Reuschtools Administrators' Manual

This manual uses didactic coloring:

```
example
```

```
expanded example
```

```
wrong
```

Contents

1: rtcmd.exe

Back-End console application.

1.1 Data Backup (L)

1.1.1 PrivateBackup (pb)

create or update zip file

```
rtcmd pb [-OPT] [p=PASSWORD|#SLOT] [u=USER,..] s=SOURCE [t[TOPT]=TARGET] ..
```

PrivateBackup creates one or more Zip compressed backup copies from a folder or a drive. If a file is EFS encrypted, it is assured to remain encrypted inside all backup copies.

```
rtcmd pb s=MyItems
```

The content of the folder MyItems will be copied into a Zip file.

1.1.1.1 OPT

General Options, a combination of the following characters:

	Behaviour
a Access Control	Access Control Lists will be included into the backup.
b Binary Check	All source files are compared bit by bit to the corresponding target files. If a file has changed, it will be substituted. By default static files like .exe or .dll are compared only by their date and size. This behaviour will speed up the process. However, if a static file has been modified while it's date and size remain equal, it is sucpecious to be a malicious file modified by an intrucor. The Log will mark such files with 'B'.
f Forensic Check	Same as Binary Check. If a sucpecious files is detected, a message box will appear before the file is replaced.
m Move	Deletes the source folder after a successfull backup.
n New	A new backup will be created and no Template will be used.
u Update	A Zip Backup will be created only is the content of the source folder has changed since the previous backup.
tx Targets	At least x targets must exist.

v VSS	VSS will be activated immediately. By default, VSS will be activated as soon as an open source file is detected.
x eXtended	The content of Reparse Points and Volume Mount Points will be included into the backup. Use this option to create complex backup scenarions.
Encryption	
e Encrypt	Zip files on local hard drives (NTFS), will be encrypted using EFS. All other Zip files will also be sealed.
k Key	Reports an error when a file is EFS encrypted. This option is useful to backup the EFS key itself.
p Password	Enables Zip encryption and asks for a password.
r Raw	EFS encrypted files will be backed up as RAW files. This is the default for unencrypted folders. If you do not own the EFS key for a file, it will always be backed up as RAW file.
s Seal	Seals all Zip archives with EFS. This is the default for encrypted folders.
Dialog	
i[x] Integrate	No user interaction. The Integration Number x determines if error messages, warnings, or dialogs will be displayed.
o[x] Optional	The wizard will show up and parameters provided by the command line can be modified. The wizard will store theses changes in slot x for the next run.
Log File	
q Quiet	Displays only a start and stop message. If successful, a complete log file will be written to RT_LOG and in case of failure to RT_ERROR.
t Talk	Show Access Control Lists, requires CONTROL -a to be set.

```
rtcmd pb -o3nm s=MyItems
```

The folder MyItems will be copied into a Zip file. No template will be used. The source folder will be deleted after successful backup. The wizard will show up and command line parameters can be modified. Changes will be stored in slot number 3 and reused when the wizard starts again.

1.1.1.2 PASSWORD

Passes a Zip Password or a Zip Password Slot.

```
rtcmd pb p=38zec47xc662 s=MyItems
```

The content of the folder MyItems will copied into a Zip file with Zip encryption.

1.1.1.3 USER

You must have the Public Keys for the USERs added here. It will trigger EFS encryption for the content of the generated Zip file.

```
rtcmd pb u=ben u=bob s=MyItems
```

You, Ben and Bob will be able to read the content of the Zip file.

1.1.1.4 SOURCE

Folder to be backed up. SOURCE can contain Path Wildcards:

```
rtcmd pb s="*DOCUMENTS\My Items"
```

```
rtcmd pb s="C:\Users\Ben\Documents\My Items"
```

The folder My Items will copied to a Zip file. The folder is located in Ben's Documents directory and Ben is the current user. If the name of a folder contains spaces, it must be set in quotes.

1.1.1.5 TOPT

Target Options, a combination of the following characters:

dX Day	Delete all Number Zips in the destination folder that are older than X days.
f Files	Delete as many old Number Zips in the destination folder, until the space for the new Zip is sufficient.
fX Files	Keep the latest X Number Zips in the destination folder.
m Memory	Delete as many old Zips in the destination folder, until the space for the new Zip is sufficient.
mX Memory	Delete as many old archives in the destination folder, until the disk space required by the target folder will be less than X MB.
nX Number	X targets will be selected at maximum. Use this option together with Drive Wildcards.
o Optional	This target is optional. Skip without ERROR if it is not accessible.
oX Optional	At least X targets must be accessible or the backup will fail with ERROR. Use this option together with Drive Wildcards.

```
rtcmd pb s=MyLogs to2n3f30=*NET\*
```

A minimum of 2 network targets must be accessible. A maximum of 3 network targets will be served. There will be a maximum of 30 Number Zips in each target directory.

1.1.1.6 TARGET

Target Zip file. If no file name is specified, the filename will be the name of the source folder with .zip extension:

```
rtcmd pb s=MyItems t=X:\
rtcmd pb s=MyItems t=X:\MyItems.zip
```

If a filename has been specified for a previous target, it will be used:

```
rtcmd pb s=MyItems t=c:\Jan_2024.zip t=d:\
rtcmd pb s=MyItems t=c:\Jan_2024.zip t=d:\Jan_2024.zip
```

You can control encryption by specifying a file extension. The folder MyItems will be copied to a transportable EFS encrypted Zip:

```
rtcmd pb s=MyItems t=.seal
rtcmd pb s=MyItems t=MyItems.seal
```

A * will create a Number Zip with the name consisting of the current date and time (`27 January 2022 22:42:42`):

```
rtcmd pb s=MyItems t=*
rtcmd pb s=MyItems t=220127_224242.zip
```

TARGET can contain Backup Wildcards:

```
rtcmd pb s=MyItems t=D:\*ARCH\
rtcmd pb s=MyItems t=D:\RtArch\ben\Documents\MyItems\MyItems.zip
```

1.1.2 PrivateRestore (pr)

restore from zip file

`rtcmd pr [-OPT] [p=PASSWORD|#SLOT] [t=TARGET] s=SOURCE ...`

Private Restore can show a chronological list with all backup copies, that match to a folder or a drive.

Private Restore can restore a folder or a drive from a Zip file.

```
rtcmd pr s=MyItems.zip
```

A folder with the name MyItems will be created and restored from MyItems.zip.

1.1.2.1 OPT

General Options, a combination of the following characters:

Restore	
a Access Control	Access Control Lists are restored.
b Binary Check	All files are verified bit by bit.
f Forensic Check	Like Binary Check, a message box appears before files are replaced.
m Move	Deletes the Zip file after successfull restore.
n New	Replaces all files even if they have not been modified.
x eXtended	Restoring includes the content of Reparse Points and Volume Mount Points.
Dialog	
i[x] Integrate	No user interaction. The Integration Number x determines if error messages, warnings, or dialogs will be displayed.
o[x] Optional	The wizard will show up and parameters provided by the command line can be modified. The wizard will store theses changes in slot x for the next run.
Log File	
q Quiet	Displays only a start and stop message. If successful, a complete log file will be written to RT_LOG and in case of failure to RT_ERROR.
t Talk	Show Access Control Lists, requires CONTROL a to be set.

```
rtcmd pr -o3m s=MyItems.zip
```

The folder MyItems will be restored from MyItems.zip. MyItems.zip will be deleted after a successful restore. The wizard will show up and command line parameters can be modified. Changes will be stored in slot number 3 and reused when the wizard starts again.

1.1.2.2 PASSWORD

```
rtcmd pr p=38zec47xc662 s=MyItems.zip
```

If MyItems.zip is Zip Encryption and you do not pass a password with the command line, you will be asked for the password while the restore is running.

1.1.2.3 SOURCE

You must specifie at least one Zip file. SOURCE can contain a Drive Wildcard, a Backup Wildcard and an Object Wildcard.

```
rtcmd pr t=MyItems s=*HD\*ARCH\* s=*RD\*ARCH\*
```

Scan all hard disks and all removable drives. Look for the latest Zip that matches to MyItems and restore it.

1.1.2.4 TARGET

is optional. Without TARGET, the Zip file specified in SOURCE will be extracted.

If the Zip File has been created with Private Backup, it will contain the origin folder path:

```
rtcmd pr s=Jan_2024.zip t=*
rtcmd pb s=Jan_2024.zip t=C:\Users\Ben\Documents\MyItems
```

TARGET can contain a Path Wildcard:

```
rtcmd pr s=Jan_2024.zip t=*DOCUMENTS\MyItems
rtcmd pb s=Jan_2024.zip t=C:\Users\Ben\Documents\MyItems
```

1.1.3 ZipInfo (zinfo)

show the comment field of a .zip or .seal file

`rtcmd zinfo ZIPFILE|SEALFILE`

1.2 Data Encryption (L)

1.2.1 CryptManager (cman)

mangage or backup encrypted files and folders

`rtcmd cman [FOLDER|FILE]`

1.2.2 Seal (seal)

convert encrypted file to RAW file

`rtcmd seal FILE`

1.2.3 Unseal (unseal)

convert RAW file to encrypted file

`rtcmd unseal FILE`

1.2.4 Encrypt (encrypt)

a file or folder

`rtcmd encrypt [CREDENTIALS] [u=USER,..] FILE|DIRECTORY[\]`

1.2.5 Decrypt (decrypt)

a file or folder

`rtcmd decrypt [CREDENTIALS] FILE|DIRECTORY[\]`

1.3 System Image(L)

1.3.1 InstallBackup (ib)

Create or update System Image

```
rtcmd ib [-OPT] [p=PASSWORD|#SLOT] [t[TOPT]=TARGET] ...
```

```
rtcmd ib
```

Create a System Image from the running Windows® environment and store it inside the current directory.

1.3.1.1 OPT

General Options, a combination of the following characters:

Behaviour	
b Binary Check	All source files are compared bit by bit to the corresponding target files. If a file has changed, it will be substituted. By default static files like .exe or .dll are compared only by their date and size. This behaviour will speed up the process. However, if a static file has been modified while it's date and size remain equal, it is sucpecious to be a malicious file modified by an intrucor. The Log will mark such files with 'B'.
f Forensic Check	Same as Binary Check. If a sucpecious files is detected, a message box will appear before the file is replaced.
n New	A new backup will be created and no Template will be used.
x eXtended	The content of Reparse Points and Volume Mount Points will be included into the backup. Use this option to create complex backup scenarions.
Encryption	
p Password	Enables Zip encryption and asks for a password.
Dialog	
i[x] Integrate	No user interaction. The Integration Number x determines if error messages, warnings, or dialogs will be displayed.
o[x] Optional	The wizard will show up and parameters provided by the command line can be modified. The wizard will store theses changes in slot x for the next run.
Log File	
q Quiet	Displays only a start and stop message. If successful, a complete log file will be written to RT_LOG and in case of failure to RT_ERROR.
t Talk	Show Access Control Lists.

```
rtcmd ib -o1
```

InstallBackup starts with a dialog window to modify the predefined settings(o). The modified settings are stored in registy slot 1(o1). The stored settings will prepopulate the dialog window the next time it is called.

```
rtcmd ib -p
```

Zip Encryption is enabled(p) and a pop up window will ask for the Zip password before the backup is executed.

1.3.1.2 PASSWORD

Enables Zip Encryption and determines the password.

```
rtcmd ib p=38zec47xc662
```

Create a Zip encrypted software backup.

1.3.1.3 TOPT

Target Options, a combination of the following characters:

dX Day	Delete all Number Zips in the destination folder that are older than X days.
f Files	Delete as many old Number Zips in the destination folder, until the space for the new Zip is sufficient.
fX Files	Keep the latest X Number Zips in the destination folder.
m Memory	Delete as many old Zips in the destination folder, until the space for the new Zip is sufficient.
mX Memory	Delete as many old archives in the destination folder, until the disk space required by the target folder will be less than X MB.
nX Number	X targets will be selected at maximum. Use this option together with Drive Wildcards.
o Optional	This target is optional. Skip without ERROR if it is not accessible.
oX Optional	At least X targets must be accessible or the backup will fail with ERROR. Use this option together with Drive Wildcards.

```
rtcmd ib tf5=D:\*
```

```
rtcmd ib tf5=D:\240123_074345.ib
```

Create a software backup on drive D:. The backup will be labled with a timestamp. The target path will contain a maximum number of 5 timestamp backups.

1.3.1.4 TARGET

Target path, target folder or both. Wildcards can be used. If a target folder is specified it must end with '.ib'. Multible TARGETS can bespecified.

```
rtcmd ib t=MyPC.ib
```

```
rtcmd ib t=D:\*ARCH\
rtcmd ib t=D:\RtArch\_PC\22621w64\Windows.ib
```

```
rtcmd ib t=D:\*ARCH\*
rtcmd ib t=D:\RtArch\_PC\22621w64\240123_074345.ib
```

```
rtcmd ib -o1 t=*HD\*ARCH\ to=*RD\*ARCH\ to=*NET\*ARCH\
```

Command line used by the Setup dialog.

1.3.2 InstallRestore (ir)

Restore Windows® environment from System Image

`rtcmd ir [-OPT] [p=PASSWORD|#SLOT] [t=TARGET] [s=SOURCE] ...`

InstallRestore can reset the running Windows®, programs, passwords and settings back to the time of the System Image backup. Data Folders remain unaffected.

InstallRestore can create or update a second Windows® environment on a drive, a USB drive or a second PC. InstallRestore will verify and fix the boot configuration. After a successful restore, the new Windows® environment can be selected and startet from the boot menu.

```
rtcmd ir
```

Restore a Windows® environment. The current directory must be set to a System Image folder. The target Windows® environment is determined by the origine Windows® environment stored inside the System Image.

1.3.2.1 OPT

General Options, a combination of the following characters:

Behaviour

b Binary Check	All source files are compared bit by bit to the corresponding target files. If a file has changed, it will be substituted. By default static files like .exe or .dll are compared only by their date and size. This behaviour will speed up the process. However, if a static file has been modified while it's date and size remain equal, it is sucpecious to be a malicious file modified by an intrucor. The Log will mark such files with 'B'.
d Default	The restored Windows® environment will be preselected when the boot menu appears. Restarting the PC will automatically start the restored environment. However, the boot menu will showup for typically 3 seconds to change this selection.
f Forensic Check	Same as Binary Check. If a sucpecious files is detected, a message box will appear before the file is replaced.
h Hardware	InstallRestore will copy and install all hardware drivers from the running to the newly created Windows®.
l Letters	Adapt drive letters and pathes on the target Windows® environment. See TARGET.
n New	The target Windows® environment will be deleted before the the restore process starts. This means that Data Folders are deleted aswell. This option cannot be used when restoring the running environment.
x eXtended	The content of Reparse Points and Volume Mount Points will be included into the backup. Use this option to create complex backup scenarions.
Encryption	
p Password	Enables Zip encryption and asks for a password.
Dialog	
i[x] Integrate	No user interaction. The Integration Number x determines if error messages, warnings, or dialogs will be displayed.
o[x] Optional	The wizard will show up and parameters provided by the command line can be modified. The wizard will store theses changes in slot x for the next run.
Log File	
q Quiet	Displays only a start and stop message. If successful, a complete log file will be written to RT_LOG and in case of failure to RT_ERROR.
t Talk	Show Access Control Lists.

```
rtcmd ir -o1
```

InstallRestore starts with a dialog window to modify the predefined settings(o). The modified settings

are stored in registy slot 1(o1). The stored settings will prepopulate the dialog window the next time it is called.

1.3.2.2 PASSWORD

Passes a Zip Password or a Zip Password Slot.

```
rtcmd ir p=38zec47xc662
```

```
rtcmd ir p=#ir
```

Select the Zip password that has been stored, when the System Image has been created.

1.3.2.3 SOURCE

Source folder:

```
rtcmd ir s=windows.ib
```

Or path and folder:

```
rtcmd ir s=C:\RtArch\_PC\22621w64\windows.ib
```

Wildcards can be used:

```
rtcmd ir s=*HD\*ARCH\*
```

```
rtcmd ir s=D:\RtArch\_PC\22621w64\240123_074345.ib
```

Search for the latest System Image on all hard disks and restore it.

```
rtcmd ir -o1 s=*HD\*2ARCH\* s=*RD\*2ARCH\* s=*NET\*2ARCH\*
```

Command line used by the Setup dialog.

1.3.2.4 TARGET

TARGET is optional. Without TARGET the origin Windows® drive and folders will be selected.

The behaviour of TARGET depends on -l OPT.

```
rtcmd ir s=C:\*ARCH\*t=D:\
```

-l is not set.

Select the latest System Image from drive C:\ and restore it on drive D:\.

Assuming the System Image has been created on Windows® residing in C:\Windows.

From the current point of view the target Windows® environment will be on drive D:\.

But as soon as you start the new Windows®, the drive letters will be swapped. Drive C:\ will be drive D:\ and D:\ will be C:\.

This is the behaviour of all common backup and imaging applications. The disadvantage is that drive C:\ can be on any harddisk or partition, depending on which Windows® has been started.

```
rtcmd ir -l s=C:\*ARCH\* t=D:\
```

-l is set. Drive letters will be adapted on the target Windows® environment.

If you start Windows® on drive D:\ the Windows® directory will remain in D:\Windows.

A Windows® ID can be specified together with a drive letter. A Windows® ID must exist of 3 characters followed by 3 dots.

```
rtcmd ir -l s=C:\*ARCH\*t=D:\wn2...
```

Drive letters and pathes are adapted. The target Windows® directory will be D:\wn2xwin on X64 or D:\wn2_win on WIN32.

With a Windows® ID multiple Windows® environments can be created on one single partition. This can be helpfull to setup different Windows® versions or configurations on a singel PC.

A Windows® ID can be used to setup a new clean Windows® environment when only one partition is available: Create a System Image from the old Windows®. Restore and start this Image with the help of a Windows® ID. The old Windows® directories can now be deleted with the script 'InstallClean.cmd' to prepare for a new clean Windows® setup.

Adapting drive letters or pathes will trigger the renewing of the WMI database. This process runs in the background but it will delay the first start of a restored Windows® environment.

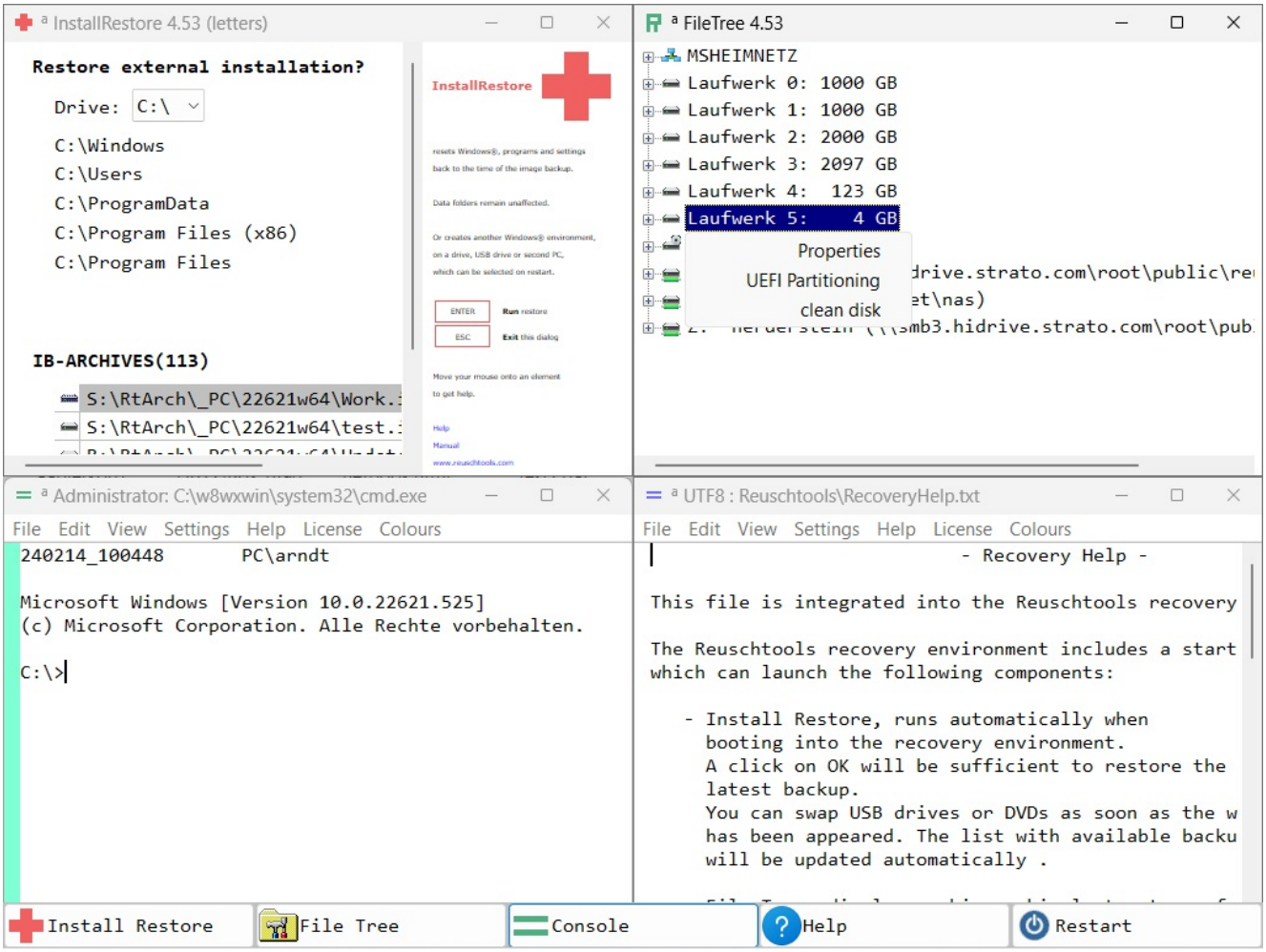
1.3.3 Recovery Environment (recovery)

create, update or remove a recovery environment

```
rtcmd recovery on|off|start|build|burn [-u] [-n] [-p] [-c] [p=PASSWORD] [LETTER:|#N
```

Recovery is an independant Windows® environment based on Windows® PE.

- Includes powerful tools to prepare, install or restore the main Windows® environment.
- Portable and hardware independent.
- Can start from the main Windows® drive or from a USB drive.
- Hovering, the start drive can be removed after Recovery has started.
- BitLocker and UEFI Secure Boot aware.
- Password protection(optional).
- Run fully automated with the AutoRecovery command.
- Run interactive with the Recovery Desktop:



Behaviour	
on	Create Recovery if it does not exist and add an entry into the Boot Menu.
off	Remove Recovery and the entry from the Boot Menu.
start	Schedule Recovery for the next restart of this PC.
build	Create Recovery, don't add an entry into the Boot Menu, but create an .iso file.
burn	Create .iso and burn it onto a CD or DVD.
Options	
-n	Renew Recovery. Use this option if your drive letters have changed, of if you have updated Reuschtools or Windows®
-u	Renew Recovery only if Reuschtools has been updated.
-p	Ask for a logon password to access the Recovery Desktop.

Password	
p=PASSWORD	Specify logon password to access the Recovery Desktop.
Target	
	No target specified. The running Windows® drive will be selected. If this drive has a recovery partition it will be used instead.
LETTER:	Create Recovery on the drive that holds the selected partition.
#NUMBER	Create Recovery on the drive with the specified number. Drive numbers can be found with 'rtcmd tree'.

```
rtcmd Recovery on -n
```

Create or update recovery on the running the Windows® drive.

1.3.4 Set AutoRecovery (autorecovery)

trigger autorecovery for the next boot

`rtcmd autorecovery [p=PASSWORD]`

1.4 Setup

1.4.1 Setup (setup)

Install or uninstall Reuschtools

`rtcmd setup [sm|su|cm|cu k=MODULES|k=rTaRCH][u=SID]`

sm	Setup Machine
su	Setup User
cm	Clear Machine
cu	Clear User

1.4.1.1 MODULES

Sum of hexadecimal codes.

Consult the Dashboard log to get the sum.

Backup	
Dektop Icon	1
One-Click Recovery	2
Backup Restore	4

FileProtection	8
Zip_Rt	10
Console	20
Scripting	40
Editor	80
CryptManager	10000
Hotkeys	
Zoom	200
Shutdown	400
Command	800
Text-Editor	1000
Archiv	2000
Documents	4000
•Setup or update this PC with the following modules:	Dektop Icon

- Backup Restore
- FileProtection
- CryptManager

```
rtcmd setup sm k=1000d
```

The Reuschtools Installer behaves like c_e.exe:

```
reuschtools_4.33_english.exe -x rtcmd setup sm k=1000d
```

This will work but some files will be missing:

```
reuschtools_4.33_english.exe \\PC2 rtcmd setup sm k=1000d
```

1.4.1.2 SID

For internal use.

1.4.2 Uninstall (uninstall)

uninstall Reuschtools

```
rtcmd uninstall [u=SID]
```

1.4.3 KeyImport (keyimport)

import license key

`rtcmd keyimport iu|im [u=SID]`

1.4.4 ClassicMenu (clamen)

switch the Windows 11 kontextmenu on or off

`rtcmd clamen [on|off|-i]`

1.4.5 Set Context Menu (rclick)

Add or remove context menu entries.

`rtcmd rclick sm|su`

will search the Registry for modified entries and update the context menu respectively.

sm	Setup Machine
su	Setup User

1.4.5.1 Registry Keys

all users	`HKLM\Software\Reuschtools\RClick\CLASS\MENU`
current user	`HKCU\Software\Reuschtools\RClick\CLASS\MENU`

1.4.5.2 Registry Values

(Default)	REG_SZ	Command line, can contain WILDCARDS.
IconFile	REG_SZ	File containing the icon to be displayed with the menu item.
IconID	REG_DWORD	Identification number of the icon to be displayd.
IconIndex	REG_DWORD	Index of the icon. If IconID was specified, IconIndex is not required and vice versa.
Menu	REG_DWORD	Number to specify the position within the context nenu. Entries with lower numbers will be inserted first.

1.4.5.3 CLASS

Directory	Right click on a directory icon.
Background	Right click on the background of an open directory.
Drive	Right click on a drive icon or on the background of an open drive.
LocalMachine	Right click on Computer.
Desktop	Right click on the background of the Desktop.

Library	Right click on or into Documents, Pictures, Music or Videos.
RemoteMachine	Right click on a PC in the Network.
Share	Right click on a Share in the Network.
Archiv	Right click on a .zip file or on a .seal file.

1.4.5.4 WILDCARDS

***PATH**	Path of the selected file or folder
***DIR**	Directory without the file or folder
***FILE**	Filename or foldername
***NAME**	Filename without extension
***EXT**	Extension
***MASCH**	PC's name

1.4.5.5 Example

This script (ZipInfoSet.cmd) creates a context menu entry with the name ZipInfo.

It must run with administrative rights because the entry will be for all users.

The CLASS is Archiv to tie the entry to all .zip and .seal files.

The command will list the Zip file's comment data.

An icon from shell32.dll will be used to visualize the entry.

```
set KEY=HKLM\Software\Reuschtools\RClick\Archiv\ZipInfo
set CMD=c_a.exe -xp rtcmd zinfo \"*PATH\"
reg add %KEY% /ve                       /d "%CMD%"     /f
reg add %KEY% /v  IconFile              /d shell32.dll /f
reg add %KEY% /v  IconID   /t REG_DWORD /d 1001        /f
RtCmd rclick sm
```

This script (ZipInfoRemove.cmd) will remove the entry set by ZipInfoSet.cmd:

```
set KEY=HKLM\Software\Reuschtools\RClick\Archiv\ZipInfo
reg delete %KEY% /f
RtCmd rclick sm
```

Both scripts and more examples are in Scripts\ContextMenu\

1.4.6 Password AutoRecovery (pwautorecovery)

Set or remove the Autorecovery Password.

```
rtcmd pwautorecovery [PASSWORD]|clear
```

1.4.7 Password UnProtect (pwunprotect)

Set or remove the Unprotect Password.

```
rtcmd pwunprotect [PASSWORD]|clear
```

1.4.8 Path Environment (path)

Add or remove a path to the environment variable PATH

```
rtcmd path sm|su|cm|cu PATH
```

1.4.9 Install Info (ii)

show basic information and secure boot on the running Windows(R)

```
rtcmd ii
```

1.4.10 License (lic)

verify Reuschtools license

```
rtcmd lic
```

1.5 User Accounts

1.5.1 Account (account)

create user account and logon to generate profile

```
rtcmd account CREDENTIALS [GROUP] ...
```

1.5.2 Efs Key (efskey)

verify or generate EFS key for a user account

```
rtcmd efskey CREDENTIALS [-i] [-KEYLENTH] [PFXPASSWROD]
```

1.5.3 Profiler (profiler)

move folder and create reparse point instead

```
rtcmd profiler [CREDENTIALS] [-nd] [SOURCE][*] [TARGET]
```

1.5.4 Password (password)

generate strong random passwords for user accounts

```
rtcmd password [NUMBER]
```

1.6 File System

1.6.1 CopyMob (copymob)

sychronise pictures or music from a mobile device with this PC

```
rtcmd copymob [pictopc|musictopc|pctopic|musictopc] [MEMORY_INDEX]
```

1.6.2 TreeExplorer (tree)

user interface showing all drives, folders and files

```
rtcmd tree [DIRECTORY]
```

1.6.3 Mirror (mirror)

mirror a directory to another drive or directory

```
rtcmd mirror [-b|-i] [DRIVE|DIRECTORY] DRIVE_LETTER|DIRECTORY
```

1.6.4 List (list)

content of a folder or drive sorted by name, size(-s), extension(-e), modified(-t), access time(-a), mft time(-m) link(-l), stream(-x), ptl(-p), compact(-c)

```
rtcmd list [-s|-e|-t|-a|-m|-l|-x|-p|-c] [DIRECTORY]
```

1.6.5 Protect (protect)

a file or folder from being modified

```
rtcmd protect FILE|DIRECTORY
```

1.6.6 Unprotect (unprotect)

a file or folder from being modified

```
rtcmd unprotect [p=PASSWORD] FILE|DIRECTORY
```

1.6.7 Assert Path (assert)

creat path if it does not exist

```
rtcmd assert DIRECTORY
```

1.6.8 Hardlink (hardlink)

create hardlink

```
rtcmd hardlink TARGET SOURCE
```

1.6.9 Signature (signature)

verify

```
rtcmd signature FILE
```

1.6.10 DeleteTree (deltree)

deletes a folder

```
rtcmd deltree [-o] DIRECTORY
```

1.6.11 File Commands (file)

Create, rename, copy, move or delete a file

```
rtcmd file new|rename|copy|move|delete FILE [TARGET]
```

1.6.12 Clean Tree (cleantree)

creates a folder or deletes it's content

```
rtcmd cleantree DIRECTORY
```

1.6.13 Show Acl (acl)

show 'Security Descriptor String Format' for a file or folder

```
rtcmd acl DIRECTORY|FILE
```

1.6.14 Access Directory (access)

set ACLs for a file or folder to administrator

```
rtcmd access [-r] FILE|DIRECTORY
```

1.6.15 Wim Capture (wimc)

copy drive or folder int a .wim file

```
rtcmd wimc DRIVE|FOLDER WIMFILE
```

1.6.16 Wim Apply (wima)

restore drive or folder from .wim file

```
rtcmd wima WIMFILE DRIVE|FOLDER
```

1.7 Drives

1.7.1 FakeDriveCheck (fakedrivecheck)

verify if a USB flash drive is fake, corrupted or OK

```
rtcmd fakedrivecheck [LETTER]
```

1.7.2 Prepare Drive (prepare)

verify or format a drive for UEFI or MBR

```
rtcmd prepare [-b] [-c] [-m] [-n] [-t] [-u] [-w] LETTER:|#NUMBER
```

1.7.3 Drives (drives)

show drive or partition information

```
rtcmd drives [#NUMBER|#|LETTER:] [-e|-c]
```

1.7.4 Update Sequence Number (usn)

show Update Sequence Number in realtime

```
rtcmd usn DRIVE [SECONDS|off]
```

1.7.5 Usb Info (usb)

show properties for USB devices

```
rtcmd usb
```

1.7.6 Unlock (unlock)

verify BitLocker status and unlock

```
rtcmd unlock [LETTER:]
```

1.7.7 Security Data (sdat)

verify or optimise security database

```
rtcmd sdat DRIVE [commit|list]
```

1.7.8 NVMe Selftest (selftest)

run a NVMe Selftest or show previous results

```
rtcmd selftest [-l] [-e] #NUMBER
```

1.8 Registry

1.8.1 Registry Show (rs)

show content of registry.

```
rtcmd rs [-BINARYLINES] [user|sam|security|software|system|components|bcd00000000]
```

1.8.2 Registry Export (re)

export registry into hives

```
rtcmd re [user|sam|security|software|system|components|bcd00000000]
```

1.8.3 Registry Compare (rc)

compare previosly exported registry with current

```
rtcmd rc [-BINARYLINES] [user|sam|security|software|system|components|bcd00000000]
```

1.8.4 Hive Show (hs)

show content of a hive.

```
rtcmd hs [-BINARYLINES] HIVE
```

1.8.5 Hive Compare (hc)

compare two hives

```
rtcmd hc [-BINARYLINES] HIVE1 HIVE2
```

1.8.6 Delete Key (delkey)

delete a registry key

```
rtcmd delkey HKLM\KEY|HKCU\KEY
```

1.9 Services

1.9.1 Start Service (start)

send the start command to a service and wait until it has started

```
rtcmd start SERVICE
```

1.9.2 Stop Service (stop)

send the stop command to a service and wait until it has stopped

```
rtcmd stop SERVICE
```

1.9.3 Disable Service (disabled)

disable a service or list disabled services

```
rtcmd disabled [SERVICE],[DUMMY],...
```

1.9.4 Auto Start Service (auto)

set a service to auto start or list auto start services

```
rtcmd auto [SERVICE],[DUMMY],...
```

1.9.5 Delayed Auto Start Service (delayed)

set a service to delayed or list delayed services

```
rtcmd delayed [SERVICE],[DUMMY],...
```

1.9.6 Start Service on demand (demand)

set a service to start on demand or list start on demand services

```
rtcmd demand [SERVICE],[DUMMY],...
```

1.9.7 Early Launch (early)

manage early launch drivers

```
rtcmd early [off|on]
```

1.10 Scripting

1.10.1 Sleep (sleep)

delay script for SLEEPTIME seconds

```
rtcmd sleep SLEEPTIME
```

1.10.2 Message (mb_ok)

display message box with OK

```
rtcmd mb_ok MESSAGE [HEADER] [ICON]
```

1.10.3 Warning (mb_yes)

display message box with yes (EXIT 0)

```
rtcmd mb_yes QUESTION [HEADER] [ICON]
```

1.10.4 Question (mb_yesno)

display message box with yes (EXIT 0) and no (EXIT 2)

```
rtcmd mb_yesno QUESTION [HEADER] [ICON]
```

1.10.5 Zip Password (zippwd)

Encrypts a Zip password and strores it inside a user's account.

```
rtcmd zippwd SLOT [PASSWORD]|clear
```

2: c_e.exe

Front-End Windows® application.

2.1 Console

c_e can execute applications locally or remotely.

A command line application logs to RT_LOG or RT_ERROR, dependig on EXIT.

```
c_e [-OPT] [CREDENTIALS] [(D,T)SCHEDULE] [PATH\] [PROGRAM] [PARAM] ...
```

Stubes with the same behaviour like c_e.exe can execute with administrative rights on various accounts:

	User	Administrator with UAC	True Administrative Account
c_e			x
c_u		x	x
c_a	x	x	x

Start notepad with administrative rights:

```
c_a -x notepad
```

2.1.1 OPT

Console options, a combination of the following characters:

x Execute	Run PROGRAM with all PARAMs in the c_e Console window. Without PROGRAM 'ComSpec' will be started.
h Hidden	Run PROGRAM without visible window. This parameter cannot be used together with x.
c Clean	Do not show PARAMs in the console window's title bar or in a message box. Use this option to hide passwords specified in the command line.
e Exit	Quits a running program without warning if the user logged off or closed the window.
g Go standby	This computer will go into standby after the program exits with SUCCESS or if no PROGRAM has been specified.

l Logoff	The user account will be loged off after the program exits with SUCCESS or if no PROGRAM has been specified.	
s reStart	The computer will restart after the program exits with SUCCESS or if no PROGRAM has been specified. The restart will be delayed for 60 seconds on a remoted machine.	
t Terminate	The computer will shut down after the program exits with SUCCESS or if no FILE has been specified. The restart will be delayed for 60 seconds on a remoted machine.	
	-x Visible Run	**-h Hidden Run**
default	The window will be closed on SUCCESS. Reuschtoos Setup sets this behaviour for .bat scripts.	A message box will appear on ERROR.
i Integrate	The window will be closed on SUCCESS and on ERROR.	No message box will appear.
p Pause	The window will be keeped open on SUCCESS and on ERROR. Reuschtoos Setup sets this behaviour for .cmd scripts.	A message box will appear on SUCCESS and on ERROR.

Run the dir command with cmd.exe in a visible Console window. The window will not be closed, even if the command returns zero:

```
c_e -xp cmd /c dir
```

Restart this machine:

```
c_e -hs
```

2.1.2 CREDENTIALS

Run a program inside a user account or on another computer in the network.

`\\[MACHINE]:[USER]:[PASSWORD]`

- -x is obviously if you apply CREDENTIALS
- Firewalls can considarably slow down the handshake.
- The communication with another computer and the communication with the System Account is encrypted with DES 2048 and AES 256.

There are 2 ways to use the remote function:

1. Either, you will need full administrative rights without UAC on the target computer. ADMIN$ and IPC$ must be shared.
2. Or, Reuschtools FileProtection must be installed on the target computer with the same version you use here.

Sign into Ben's account on PC2 and start the command-line interpreter:

```
c_e \\PC2:Ben
```

Start the Install Restore dialog for PC2 with Ben's account and list all matching System Image Backups on PC2:

```
c_e \\PC2:Ben rtcmd ir -o s=*HD\*ARCH\*
```

Without MACHINE the local machine will be selected:

```
c_e \\:ben
```

Without USER the System Account will be selected:

```
c_e \\
```

You will need a true administrative account without UAC on a target machine to sign into its System Account:

```
c_e \\PC2
```

Without a true administrative account it is not possible to get administrative rights or restore a target machine.

Exeption:

If you have set an autorecovery password on a target machine, every user who has an account on the target machine and who knows the password can start an autorecovery sequence:

```
c_e -xs \\PC2 rtcmd autorecovery
```

2.1.3 [D,T]SCHEDULE

Repeat function, starts a visible or invisible console every SCHEDULE seconds.

Repeat will be aborted if Exit is non-zero (ERROR).

SCHEDULE commands should be startet with a Logon Script or from the Run key of the Registry.

See Scripts\Backup\AutoBackupON.cmd and Scripts\UserAccount\Zeitsparkasse.cmd.

Backup MyItems every 4 working hours:

```
c_e -h 14400 rtcmd pb -i s=*DOCUMENTS\MyItems t=D:\*ARCH\*
```

D sets the maximum daily session time.

Shutdown Ben's computer after 4 hours of daily session time:

```
c_e -ht D14400
```

T accumulates a fixed daily session time.

Ben is eligible for 1 hour of daily session time. If he does not use the computer for one day, the saved session time will be avaliable the next day.

```
c_e -ht T3600
```

2.1.4 PATH

Sets the current directory for a script or program.

PATH can contain Path Wildcards.

PATH must end with a \.

This will list the documents directory of the current user.

```
c_e -xp *DOCUMENTS\ cmd /c dir
```

2.1.5 PARAM

Command line parameters.

PARAMs can be replaced at the start of c_e:

?xxxx?	Ask for a string.
??xxxx??	Ask for a password.
???xxxx???	Ask twice for a password and double check it.

This will as ask for a drive letter and start a backup of the Documents folder:

```
c_e -x rtcmd pb s=*documents t=?Drive Letter?:\*ARCH\*
```

2.2 Editor

c_e is an editor and monitor suitable for very large text and log files.

`c_e [-OPT] [PATH\] [FILE]`

2.2.1 OPT

b Binary	Opens FILE in binary format, all characters are displayed as hexadecimal numbers.
o OEM	Opens FILE with the OEM character set. The OEM character set is often used by command line programs and differs from the ANSI character set used by Windows® when it comes to umlauts.
r Read Only	FILE cannot be modified.
v View	Steadily rescans FILE to monitor it.

2.3 Tools

2.3.1 Start (*)

c_e * PROGRAM [PARAM] ..	Start PROGRAM and return imediately, equal to the Windows® *start* command.
c_u * PROGRAM [PARAM] ..	Start PROGRAM with administrative rights if the user is an administrator.
c_a * PROGRAM [PARAM] ..	Start PROGRAM with administrative rights.

2.3.2 Code Page Converter (-in, -out)

`c_e [-in=CP_IN] [-out=CP_OUT] FILE`

in	Load FILE into the editor and apply code page CP_IN. c_e usually automatically detects the correct code page. c_e preferes UTF8 if there are no umlauts in FILE.
out	If you specify CP_OUT, c_e will work as a hidden codepage converter.

CP can be any well known code page:

- utf8
- unicode
- oem
- mac
- ansi

Or any code page number your Windows® supports. You will find all available numbers in the c_e menu:

`Settings->Code Page`

Convert all .cpp files from C:\Source to Unicode and store them in the current directory with the same names:

```
for %d in (C:\Source\*.cpp) do c_e -out=unicode %d
```

Or within a script respectivly:

```
for %%d in (C:\Source\*.cpp) do c_e -out=unicode %%d
```

2.3.3 Shell Icons (-icons)

`c_e -icons`

will shows all icons and their corespondig ID numbers which are embeddet in c_e.exe and shell32.exe. The icon numbers can be used with:

- `rtcmd mb_ok MESSAGE [HEADER] [ICON]`
- `rtcmd mb_yes QUEST [HEADER] [ICON]`
- `rtcmd mb_yesno QUEST [HEADER] [ICON]`

```
rtcmd mb_yesno "Did you water the plants" "Dad" 42
```

To use an icon from c_e.exe the icon number be signed with -.

```
rtcmd mb_ok "You are late" "Mum" -175
```

Icon numbers can also be used to customise the context menu.

2.3.4 Screen Resolution (-zoom)

`c_e -zoom[+][-]`

Increase or decrease the screen resoulution.

2.3.5 Seal Open (-sopen)

`c_e -sopen FILE`

Open a transportible Zip with the Windows® Explorer.

```
c_e -sopen MyItems.seal
```

3: Appendix

3.1 Wildcards

3.1.1 File (*)

TIMESTAMP	pb, ib, RT_LOG, RT_ERROR
pb s=MyItems t=*	
pb s=MyItems t=220214_194843.zip	
ORIGIN	pr, ir
pr s=220214_194843.zip t=*	
pr s=220214_194843.zip t=C:\Users\Ben\Documents\MyItems	
list ALL, select LATEST	pr, ir
pr s=* t=MyItems	
pr s=220214_194843.zip t=MyItems	

But this cannot work:

```
pr s=* t=*
```

3.1.2 Drive (*HD,*RD,*CD,*NET)

***HD**	All accessible hard drives
***RD**	Removable drives, USB drives.
***CD**	CD drives.
***NET**	Net drives.

Drive Wildcards can resolve to multiple targets:

```
pb s=MyItems t=*HD\
pb s=MyItems t=C:\MyItems.zip t=D:\MyItems.zip
```

3.1.3 Path (*DOCUMENTS,..)

***documents**	C:\Users\Ben\Documents
***desktop**	C:\Users\Ben\Desktop
***downloads**	C:\Users\Ben\Download
***pictures**	C:\Users\Ben\Pictures
***music**	C:\Users\Ben\Music
***videos**	C:\Users\Ben\Videos
***user**	C:\Users\Ben
***profiles**	C:\Users
***alldoc**	C:\Users\Public\Documents

3.1.4 Match (*ROOT,*ARCH)

***ROOT**	Generates a path from the location of the source folder. This path will help to find all matching backups even if the Windows® machine or drive has changed.
pb s=C:\Users\Ben\Documents\MyItems t=D:*ROOT\	
pb s=C:\Users\Ben\Documents\MyItems t=D:\Ben\Documents\MyItems\MyItems.zip	
***ARCH**	Same as *ROOT but with *RtArch*\ as prefix. The Reuschtools Wizards use *ARCH as default.
pb s=C:\Users\Ben\Documents\MyItems t=D:*ARCH\	
pb s=C:\Users\Ben\Documents\MyItems t=D:\RtArch\Ben\Documents\MyItems\MyItems.zip	
pb s=C:\AllStuff t=D:*ARCH*	
pb s=C:\AllStuff t=D:\RtArch_PC1\DRIVE_C\AllStuff\220214_194843.zip	

3.1.4.1 Filter Prefix

A filter prefix together with *ROOT or *ARCH can extend the resulting list or selection for restore operations.

pr, source folder was inside a user profile	foreign user	foreign folder	all backups
pr, source folder was outside a user profile	foreign machine	foreign folder	all backups
Install Restore	foreign machine	foreign Windows® version	all backups

1	x		
2		x	
3	x	x	
4			x

This example assumes the current directory to be set to the user's Documents folder.

After work, Ben creates a backup of *Project* on cloud drive Z:

```
rtcmd pb s=Project t=Z:\*ARCH\
rtcmd pb s=Project t=Z:\RtArch\Ben\Documents\Project\Project.zip
```

The next day, Mary restores *Project* to continue working:

```
rtcmd pr t=Project s=Z:\*1ARCH\
rtcmd pr t=Project s=Z:\Ben\Documents\Project\Project.zip
```

3.1.4.2 RT_LOG, RT_ERROR, RT_SCHEDULE

Replacement for *ROOT:

RT_LOG user	
visible (-x)	_LOG_\Console
hidden (-h)	_LOG_\Hidden
RT_LOG system	
visible (-x)	%COMPUTERNAME%$_LOG_\Console
hidden (-h)	%COMPUTERNAME%$_LOG_\Hidden
RT_ERROR user	
visible (-x)	_ERROR_\Console
hidden (-h)	_ERROR_\Hidden
RT_ERROR system	
visible (-x)	%COMPUTERNAME%$_ERROR_\Console
hidden (-h)	%COMPUTERNAME%$_ERROR_\Hidden

3.2 Word explanations

3.2.1 Access-control list (ACL)

On NTFS drives, a list with the following information is appended to each folder and file:

- Who can read or change a file (Discretionary Access Control List).
- Should be monitored, who has read or changed a file and when (System Access Control List).

Install-Backup will always store acls in the backup. Private Backup can optionally store acls in the generated Zip.

Access-control list on Wikipedia

3.2.2 Data Folder

Data Folders are special folders for each PC user. Users should always store their data inside a Data Folder.

Documents	C:\Users\Ben\Documents
Desktop	C:\Users\Ben\Desktop
Downloads	C:\Users\Ben\Download
Pictures	C:\Users\Ben\Pictures
Music	C:\Users\Ben\Music
Videos	C:\Users\Ben\Videos

3.2.3 EFS Encryption

EFS (Encrypting File System) stores all data securely encrypted on a hard disk or USB Stick.

It is transparently. This means that a user does not have to enter a passwort. A user will only remark a lock sign on the icon of a encrypted folder or file.

The encryption key is stored inside a users account. It can only be accessed when the user is signed in.

A thief who steals a harddisk or someone who unintentionally finds a lost USB stick, will newer be able to read data as long as he does not know the user's account password.

EFS is delivered with all Windows® professional versions. A user can read EFS encrypted files on Windows® home versions but writing is restricted.

Compared to Bitlocker EFS has the following advantages:

- No password required on startup.
- Each user has his own key. Even an administrator will not be able to read encrypted data.
- Multible trusted users can be linked to an encrypted folder or file. Each project can have individual trustees.
- The same encryption key can be installed on multible PCs. A user can change the desk but has the same access to his encrypted data.
- A EFS encrypted folder can securely be transported across unsecure channels (.seal file).

EFS on Wikipedia

3.2.4 Exit

Return code.

Each program or script returns a number when finished. The programmer decides which number to return.

Zero usually marks success.

End the command line or script and return 99:

```
exit 99
```

3.2.5 Hardlinks

are files that exist once on a hard disk but show up several times at different places.

A user does not recognise a hardlink.

List Hardlinks and Reparse Points on drive C:

```
rtcmd list -h C:
```

Hardlinks on Wikipedia

3.2.6 Integration Number

	Error	Warning	Dialog
0			
1	x		
2		x	
3	x	x	
4			x
5	x		x
6		x	x
7	x	x	x

Show the dialog and an error message if an error appears.

But do not show an overwrite warning.

```
rtcmd pb -i5 s=*documents\MyItems t=C:\*ARCH\
```

3.2.7 Local Area Network

Local Area Network on Wikipedia

3.2.8 NTFS

NTFS (New Technology File System.) is a hard disk format used as standard since Windows® XP. Unlike FAT32(Windows® 98), NTFS supports Access-control lists.

If Reuschtools runs with administrative rights it can read the content table of NTFS drives and directly read data. This could speed up large backup or restore operations considerably.

NTFS on Wikipedia

3.2.9 Number Zip

.zip or .seal file who's name begins with a number and not with a character.

This is typical the case with time stamped Zips:

```
220127_224242.zip
```

Number Zips can easily be recycled with Target Options parameters.

3.2.10 RAW Data (.seal)

RAW data is the EFS encrypted data that is actually stored on the harddisk.

A legitimate user is not in touch with RAW data, because all files are automatically decrypted by EFS as soon as they are read from the drive.

A backup administrator however, who has no encryption key for a file can read RAW data directly from the harddisk.

A user without administrative can read his own RAW data.

A transportible Zip (.seal file) is nothing more but the RAW data of an EFS encrypted Zip.

Warning!, never create a Zip file with the Windows® explorer if you have EFS encrypded data. Windows® decryps the files and stores them without encryption in the Zip.

If you create a Zip file (.zip) with Reuschtools, all EFS encryped files are assured to be stored as RAW data. You can open such a Zip with the Windows® explorer. But you will only see garbitch if you try to read a previosly EFS encrypted file.

Because RAW data is arbitrary (pseudo random) it does not contain redundancy which could be compressed. This is why a Reuschtools Zip created from an EFS encrypted folder will usually have the doubled size compared to a Zip that is EFS encrypted after compression (.seal file).

3.2.11 Reparsepoint

are fake folders or fake drives.

If you open a reparsepoint, you will end up in a folder or drive that could even be on another PC.

Typical reparsepoints are drive letters assigned to a network folder.

Reparsepoint on Wikipedia

3.2.12 RT_LOG, RT_ERROR, RT_SCHEDULE

Environment variables to control Reuschtools' log behaviour. If not set, the default will be used:

User Account	tf30=%LOCALAPPDATA%\RtLog*ROOT*
System Account	tf30=%SystemDrive%*ARCH*

See Private Backup for the syntax . More informationen in Section 3.1.4.2.

Characters used in logfiles:

+	add opject	**-**	remove object	*****	update oject
~	short filename	**e**	encrypt	**d**	decrypt
#	database update	**h**	hidden compress	**a**	access control list
p	file attribute	**c**	large and lower case	**l**	link
r	reparse content	**j**	reparse point	**b**	binary check
B	binary check positiv	**.**	pending object	**$**	data stream
:	stream removed	**;**	run on restart	**,**	run on sign in

3.2.13 System Image

InstallBackup creates a set of Zip files inside a directory that is ending with .ib.

This directory holds all information required to restore Windows®, settings, software and passwords on a blanc hard disc.

The directory contains the program itself that is required to do a restore operation (InstallRestore).

A System Image does not include the content of each user's Data Folders.

3.2.14 Template

Reuschtools uses previosly created backups:

- Consulting the log file, a user can check which objects have been modified.
- Backup and restore operations considerably run faster.

3.2.15 Volume Shadow Copy Service (VSS)

is part of all Windows® operating systems.

It helps backup applications to copy data even if a file or a database is currently in use.

3.2.16 Windows® Boot Manager

The Windows® Boot Manager appears when the computer is restarted. It allows the user to select a Windows® operating system or a recovery environment. The defaulted selection will usually be started within 3 seconds, if the user does not change it.

Windows® Boot Manager on Wikipedia

3.2.17 Zip Encryption

Reuschtools supports the original Zip encryption (ZipCrypto). This means that encrypted Zips can be decrypted by almost all Zip readers.

ZipCrypto was released in 1989 and has been criticized often since then:

- A Known Plaintext Attack on the PKZIP Stream Cipher, Eli Biham, and Paul C. Kocher
- ZIP Attacks with Reduced Known Plaintext, Michael Stay

Zip encryption has often been poorly implemented. This has historical reasons. The export of strong, actually working encryption from the USA has not been allowed for a long time.

Reuschtools uses additional security mechanisms to make ZipCrypto secure:

- True random numbers are used instead of pseudo-random numbers.
- If Zip encryption is used, the code tables (Huffman Codes) are scrambled, which prevents the "plaintext attack" mentioned above.

There are various commercial programs for cracking encrypted zip archives (e.g. Advanced Archive Password Recovery, (www.elcomsoft.com). These programs demonstrate that the Zip encryption used by Reuschtools is secure, provided a strong password (>12 random digits) is used.

3.2.18 Zip File

The Zip file format is industry standard for backup applications.

It is used to compress, encrypt and store the content of a folder or drive in only one file.

- Each file in a Zip is independently compressed and can therefore be easily and fast found and extracted.
- The Zip file format is extensible. Reuschtools stores many file properties and information in a Zip without loosing comptibility with common Zip readers.

Zip file on Wikipedia

3.2.19 Zip Password Slot

If a user enables Zip encryption he is asked for a password before the backup will start.

A user can opt for 'Remember this password.'

In this case Reuschtools creates a RSA 4096 certificate inside a user's Windows® account. This certificate is used to encrypt the password before it is stored inside the Windows® registry.

A thief who steals your PC or hard disk will never be able to decrypt your passwords without knowing your Windows® account's password.

Depending on the dialog window, the password will be stored inside a different registry slot:

Dialog	Slot

PrivateBackup	**pb**
PrivateRestore	**pr**
InstallBackup	**ib**
InstallRestore	**ir**

The remembered passwords can be passed on the command line by specifying the registry slot. This avoids plaintext passwords in scripts or the command line.

The command zippwd can be used to store encrypted Zip passwords without starting a backup or restore dialog.

3.3 Important Information

3.3.1 Credits

- Info-ZIP
- NSIS
- NSIS Modern User Interface 2
- Code-Projekt
- Sys-Internals
- Boost
- Python
- SCons
- Halibut

3.3.2 Brands and Trademarks

Brand names and trademarks in this manual are the property of their respective owners and are used for descriptive purposes only.

This manual or it's content can be freely distributed.