted Containers" mode in files pane.*

You can also dismount a container from the popup menu. Right click on this container and select the **Dismount** command in the popup menu.
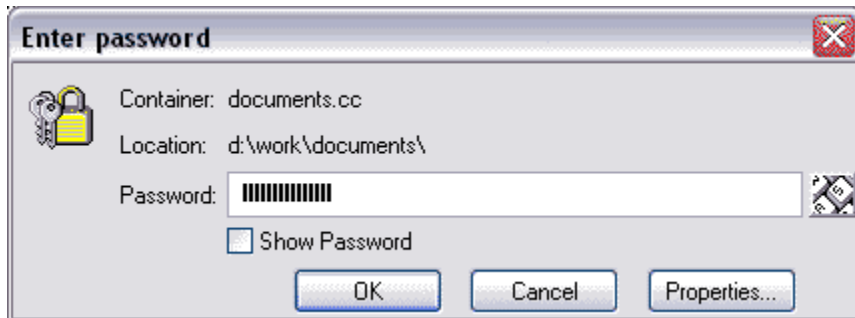
Picture 2. *How to dismount drive from context menu*

From Tray Menu

When you click on program tray icon, menu will appear.
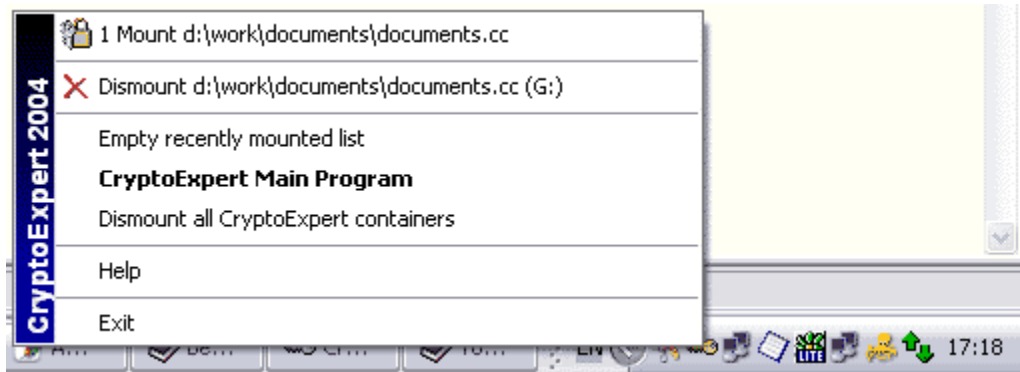
Picture 1. *Tray menu*

This menu has recently mounted containers.

So, to dismount container, choose this container from the list

From Command Line

To dismount the existing container execute the following command

cexpert.exe /UNMOUNT="d:\path\container.cc"
or
cexpert.exe /UNMOUNT /LETTER="Z:"
or
cexpert.exe /UNMOUNT

Where:

/UNMOUNT or /U - – the command to dismount the specified container file
/LETTER or /L - – the command to specify the drive letter to be dismounted. You should specify the container path or the drive letter

Examples:

a) unmount all mounted containers

cexpert.exe /u

b) dismount the "d:\test.cc" container, that was mounted as the unknown drive.

cexpert.exe /u="d:\test.cc"

c) dismount the "d:\test.cc" container that was mounted as the T: drive

cexpert.exe /u /l="T:"

About Tray Icon

Even when CryptoExpert has hidden main window, it is possible to show it again by double clicking the program icon in the tray (lower right corner of your screen).

Picture 1. *Yellow key. CryptoExpert icon in the tray*

How to mount container using tray icon

When you click the program tray icon, the menu will appear.
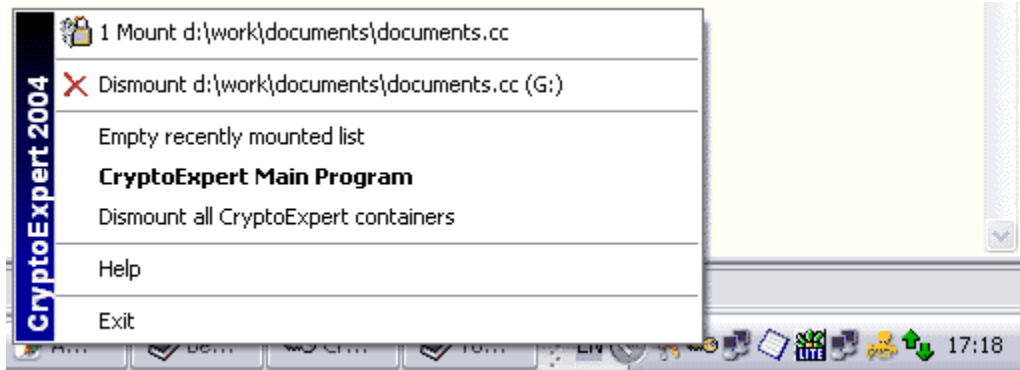
Picture 1. *Tray menu*

This menu has the recently mounted containers.

So, to mount a container, select this container in the list

How to dismount container using tray icon

When you click on program tray icon, menu will appear.
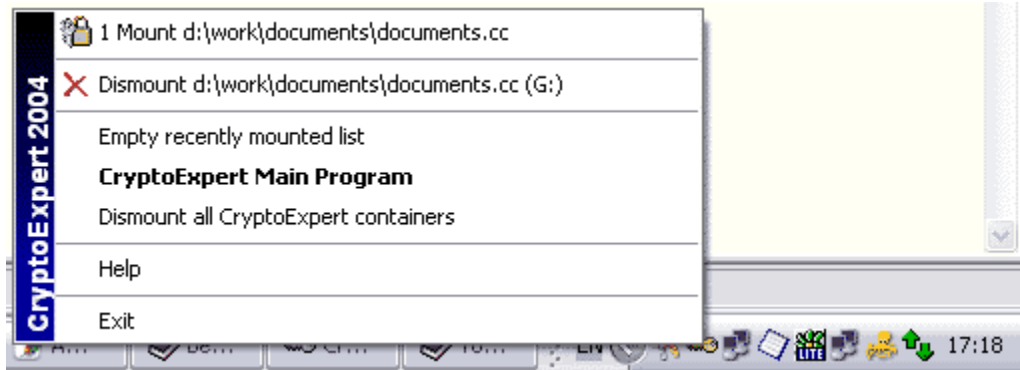
Picture 1. *Tray menu*

This menu has recently mounted containers.

So, to dismount container, choose this container from the list

Command Line Syntax

It is possible to perform **CryptoExpert** commands from the command line. Common command line syntax is described below:

   cexpert.exe [switch1] [switch2] [switch3] ... [switchN]

switch   Switches used to define a specific type of operation

Notes

switches are not case sensitive, you may write them both in upper and in lower case.

Detailed syntax

   cexpert.exe
or
   cexpert.exe /TRAY
or
   cexpert.exe /INSTALL | /UNINSTALL
or
   **cexpert.exe /MOUNT="d:\path\container.cc" [/LETTER="D:"] [/AUTOMOUNT>]
[/PASSWORD="password"] [/REMEMBER]**
or
   cexpert.exe /UNMOUNT="d:\path\container.cc"
or
   cexpert.exe /UNMOUNT /LETTER="D:"
or

Notes

1. '**[**' and '**]**' brackets mean not required statement. I.e. this switch can be specified or not.

2. '**<**' and '**>**' brackets mean **required** statement. I.e. this statement must be specified.

3. '**|**' symbol means **OR.** I.e. one switch or another

Mount container

To mount the existing container execute the following command:

**cexpert.exe /MOUNT="d:\path\container.cc" [/LETTER="D:"] [/AUTOMOUNT>]
[/PASSWORD="password"] [/REMEMBER]**

Where:

/MOUNT or /M - command to mount specified container file
/LETTER or /L - command to specify what drive letter should be assigned with the container. If the letter is not free, CryptoExpert will choose the first free drive letter for this container
/AUTOMOUNT or /AM - marks the container to be mounted at Windows start up
/PASSWORD or /PWD - the password to mount container. If this switch is not specified - the password will be asked
/REMEMBER or /RP - the password for the container will be remembered (on the computer) and will not be asked in future.

Examples:

a) mount the d:\secret\mycontainer.cc file which was encrypted by the password "mydog". Assign "Z:" drive letter for this container.

cexpert.exe /m="d:\secret\mycontainer.cc" /l="z:" /pwd="mydog"

b) mount the d:\file.cc container . The password will be asked. Assign any free drive letter for the container.

cexpert.exe /m="d:\file.cc"

c)) mount the d:\file.cc container . The password will be asked and then it will be remembered and will not be asked again in future

cexpert.exe /m="d:\file.cc" /remember (password will be asked)
then you can use command **cexpert.exe /m="d:\file.cc"**   (password will not be asked, because it is remembered)

d)) mount the d:\file.cc container. And make it mounted at every Windows start up automatically (password will be asked at every windows start up. Specify/remember the switch to enter the password for the first time only)

cexpert.exe /m="d:\file.cc" /automount

e) mount the d:\file.cc container. Specify the password "secret". Remember this password. Make the container mounted at every windows start up automatically without asking the password. Mount it as drive T: every time (at every windows start up)

cexpert.exe /m="d:\file.cc" /pwd="secret" /remember /automount /L="T:"

Dismount a container

To dismount the existing container execute the following command

cexpert.exe /UNMOUNT="d:\path\container.cc"
or
cexpert.exe /UNMOUNT /LETTER="Z:"
or
cexpert.exe /UNMOUNT

Where:

/UNMOUNT or /U - – the command to dismount the specified container file
/LETTER or /L - – the command to specify the drive letter to be dismounted. You should specify the container path or the drive letter

Examples:

a) unmount all mounted containers

cexpert.exe /u

b) dismount the "d:\test.cc" container, that was mounted as the unknown drive.

cexpert.exe /u="d:\test.cc"

c) dismount the "d:\test.cc" container that was mounted as the T: drive

cexpert.exe /u /l="T:"

Install / uninstall drivers

Sometimes, after installating specific Windows software on your computer, or after moving the CryptoExpert program folder to other computer, CryptoExpert drivers no longer work. To repair the drivers just run CryptoExpert as **"cexpert.exe /i"**, or **"cexpert.exe /install"**

To uninstall and remove all CC drivers from your computer just run **"cexpert.exe /u"** or **"cexpert.exe /uninstall"**.

Usually, these commands are executed automatically by the CC installation program

/TRAY switch

/TRAY command line switch is used to run CryptoExpert hidden with yellow icon in the windows system tray.

When specifying this command all Windows start up containers will be mounted automatically

Q: I seen two versions of CryptoExpert - Standard and Professional. What is difference?
A: Yes, CryptoExpert has two editions - standard and professional. The difference is: Standard version can mount one container at the same one. And can create container with size up to 100 MB. Professional version can create containers with size up to 2 GB and can mount several containers at the same time.

Q: What is happened with my encrypted drives when I close CryptoExpert program?
A: If you minimize or close your CryptoExpert window - your virtual drives aren't disappeared. Any loaded volume still remains loaded. You can copy/move/delete/etc files on encrypted drive using Windows Explorer, MS-DOS prompt, or any another program. To mount/dismount new drive just use tray menu of the CryptoExpert (yellow key in tray) or just run cryptoexpert from START->Programs menu

Q: How it works?
A: CryptoExpert uses an on- the-fly encryption system to encrypt and decrypt data. Data is stored in the encrypted form, but when it is requested by any application, it gets decrypted on-the-fly. Conversely, unencrypted data to be stored is encrypted instantaneously and then stored. The CryptoExpert   system mounts a volume file to create a "virtual drive" that appears to applications and users like any other physical drive. Any data that the user attempts to write to this drive is intercepted by CryptoExpert, encrypted, and written to the volume file. Attempts to read from this volume are also intercepted, and the relevant data is read by CryptoExpert from the volume file, decrypted, and presented to the application trying to read the data.
Dismounting the CryptoExpert "virtual drive" ensures that data cannot be read from or written to it. All data is stored encrypted within the "container". As far as windows is concerned, there is a 'new' disk that has suddenly appeared. When the program exists or the volume is unmounted, the file system stays encrypted and there is absolutely no way anyone can recover/get the data without the pass phrase.

Q: What is a "volume" / "virtual drive"?
A: A "volume" is an encrypted container that CryptoExpert creates. It shows up under Windows as a new drive (E: or F: etc.)

Q: How is secure my data?
A: Passwords within most programs (Word, Excel, Access, etc.) can be broken by mere novices without any computing knowledge. Such password breaking tools are easily available on the World Wide Web, for as little as $5.95, or sometimes even for free! A file that is encrypted with a strong encryption algorithm, for example Blowfish   that CryptoExpert uses, is statistically impregnable against brute force attacks. It would take 10 years for all the computers in existence to break this encrypted file! To put this in perspective, the age of the universe is 10PEears!

Q: Why do I need CryptoExpert?
A: Because it is the easiest way to ensure privacy of your data. CryptoExpert guarantees the sanctity of your data by harnessing the power of a powerful encryption algorithm that would take all the computers in the world working together more than the age of the universe to decipher. Using CryptoExpert, you can secure your data, be it in any form textual, graphical, audio or video.

Q: What happens in case of a drive crash?
A: Hard drives, like any other piece of electronic equipment, crash for a variety of reasons. We very strongly recommend routine backups of all important data including CryptoExpert   files.

Q: What happens to my data when CryptoExpert is Uninstalled?
A: Even if CryptoExpert is uninstalled the encrypted volume will stay intact. The security of your data is not jeopardised in any way. However, you will not be able to access the volume unless you have CryptoExpert installed on the machine.

How to order

Here are two versions of this software: PE (Personal Edition) and Professional. To find out what version you use at the moment, select the Help->About... menu item.

Choose which version of the software you wish ro order:

or

Professional version

CryptoExpert PE (Personal Edition) is "try-before-you-buy" software. To check what version do you use at this moment, just choose menu item Help->About. Registration gives you the right to use **CryptoExpert PE** after the 30-day trial period, receive technical support and use features available only for registered users including 1 home license. If you have a question about the registration procedure details, write a message to sales@secureaction.com.

The registration of CryptoExpert PE gives:
1 user home license (for noncommercial usage, at home only)

- Ability to mount/unmount encrypted container

- No nags at startup and in messages

- Ability to use passwords with length more than 3 symbols

- Using powerful encryption algorithm to encrypt your data - CAST 128 bit

- Ability to create containers larger than 20 MB (demo version restriction)

- Lifetime technical support including support via e-mail.

- FREE upgrade to new versions.

- Product notification by e-mail.

- Beta testing for newest version.

After registration (in 1 **hour**) you will receive **Activation Code(s)** and detailed instructions**. This code will transform CryptoExpert to fully registered version and enable all disabled features.**

You can register your copy of **CryptoExpert 2004 PE** for US$39.95

To order the software just go to URL:

http://www.cryptoexpert.com/std/order/

The program can be ordered using credit cards: **VISA, MasterCard, American Express, Dinners Club, Switch, Solo**
It can be ordered in 1 minute via our SSL sales server (online) or via Mail, FAX, Purchase Order and other..
You will also receive an invoice.

Professional

CryptoExpert Pro (Professional Version) is a "try-before-you-buy" software. To find out what version you use at the moment, select the Help->About... menu item. The registration provides you with the right to use CryptoExpert Pro after the 30-day trial period, to get free technical support and use the features available only for the registered users including one business license. If you have any questions about the registration procedure, contact us at sales@secureaction.com.

The **CryptoExpert Pro** registration provides you with:

One user business license (for professional, commercial use)

- The ability to mount/dismount several encrypted containers simultaneously

- No nags at startup and in messages

- The ability to use four powerful encryption algorithms (PE version includes 1 algorithm only)

- The ability to share the virtual drive in a network and load containers from other network drives

- The ability to use more than 3 symbols length passwords

- The ability to create containers up to 2 GB size

- The ability to mount an unlimited number of virtual drives at the same time

- Lifetime technical support including support via e-mail.

- FREE upgrade to new versions.

- Product notification by e-mail.

- Beta testing for the latest version.

You will receive the Activation Code(s) and the detailed instructions after the registration (within the hour). This code will transform CryptoExpert to the fully registered version and enable all the disabled features.

You can register your copy of CryptoExpert 2004 Professional for US$59.95. Volume discounts available.

http://www.cryptoexpert.com/pro/order/

Advanced Encryption Package 2004 Professional
()

AEP2004 Pro allows you to encrypt, make self-
executable files and even shred files contents!
Work with .ZIP files!

AEP2004 Pro features:

* Using 17 powerful encryption algorithms to encrypt
  your data: DESX, BLOWFISH, RIJNDAEL(AES), CAST,
  3-DES, RC2, DIAMOND2, TEA, SAFER, 3-WAY, GOST,
  SHARK, SQUARE, SKIPJACK, TWOFISH, MARS, SERPENT
* Complete .ZIP support (creating .zip
  archives, browsing & extracting ZIP contents)
* Making self-extracting encrypted executable files
  to send it via e-mail to people who do not have
  AEP2004
* Built in file shredder - i.e. wiping the contents
  of the original pre-encrypted file beyond recovery
  to make sure that not even a trace remains after
  shredding. (matching and exceeding the
  specifications of the U.S. Department of Defence)
  to stop hardware recovery tools.
* Ability to send encrypted files and selfextractors
  via email (MAPI)
* Ability to encrypt text to send it via your
  favourite e-mail program like Outlook Express,
  Eudora, ICQ and etc
* Integrating with Windows (TM) Explorer. I.e. ability
  to encrypt/decrypt/shred files directly from Explorer
  context menu
* Complete command line interface support
* Ability to assign a riddle with your password inside
  encrypted file
* Built-in packer to reduce a size of encrypted files. So,
  AEP2004 is not only encryptor, but tool like WinZip!
* Skins support! And 12+ nice-looking skins for program.
* User-Friendly easy-to-understand Graphical interface
  designed to hide the complexities of encryption
  technology from the end user.

Secure Notes Organizer
(http://www.notesorganizer.com)

lets you store and arrange all your information in a tree   outline   form. The possibilities for its use are
practically   endless: to-do lists, recipes, project notes, personal   contacts,   bookmark   lists,
reports, term papers and more.

It allows you:

* Organizing   information   in   a very convenient form -
  folders. Every   folder   can   be   represented as Tree,

Calendar or Stack of Shortcuts

* Arranging items using mouse

* Searching information in all database

* Instant saving changes and minimizing using ESC key

* Automatical URL recognition in the document

* Protecting document by password

* Using Multi-lingual interface

* Customizing menus and toolbars

Founded in 1998, SecureAction Research is an award winning, software engineering company, that has since developed, and continues to develop, a wide scope of quality software products. The SecureAction software assortment is composed of high-quality software products, e.g. applications, software components and controls, to be used in all major Windows™ systems.

Our registered office:
SecureAction Research, LLC
25 Greystone Manor, Lewes, Sussex County, Delaware, 19958, USA

Our corporate web site:

SecureAction is a member of ASP and ISDEF.

To contact us, just drop a message via e-mail:

to our support   team

If you have already purchased license(s) for our products, please include your UserID. We quickly respond to all questions submitted to this e-mail in the order they are received. If you are not yet a SecureAction customer, please also use this mail. Our staff is available to respond to your inquiries 24 hours a day, excluding holidays. Messages are normally answered within two hours.

to our sales team sales@secureaction.com

You also can contact with us by recording a voice message on our voice mail answering machine (please *include your email* into this voice message):

Phone and fax:

 USA:
   +1-800-XCRYPTO   or
   +1-800-927-9786

Outside USA:
   +1-501-421-3143

Please visit our site in Internet -
http://www.secureaction.com (Corporate site)
 (CryptoExpert Site)

Every time you can find on our site information about new version of SecureAction's products,
announces, new beta-versions, special offers and more.

In this mode, First or Second pane shows containers repository. You can see here all your encrypted containers and its states.

To see this pane, click **"Drives"** Button, then click on **"Containers"** icon.

When **Folders pane** has *folders mode,* you can change the root folder for active files pane by changing folder in folders pane. To activate folders mode in **folders pane**, just click on **Folders** button.

In this mode, **Folders Pane** has to icons to click : **"Containers"** and **"All Drives"**. By clicking on "Containers" icon, you change the mode of active files pane to "Encrypted Containers" mode

In this mode, First or Second Pane shows folders and files

Virtual drive looks like any other storage device in your system.

Picture 1. *How virtual drive looks in Windows Explorer*

You can use CryptoExpert to mount your existing encrypted container file to make it visible as virtual drive. At **Picture 1**, **"Documents G:"** drive is not real device, it is virtual drive of CryptoExpert.

When you delete your sensitive files from a disk on your computer, the Windows operating system does not erase these files' contents from the disk - it only deletes 'references' to these files from system tables. Contents of the deleted file (file body) continue to be stored on the disk and can be easily restored using any disk tool utility.After running a secure file deleting utility, it is impossible to restore the deleted data.