Reset Windows Password

USER MANUAL

Passcape Software

Introduction

1 Introduction

1.1 About the program

Reset Windows Password was developed for resetting, changing and recovering Windows logon passwords. For example, when the computer Administrator's password is lost or forgotten. Reset Windows Password is the most optimal and functionally richest solution in its class. The application supports all versions of Windows (based on NT), works with Active Directory and domain cached credentials, possesses artificial intelligence skills for recovering passwords instantly to certain accounts and demonstrates a number of additional unique features. It also includes a widest range of forensic and data analysis tools.

The interface of the application is traditionally carried out in the form of a step-by-step wizard. Therefore, the operation process does not seem complicated to even an inexperienced user. For example, resetting an administrator password takes just three simple steps:

1. Select the SAM and SYSTEM files (the application automatically searches all hard drives for the registry files.)
2. Select the user account.
3. Reset or modify the password.

Using a built-in utility, you can easily create a bootable CD, DVD or USB disk (including devices like Compact Flash, SmartMedia, SONY Memory Stick, Secure Digital, ZIP drives, USB Hard Disk drives, etc.) within a few minutes, from an existing ISO image with the program. Reset Windows Password has a graphic user interface, supports loading IDE, SATA, SCSI, RAID volumes on the fly, is compatible with FAT, FAT32, NTFS, NTFS5, ReFS file systems, goes with a large collection of hard disk drivers from Highpoint, Intel, Jmicron, Marvell, Nvidia, Silicion Image, Sis, Uli, Via, Vmware.

1.2 Features and benefits

Application's advantages:

- Support for all versions of NT-based Windows.
- Support for 32/64-bit Windows.
- Large collection of hard disk drivers. Loads additional drivers from the application.
- Reset and modify passwords of local and domain users, local administrator, domain administrator, other Active Directory accounts.
- Enable and unlock user accounts, both local and domain administrators.
- Disable password expiry options.
- Detect several operating systems.
- Support for non-English versions of Windows and passwords in national encoding.
- Dump user password hashes from SAM for further analysis.
- Dump password hashes from Active Directory.
- Dump domain cached passwords.
- Several modules to extract and decrypt Active Directory plain-text passwords.
- Allow undoing changes made to the system.
- Delete passwords and other sensitive data from PC.
- Advanced password search and recovery algorithms.
- Reset SYSKEY security.
- SYSKEY startup password recovery.
- Search for lost serial keys.
- Search for network passwords.

- Search for virtual machine passwords.
- Backup registry/Active Directory and other sensitive information.
- Unlock Bitlocker drives.
- A lot of forensic tools such as logon statistics, hardware, software, network, browsing, clipboard and USB history, user activity, system events, hardware access tracking, activity timeline, Windows media forensic tools, system resource usage monitor, Windows Search explorer, etc.
- Miscellaneous file utilities.
- Password search and recovery for MS Office, OpenOffice, LibreOffice, MyOffice, and PDF documents.
- Edit local or domain password policy, as well as system and interface restrictions.

The software is available in three editions: **Light**, **Standard** and **Advanced**. The detailed list of features for each edition is available here.

1.3 System Requirements

Requirements
x64-based microprocessor, a minimum of 1 GB of RAM, CD-ROM or USB drive. The size of the bootable USB drive should be 512 Mb or bigger (it is recommended 2-32 Gb USB stick for better compatibility). Computer BIOS must support booting from CD, DVD or USB device.

Compatibility
Windows NT or newer OS, Windows Server 2000 or newer. File systems: FAT, FAT32, exFAT, NTFS, ReFS. The program is compatible with the majority of CD/DVD recorders and USB devices, including Memory Stick, Compact Flash, SmartMedia, Secure Digital, USB flash drives, USB ZIP drives, USB Hard Disk drives, etc.

Restrictions
Once your system uses a non-standard mass storage device, you may need to specify a 3d-party driver compatible with Windows 10-11. Please refer to your motherboard manual for the details.

Known issues or bugs

- If you have 2 or more logical disks in your system, the disks letters may be reassigned/reodered.
- If you are resetting a password of the built-in Administrator account in some editions of Windows, please keep in mind that in order to activate the built-in Administrator account and log on the system, you will need to load the system in the safe mode.
- The program supports all types of SYSKEY encryption. In some cases you may need to provide the SYSKEY startup password or startup diskette. However the program also allows to reset/lookup SYSKEY password. So even if you forgot your SYSKEY, it's not a problem.
- After you reset the password of a local account, you may lose access to your Web page passwords, wireless network and file share credentials, EFS-encrypted files, e-mail messages encrypted with private keys. Please refer to Microsoft Knowledgebase for further details.
- Resetting Active Directory passwords for certain accounts may have no effect. For example, on a RODC.
- Password reset (as well as other features that imply disk-write operations) on a virtual OS will have no effect.
- When resetting a password for Microsoft Account, you should provide a non-empty password. Otherwise you will not be able to log on the system.

Creating bootable environment

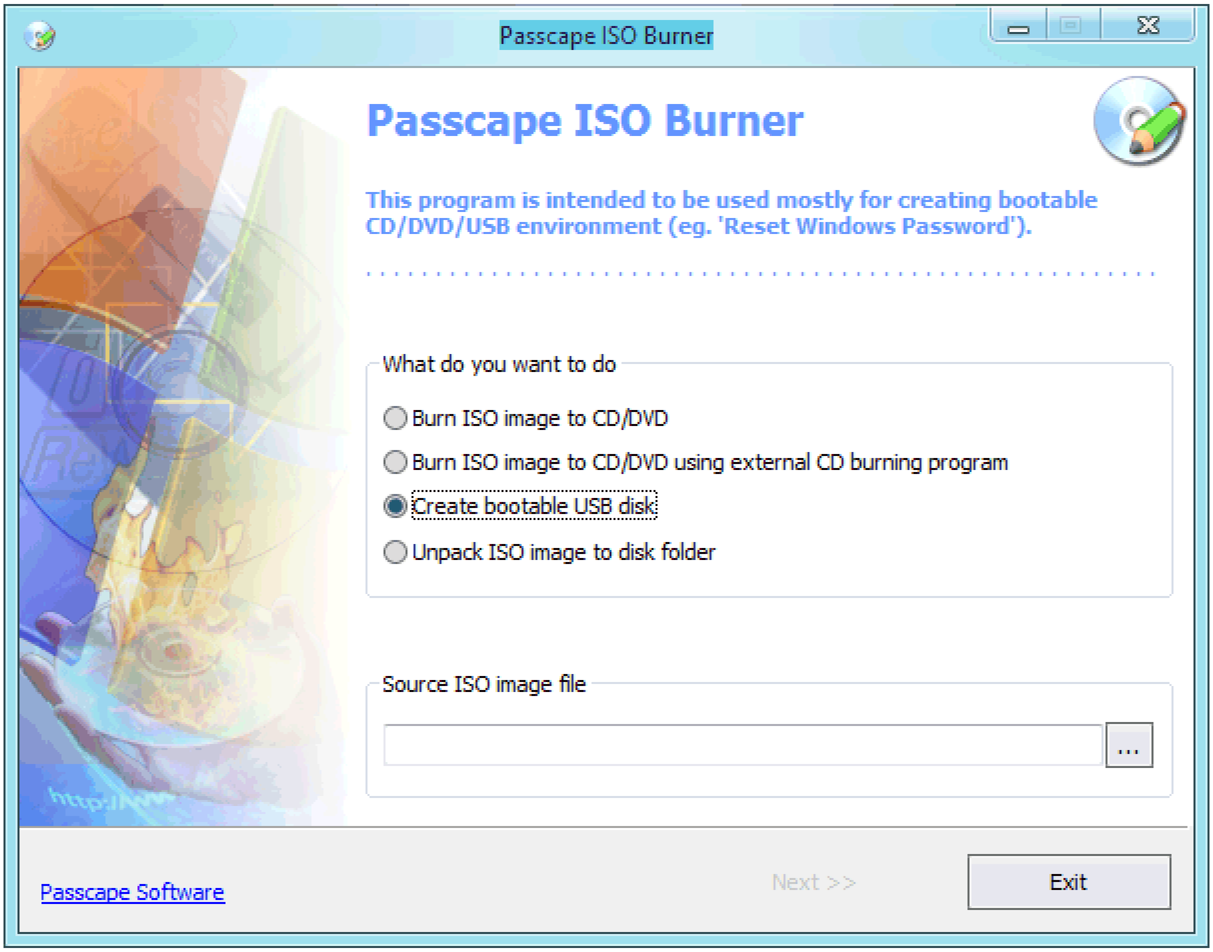
2 Creating bootable environment

2.1 3 simple steps to launching the application from a boot disk

1. Download Reset Windows Password package at https://www.passcape.com/download/rwp.zip (or using the link that was sent to you in the registration e-mail)
2. Create RWP boot disk: unpack the RWP.ZIP file, run IsoBurner.exe, select an item for creating bootable CD/DVD/USB, specify the path to the unpacked ISO image and write it to the disk.
3. Start the target computer and change its BIOS/UEFI settings to make the boot device (CD-ROM, DVD-ROM or USB disk) first on the list. Save the settings, reboot once again to start the program off your bootable CD, DVD or USB disk. You can use fast boot option if your BIOS/UEFI supports fast boot media selection during startup.

2.2 Creating RWP boot disk

Passcape ISO Burner



Passcape ISO Burner

This program is intended to be used mostly for creating bootable CD/DVD/USB environment (eg. 'Reset Windows Password').

What do you want to do

○ Burn ISO image to CD/DVD

○ Burn ISO image to CD/DVD using external CD burning program

● Create bootable USB disk

○ Unpack ISO image to disk folder

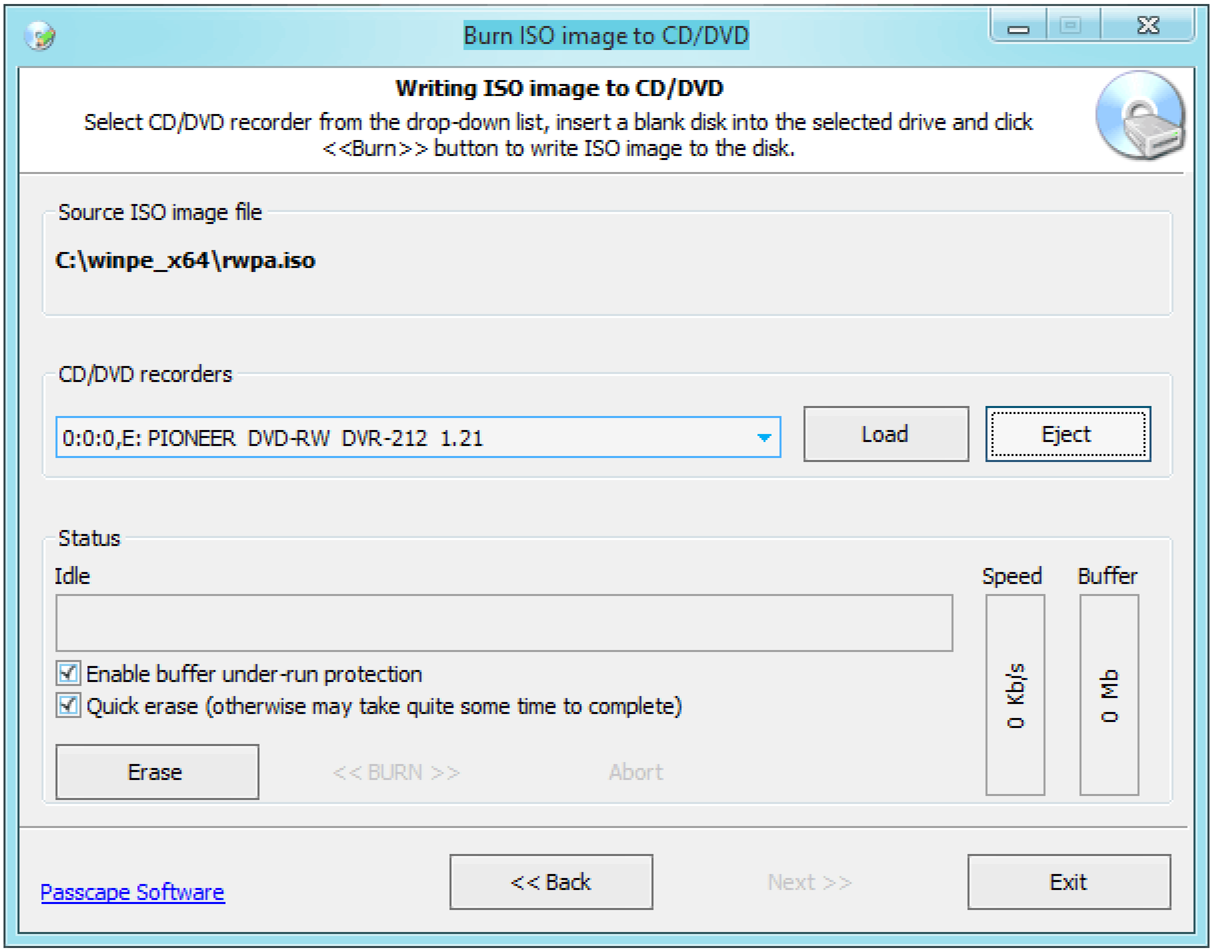
Source ISO image file

Passcape ISO Burner is a program for creating bootable CD, DVD or USB disks from ISO-9660 images. The program is free and comes with RWP. it is also available for downloading and using at our website:

https://www.passcape.com/download/pib.zip

The application’s interface is ultimate-simple. When started, the application asks you to select what you would like to do:
- Record ISO image to CD/DVD using this application
- Record ISO image to CD/DVD using an external burning application installed on your computer. For example, Nero or its free analog ImgBurn.
- Use ISO image to create a USB boot disk
- Extract ISO image to disk (keep in mind that this action causes the loss of boot data).

Creating Reset Windows Password bootable CD



Burn ISO image to CD/DVD

Writing ISO image to CD/DVD

Select CD/DVD recorder from the drop-down list, insert a blank disk into the selected drive and click <<Burn>> button to write ISO image to the disk.

Source ISO image file

C:\winpe_x64\rwpa.iso

CD/DVD recorders

0:0:0,E: PIONEER DVD-RW DVR-212 1.21

Status

Idle

Speed: 0 Kb/s

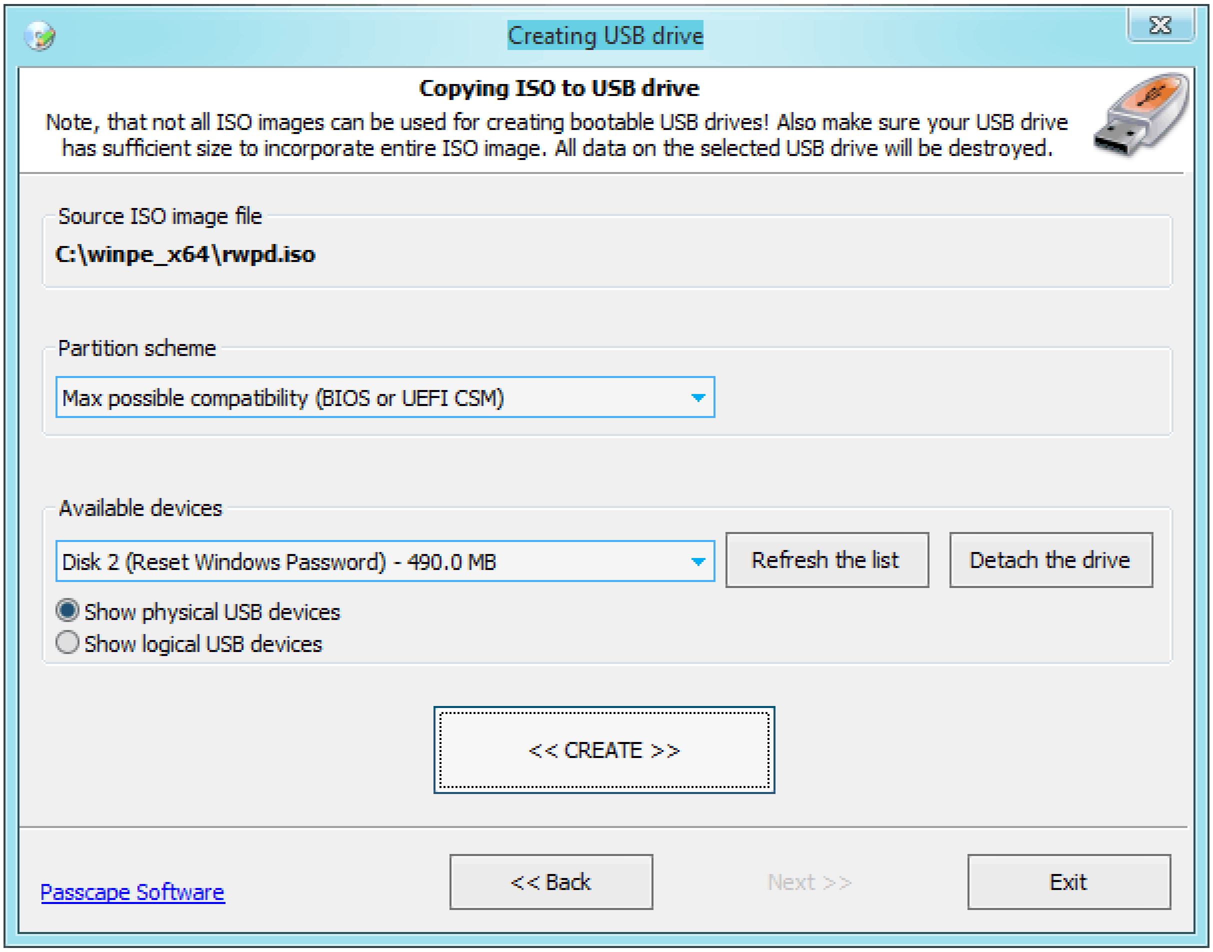
Buffer: 0 Mb

☑ Enable buffer under-run protection

☑ Quick erase (otherwise may take quite some time to complete)

Select the first menu item: '*Burn ISO image to CD/DVD*'. At the bottom of the screen, enter path to the file with the ISO image. That enables the '*Next*' button, and you can move on to actually creating the disk. All we need to do here is select the recorder we are going to use, insert a blank CD/DVD in it and click on the <<BURN>> button to create a boot disk from the ISO image selected on the previous step.

Creating Reset Windows Password bootable USB



Creating USB drive

Copying ISO to USB drive

Note, that not all ISO images can be used for creating bootable USB drives! Also make sure your USB drive has sufficient size to incorporate entire ISO image. All data on the selected USB drive will be destroyed.

Source ISO image file

C:\winpe_x64\rwpd.iso

Partition scheme

Max possible compatibility (BIOS or UEFI CSM)

Available devices

Disk 2 (Reset Windows Password) - 490.0 MB

● Show physical USB devices

○ Show logical USB devices

Select the existing bootable ISO image with the program and set the '*Create bootable USB disk*' option on. Enter the product serial number if you have one. When the next window appears, plug the USB device to your computer; it should automatically appear on the list of found USB devices. Click on the '*Create*' button to format and create the boot USB. In some cases (for example, if the USB device is installed as a hard disk drive, and an extended partition entry is found on that disk) the application will require restarting for reassigning drive letters.

The program offers several partition schemes (formatting modes) to supply better compatibility when booting from USB devices. If you feel uncertain about what partition scheme to select, consider using the following simple algorithm:
- If the target PC is based on UEFI (graphical) interface, select 'Max compatibility with new PCs (FAT32 MBR for UEFI)' mode. This scheme will create a USB to be run on UEFI-based PCs where secure boot mode is turned on.
- If your target PC is based on BIOS (textual) interface, select 'Max compatibility with old PCs (FAT32 MBR for BIOS)' mode. This mode will create a USB that is fully compatible with BIOS firmware.
- If you know nothing about target PC, switch to 'Max possible compatibility' scheme. This mode creates bootable USBs that can run on both BIOS- and UEFI-based computers (with **Compatibility Support Mode** is turned on). On some PCs or laptops the Compatibility Support Mode is also known as **Legacy Boot Mode**.

If you bought your PC after 2010, most likely, it comes with UEFI. New computers use UEFI firmware instead of the traditional BIOS. Both are low-level software that starts when you boot your PC and are used to 'communicate' with hardware. Unlike BIOS, UEFI is a more modern solution with graphic interface, supporting larger hard drives, faster boot times and more security features.

Be careful! All data on the target drive will be overwritten. If the application is unable to detect boot files in the source ISO image, it will show the respective warning.

Some AntiVirus/AntiMalware software block creating bootable disks or copying some boot files to media even without onscreen warnings!

2.3 Changing BIOS/UEFI settings

General information

In order to load Reset Windows Password, you may need to adjust your computer's BIOS/UEFI settings to make the boot device (CD, DVD, or USB) first on the list of devices. This is the routine to follow for that:

1. When booting the computer, press the **Del** key to enter the BIOS menu. Some versions of BIOS use other hotkeys; those could be **F2**, **F10**, **F11**, **ESC**, etc. The hint is normally displayed at the bottom of the boot screen.
2. Enter the BIOS/UEFI, then on the menu find the item that's in charge of the initial boot devices. Edit it to make the CD or USB with the Reset Windows Password first on the list.
3. Make sure to have saved the changes and then reboot the computer.

If your PC uses UEFI firmware, you can use fast boot selection switch without altering any settings. For more information, please refer to your computer's motherboard user manual.

Setting up BIOS, questions and answers

Q: My computer's BIOS has several items for booting from USB devices: USB FDD, USB ZIP, USB HDD, USB CDROM. Which one should be selected?
A: Different BIOS manufacturers set up the initial boot different ways. In the majority of cases, to boot from a regular flash: on old motherboards you would need to select the USB ZIP option; on some other ones - USB HDD.

Q: The application takes too long (sometimes up to 10 minutes) to boot from USB media.
A: That indicates that the device runs over the slow USB protocol, 1.1. First, the storage device must support the 2.0+ specification. Second, the USB port in the motherboard where you plug the storage device must support the 2.0+ specification. And third, you must enable the USB 2.0 (or higher) support in the BIOS.

Q: The computer wouldn't boot from USB devices at all. When attempting to boot – either black screen or the '*no operating system*' error message.
A: Try finding the '*Legacy USB storage detect*' option and make it '*Enabled*'. In the boot options, you should have only one USB device. If you have two or more USB devices plugged to the computer (eg. UPS, printer, scanner, modem, etc.), leave only one bootable USB disk. Unplug the USB device from the computer, turn the computer off, plug the USB device to a different USB port, turn your computer on and attempt to boot again. If that didn't help – update your BIOS. Also there is a chance that your motherboard doesn't support booting from USB devices or doesn't support the file system used on this USB storage device.

Q: Blue or black screen, all kinds of driver, registry load, etc. errors occur when booting from CD or USB.
A: Maybe your computer does not have sufficient memory. The minimum required by the application is 1 GB RAM. To run it with comfort, you would need 2 GB or more.

Q: Can't get into my BIOS. A password is required.
A: An unpleasant surprise can watch for you when you try to modify the boot device settings in BIOS. The matter is that some hardware manufacturers, sellers or previous owners of the PC may have set their own passwords for accessing BIOS. In other words, in order to modify BIOS settings, you would need to enter that password, which usually is not possible to find out.
Some versions of BIOS allow resetting their settings by pressing a certain key on the keyboard; normally that's

Ins. For some type of AMI BIOS it is a **Ctrl+Alt+Del+Ins** combination. On AWARD BIOS, the key is to be pressed and held down until the computer is turned on. That will load the default settings. However, this option is to be used extremely carefully, as it resets all other settings of the BIOS.

Also, there are universal back-door passwords. They are provided below for many popular old versions of BIOS. If you don't know it, BIOS type and version is normally displayed for a few seconds during the initial boot of the computer at the bottom of the screen.

If none of the universal passwords has worked out, you can take advantage of the method described in many motherboard user manuals: simply reset BIOS settings by shorting the respective jumper. It is normally located near the large CMOS battery. If the motherboard doesn't have a CMOS battery, find the microchip with the Dallas or Odin marking; the jumper must be somewhere nearby. Simply removing the CMOS battery doesn't always help, as the BIOS microchip can live for several hours without the power. Also, you are highly discouraged from shorting the CMOS itself for resetting BIOS settings, as that may cut the battery life essentially.

On the Net, you can find a number of software solutions for recovering passwords and resetting BIOS. For example, cmospwd and killcmos. You are highly discouraged from resetting all BIOS settings in laptops. That may lead to the complete halt of the system.

Q: A error pops up which states that the CPU does not support 64-bit mode or running 64-bit applications.
A: Reset Windows Password does not support 32-bit CPUs any longer (but has support for 32-bit OSes though). Contact tech. support to get a link for the latest 32-bit compatible version.

Q: Can I boot a BIOS compatible CD/USB drive in UEFI?
A: Yes. Enter your UEFI settings (press ESC, F2 or DEL). Open 'Boot' menu and enable 'Launch CSM' option. Now locate 'Security' tab and disable 'Secure Boot Control'. Save changes and reset your PC. Enter the UEFI setup once again and make sure your DVD/USB drive is available under the 'Boot' tab. Some UEFIs also have a boot device menu (it is usually launch by hitting F8) where you can select your boot device and mode.

Q: Can I create a USB drive that will be able to boot in both BIOS and UEFI?
A: Yes. Run the IsoBurner tool and select 'Max possible compatibility' partition scheme when creating a bootable USB. This mode creates bootable USBs that can run on both BIOS- and UEFI-based computers (with Compatibility Support Mode is turned on). On some PCs or laptops the Compatibility Support Mode is also known as Legacy Boot Mode.

Q: USB is not listed as a boot option in my UEFI. How can I enable booting for a USB stick?
A: Seems that the USB was formatted either to BIOS or UEFI CSM mode but your UEFI allows booting in Secure Boot mode only. You will have to allow booting in legacy mode. In your UEFI settings disable both 'Boot - Fast Boot' and 'Security - Secure Boot' and enable 'Compatibility Support Mode (CSM)' or similarly worded options. Another workaround would be just creating a bootable USB using 'Max compatibility with new PCs (FAT32 MBR for UEFI)' scheme. This scheme is fully compatible with UEFI Secure Boot mode.

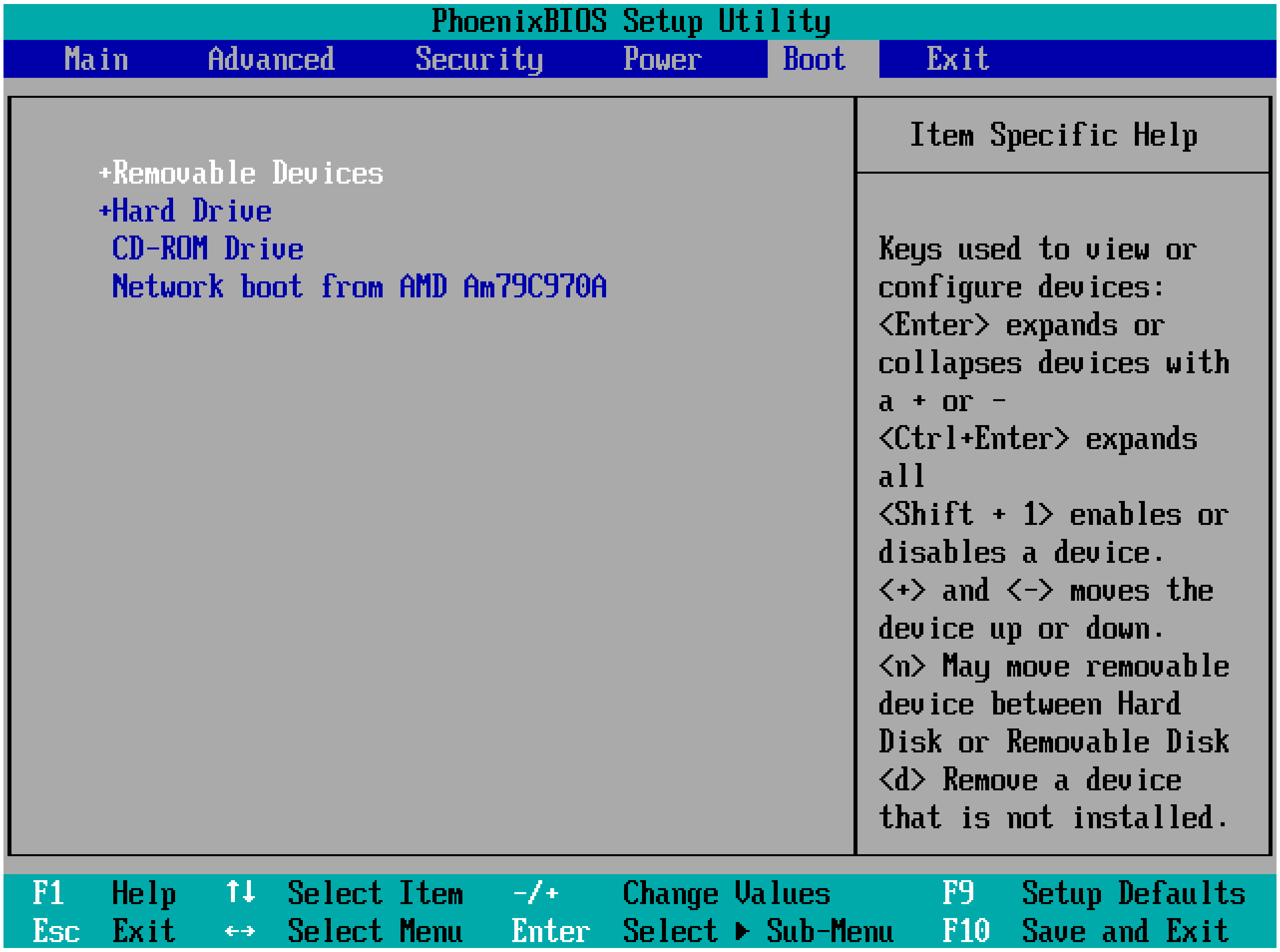
Back-door BIOS passwords

BIOS manufacture	Universal password
AWARD BIOS 2.50	AWARD_SW, 01322222, j262, TTPTHA, KDD, ZBAAACA, aPAf, lkwpeter, t0ch88, t0ch20x, h6BB
AWARD BIOS 2.51	AWARD_WG, HLT, BIOSTAR, SWITCHES_SW, 256256, j256, ZAAADA, Syxz, ?award, alfarome, Sxyz, SZXY
AWARD BIOS 2.51G	HEWITTRAND, HLT, biostar, HELGA-S, bios*, g6PG, j322, ZJAAADC, Wodj, h6BB, t0ch88, zjaaadc

AWARD BIOS 2.51U	condo, biostar, CONDO, CONCAT, 1EAAh, djonet, efmukl, g6PG, j09F, j64, zbaaaca
AWARD BIOS 4.5	AWARD_SW, AWARD_PW, PASSWORD, SKYFOX, award.sw, AWARD?SW, award_?, award_pc, ZAAADA, 589589
AWARD BIOS 6.0	AWARD_SW, HLT, KDD, ?award, lkwpeter, Wodj, aPAf, j262, Syxz, ZJAADC, j322, TTPTHA, six spaces, nine spaces, 01355555, ZAAADA
AMI BIOS	AMI, SER, A.M.I., AMI!SW, AMIPSWD, BIOSPASS, aammii, AMI.KEY, amipswd, CMOSPWD, ami.kez, AMI?SW, helgaЯs, HEWITT RAND, ami', AMISETUP, bios310, KILLCMOS, amiami, AMI~, amidecod
AMPTON BIOS	Polrty
AST BIOS	SnuFG5
BIOSTAR BIOS	Biostar, Q54arwms
COMPAQ BIOS	Compaq
CONCORD BIOS	last
CTX International BIOS	CTX_123
CyberMax BIOS	Congress
Daewoo BIOS	Daewuu, Daewoo
Daytec BIOS	Daytec
DELL BIOS	Dell
Digital Equipment BIOS	komprie
Enox BIOS	xo11nE
Epox BIOS	Central
Freetech BIOS	Posterie
HP Vectra BIOS	hewlpack
IMB BIOS	IBM, MBIUO, sertafu
Iwill BIOS	iwill
JetWay BIOS	spooml
Joss Technology BIOS	57gbz6, technology
M Technology BIOS	mMmM
MachSpeed BIOS	sp99dd

Magic-Pro BIOS	prost
Megastar BIOS	star, sldkj754, xyzall
Micronics BIOS	dn_04rjc
Nimble BIOS	xdfk9874t3
Packard Bell BIOS	bell9
QDI BIOS	QDI
Quantex BIOS	teX1, xljlbj
Research BIOS	Col2ogro2
Shuttle BIOS	Col2ogro2
Siemens Nixdorf BIOS	SKY_FOX
SpeedEasy BIOS	lesarot1
SuperMicro BIOS	ksdjfg934t
Tinys BIOS	tiny, tinys
TMC BIOS	BIGO
Toshiba BIOS	Toshiba, 24Banc81, toshy99
Vextrec Technology BIOS	Vextrex
Vobis BIOS	merlin
WIMBIOS v.2.10 BIOS	Compleri
Zenith BIOS	3098z, Zenith
ZEOS BIOS	zeosx

2.4 Running the program from the bootable CD/DVD/USB

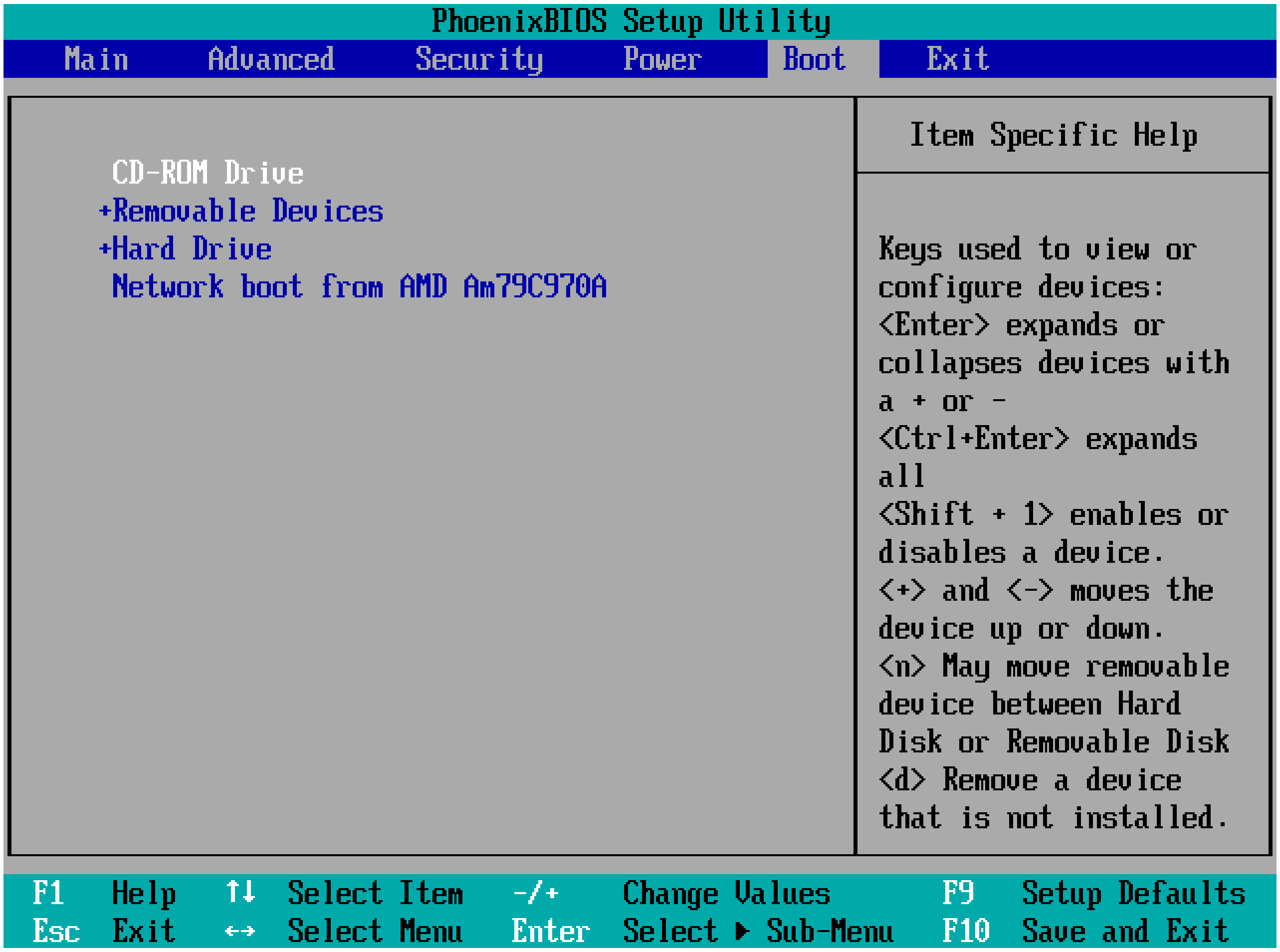


```
                      PhoenixBIOS Setup Utility
   Main    Advanced    Security    Power    Boot    Exit

                                          |  Item Specific Help
     +Removable Devices                   |
     +Hard Drive                          |
      CD-ROM Drive                        | Keys used to view or
      Network boot from AMD Am79C970A     | configure devices:
                                          | <Enter> expands or
                                          | collapses devices with
                                          | a + or -
                                          | <Ctrl+Enter> expands
                                          | all
                                          | <Shift + 1> enables or
                                          | disables a device.
                                          | <+> and <-> moves the
                                          | device up or down.
                                          | <n> May move removable
                                          | device between Hard
                                          | Disk or Removable Disk
                                          | <d> Remove a device
                                          | that is not installed.

 F1   Help   ↑↓  Select Item   -/+     Change Values       F9   Setup Defaults
 Esc  Exit   ↔   Select Menu   Enter   Select ▸ Sub-Menu   F10  Save and Exit
```

Turn on your computer. Press the Del key to enter the BIOS menu. Some versions of BIOS use other hotkeys; those could be F2, F10, F11, ESC, etc. The hint is normally displayed at the bottom of the boot screen.



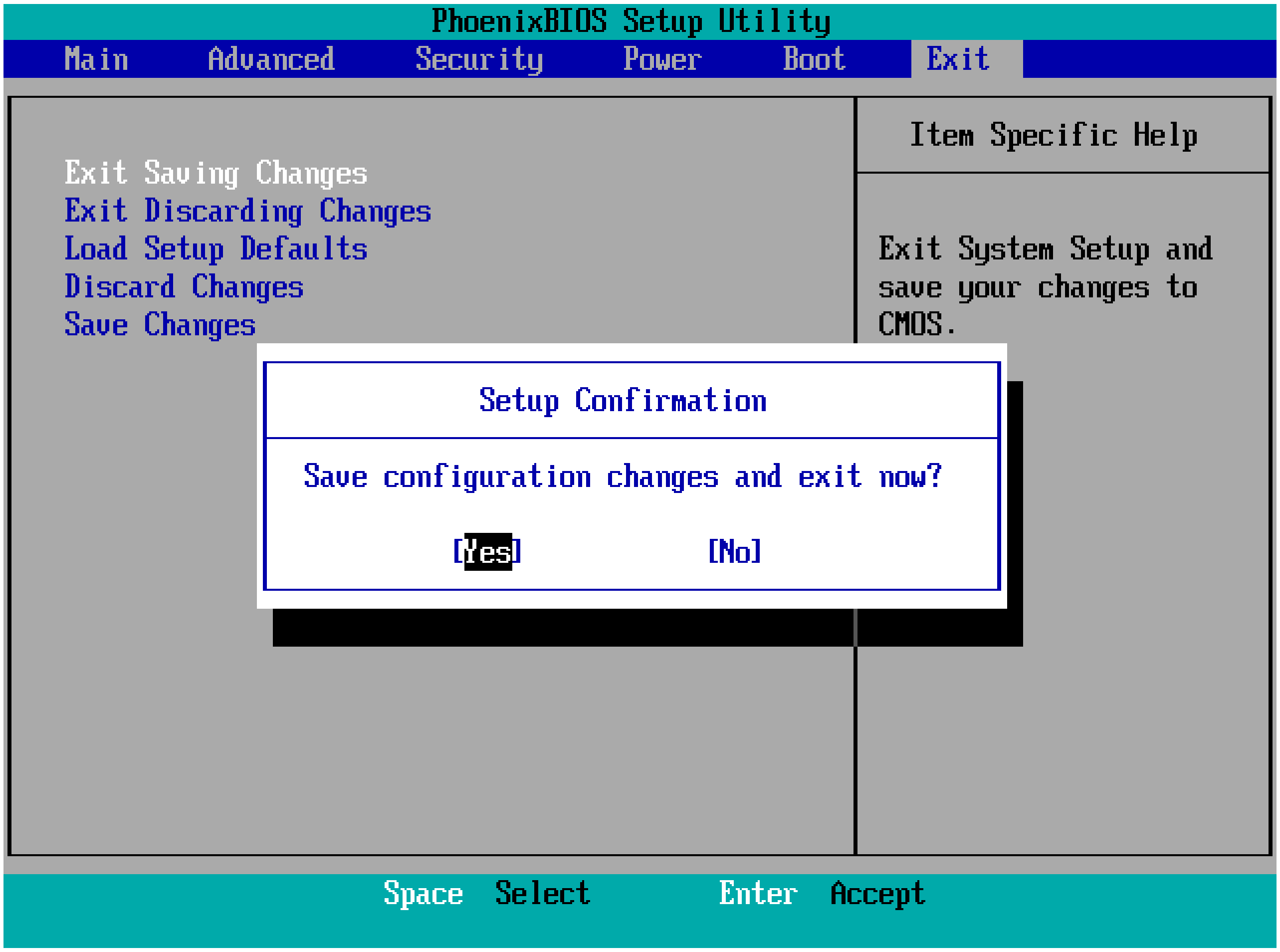
```
                     PhoenixBIOS Setup Utility
  Main     Advanced     Security     Power     Boot     Exit

                                                    Item Specific Help

     CD-ROM Drive
    +Removable Devices                           Keys used to view or
    +Hard Drive                                  configure devices:
     Network boot from AMD Am79C970A             <Enter> expands or
                                                 collapses devices with
                                                 a + or -
                                                 <Ctrl+Enter> expands
                                                 all
                                                 <Shift + 1> enables or
                                                 disables a device.
                                                 <+> and <-> moves the
                                                 device up or down.
                                                 <n> May move removable
                                                 device between Hard
                                                 Disk or Removable Disk
                                                 <d> Remove a device
                                                 that is not installed.

 F1   Help   ↑↓  Select Item   -/+    Change Values        F9   Setup Defaults
 Esc  Exit   ↔   Select Menu   Enter  Select ▶ Sub-Menu    F10  Save and Exit
```

Edit Boot menu the way to make the CD or USB disk with the Reset Windows Password first on the list of boot devices.

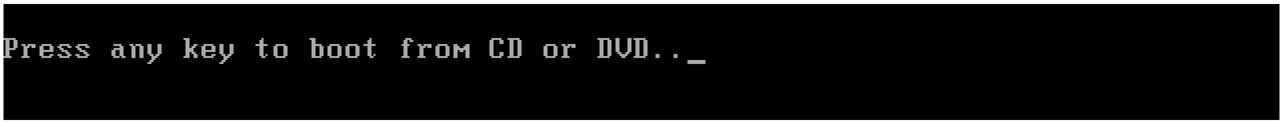


Exit System Setup and save your changes to CMOS.

Setup Confirmation

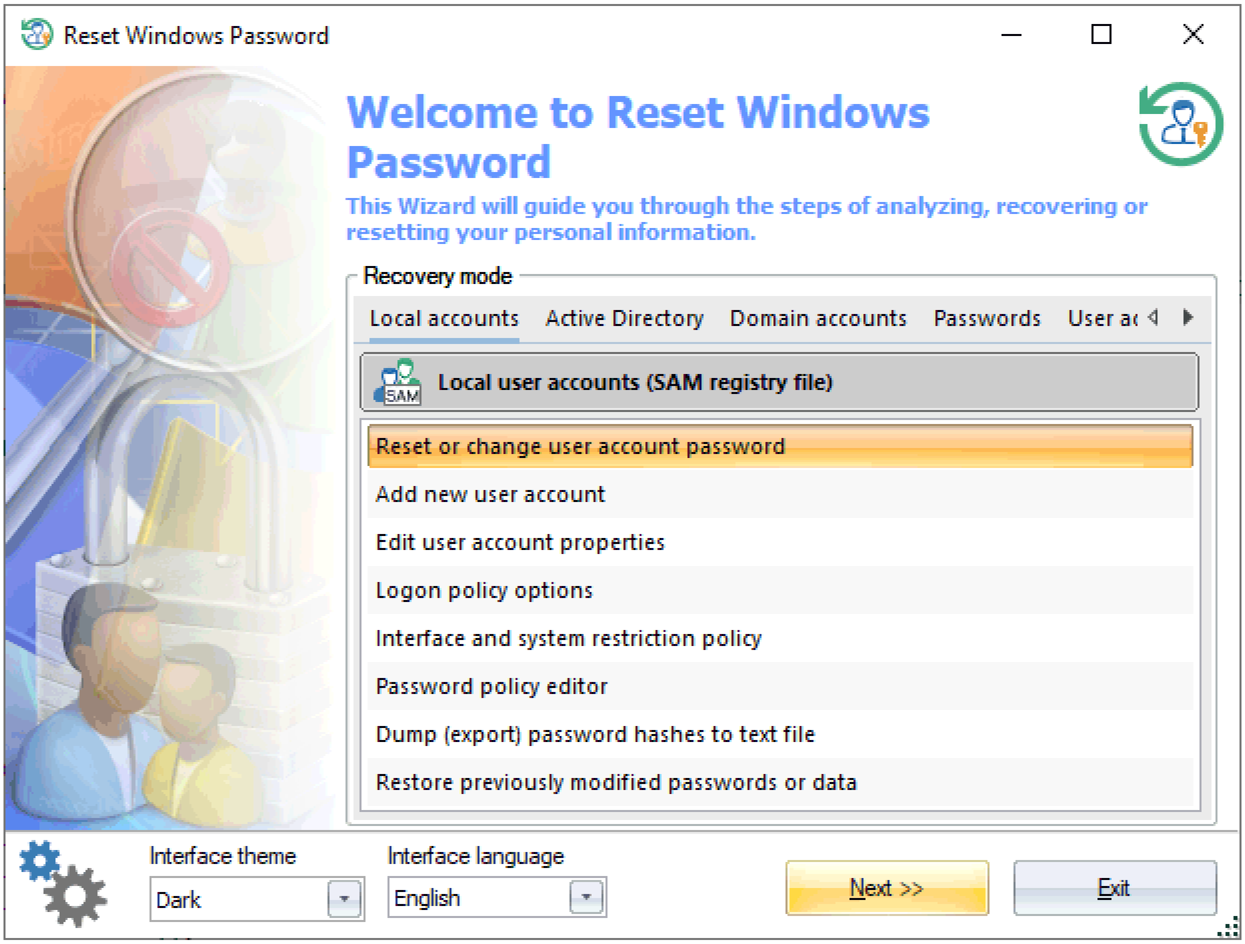
Save configuration changes and exit now?

Make sure to have saved the changes and then reboot the computer.



```
Press any key to boot from CD or DVD.._
```

If everything's gone smoothly, you'll see the following textual message. Hit any key to load from Reset Windows Password bootable disk. Otherwise your old OS will started.



Reset Windows Password

Welcome to Reset Windows Password

This Wizard will guide you through the steps of analyzing, recovering or resetting your personal information.

Recovery mode

Local accounts
Active Directory
Domain accounts
Passwords
User ac
Local user accounts (SAM registry file)
Reset or change user account password
Add new user account
Edit user account properties
Logon policy options
Interface and system restriction policy
Password policy editor
Dump (export) password hashes to text file
Restore previously modified passwords or data
Next >>
Exit

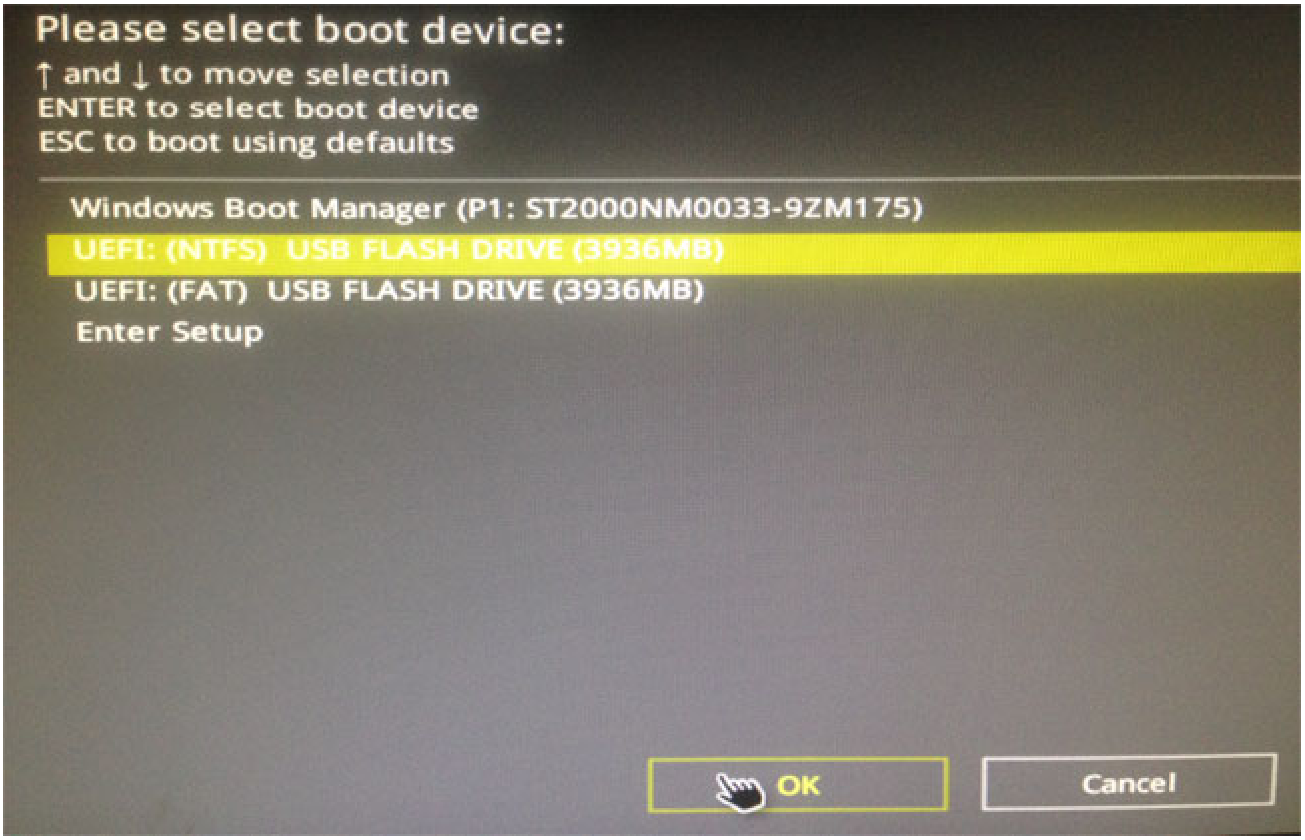
Interface theme: Dark

Interface language: English

RWP has been successfully loaded and ready to use.

2.5 Running the program using UEFI's boot media selection option

If your UEFI supports boot media selection, you can use it to start the program easily off the boot disk. The option is invoked by hitting a hot key (for example, F8) on PC startup. In most versions of UEFI this option is also available from the main menu.



Please select boot device:

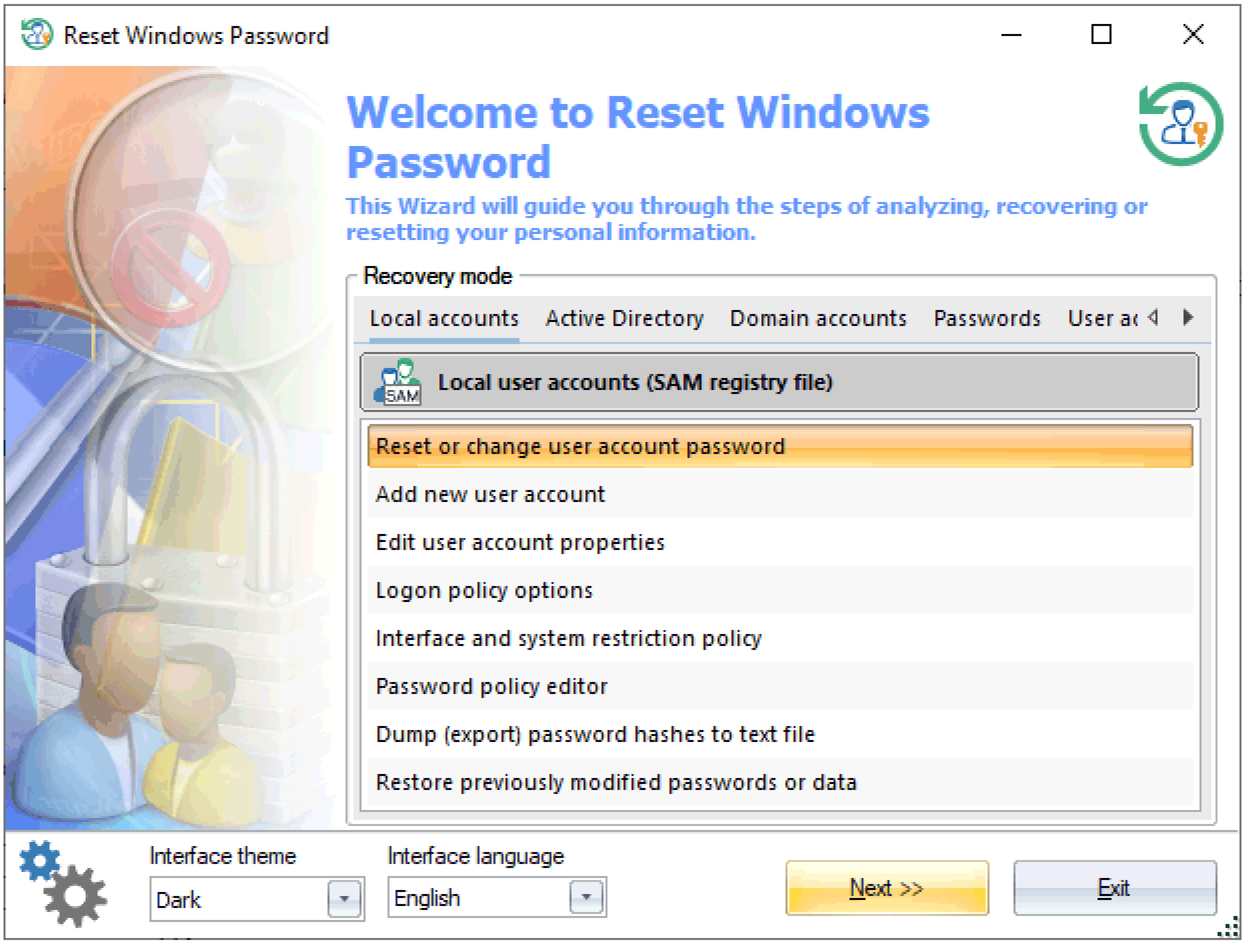
↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults

Windows Boot Manager (P1: ST2000NM0033-9ZM175)
UEFI: (NTFS) USB FLASH DRIVE (3936MB)
UEFI: (FAT) USB FLASH DRIVE (3936MB)
Enter Setup

Working with the program

3 Working with the program

3.1 Main window



Reset Windows Password

Welcome to Reset Windows Password

This Wizard will guide you through the steps of analyzing, recovering or resetting your personal information.

Interface theme: Dark

Interface language: English

Recovery mode
Local accounts
Active Directory
Domain accounts
Passwords
User ac
Local user accounts (SAM registry file)
Reset or change user account password
Add new user account
Edit user account properties
Logon policy options
Interface and system restriction policy
Password policy editor
Dump (export) password hashes to text file
Restore previously modified passwords or data
Next >>
Exit

First, the program suggests to select one of the recovery modes: **Local accounts** – regular user accounts stored in SAM registry file, **Active Directory** – server accounts stored in NTDS.DIT database, **Domain accounts** - domain user accounts (stored in SECURITY registry), **Passwords** - password recovery tools, **User activity** - recent user activity, **Forensic tools** - system investigation and forensic tools, **Files and drives** - miscellaneous forensic tools to work with files, folders, drives, disk images and so on, **Utilities** - other utilities. As you make the selection, the list of available operations should be available for the mode.

Local accounts

- Reset user account password
- Add new user account
- Edit account properties
- Logon policy options
- Interface and system restriction policy editor
- Password policy editor

- Dump password hashes
- Dump Windows Hello PIN
- Restore previously modified passwords, rollback changes

Active Directory

- Reset user account password
- Reset or change DSRM (Directory Services Restore Mode) password
- Edit account properties
- Password policy editor
- Extract BitLocker recovery passwords
- Dump password hashes
- Restore previously modified passwords, rollback changes

Domain accounts

- Reset domain cached password
- Dump domain cached credentials to text file
- Restore previously modified passwords, rollback changes

Passwords

- Search passwords of the local accounts
- Seach passwords of the Active Directory accounts
- Search passwords of the domain cached accounts
- Decrypt Windows Hello credentials
- Lookup PIN
- Lookup SYSKEY startup password
- Lookup passwords for virtual machines
- Lookup passwords for encrypted documents
- Search for Internet/mail/network passwords
- Lookup lost product keys and serial numbers

User activity

- View recent user activity
- View logon history and statistics
- View hardware history
- View software history
- View network history
- Search for recently opened documents
- View Web history
- User IP address history

Forensic tools

- View program execution timeline

- Windows activity timeline
- Windows media forensics
- Sticky notes
- Camera and microphone access tracking
- Clipboard history
- Recycle Bin history
- USB history
- System resource usage monitor
- Windows Search database explorer
- Remote Desktop
- View system events
- Telegram decryptor

Files and drives

- Create disk image
- Load HDD/SSD driver
- Unlock BitLocker-encrypted drives
- Mounting virtual drives
- Hidden volumes explorer
- View last modified files
- View last modified directories
- File checksum calculator
- Duplicate file finder
- Junk file remover and registry cleaner
- Disk space analyzer
- File statistics
- Fast disk search

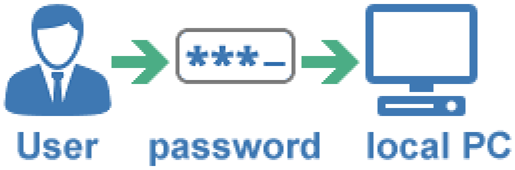
Utilities

- Search for protected documents
- Backup Passwords and sensitive information
- Remove user sensitive information
- Network drive mapper
- ESE (Extensible Storage Engine) database explorer
- SQLite database viewer
- Boot status explorer

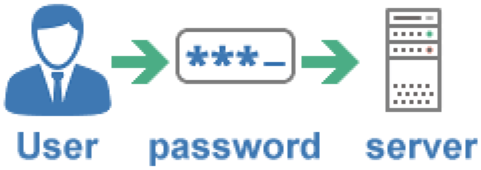
Schematic description of the logon types

SAM

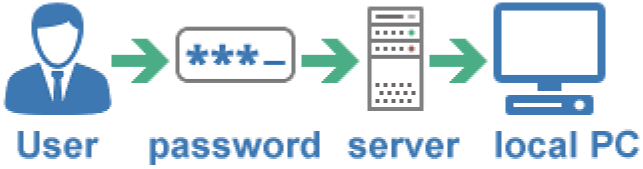
A regular user account of any home PC. Password hashes are stored in SAM registry file on the same computer.

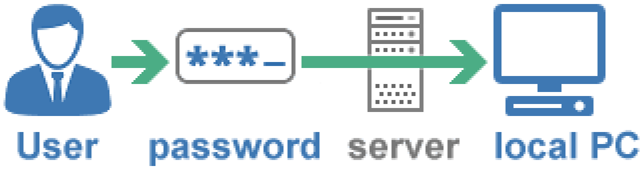


Active Directory
A domain user account. Password hashes are stored in NTDS.DIT database on domain PC.



DCC
Cached credentials of domain accounts. Password hashes can be stored (depending on domain security policy) on the local PC. The account login is performed either through the domain or using the cached credentials.

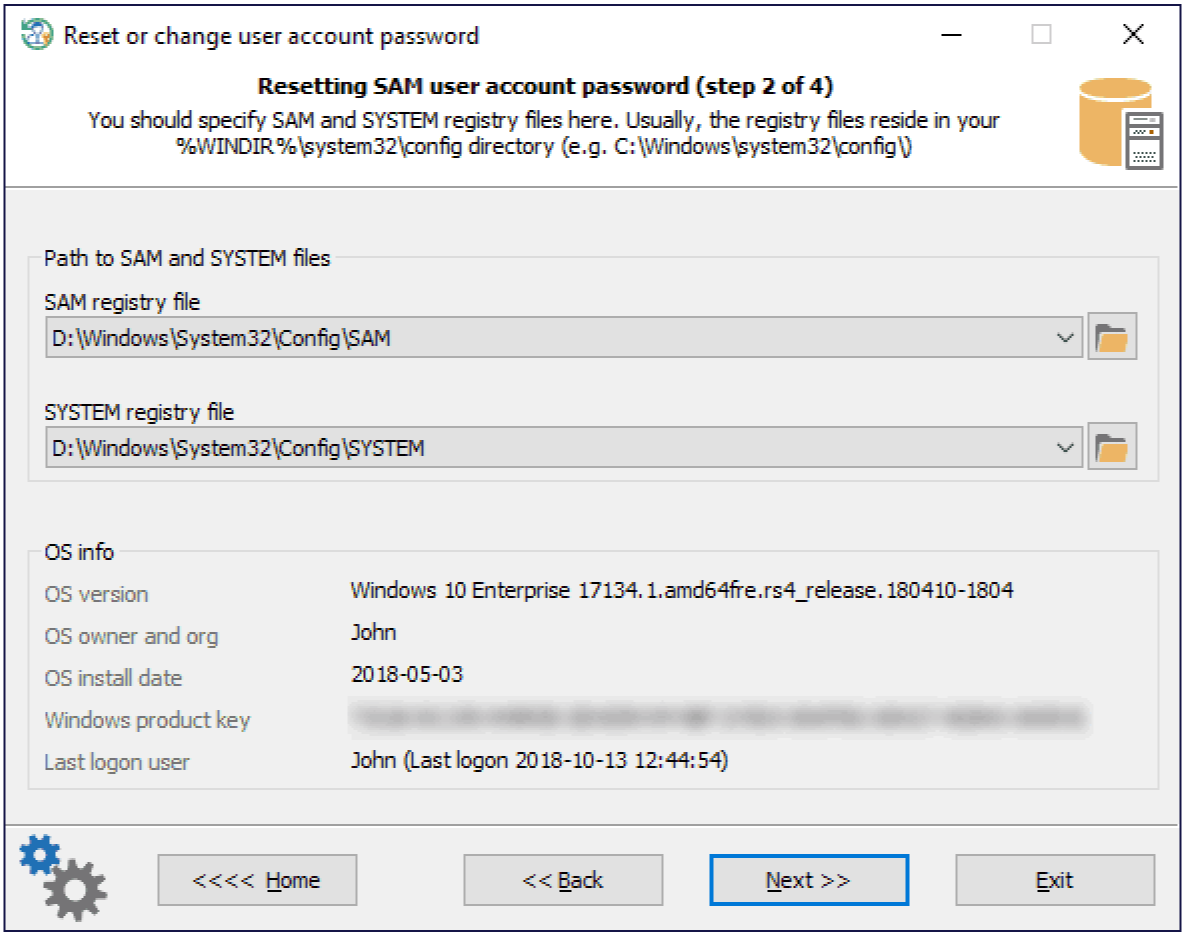




3.2 Local accounts

3.2.1 Reset user passwords

Selecting data source



Resetting SAM user account password (step 2 of 4)

You should specify SAM and SYSTEM registry files here. Usually, the registry files reside in your %WINDIR%\system32\config directory (e.g. C:\Windows\system32\config\)

Path to SAM and SYSTEM files

SAM registry file: D:\Windows\System32\Config\SAM

SYSTEM registry file: D:\Windows\System32\Config\SYSTEM

OS info

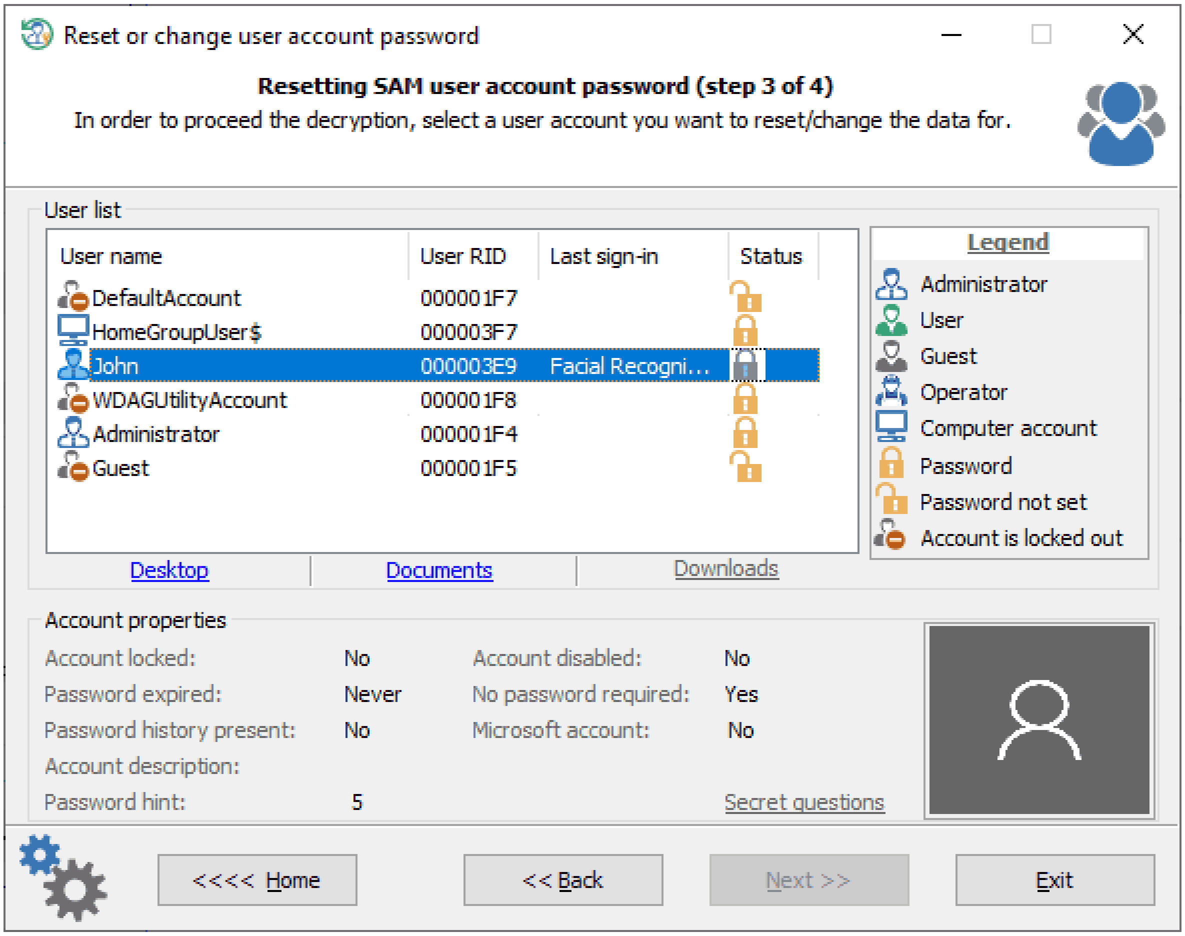
OS version	Windows 10 Enterprise 17134.1.amd64fre.rs4_release.180410-1804
OS owner and org	John
OS install date	2018-05-03
Windows product key	[redacted]
Last logon user	John (Last logon 2018-10-13 12:44:54)

To reset a regular account password, you should select two registry files: **SAM** and **SYSTEM**. The application automatically searches all files and suggests the first ones it finds. The registry files are located in the **%WINDIR%\system32\config** folder. Where %WINDIR% is your windows directory.

If you select Active Directory mode during the previous step, you should set the location of the Active Directory database instead of the SAM registry file. By default, that's the **%WINDIR%\NTDS** folder. So the full path to the AD database may look like this: C:\Windows\NTDS\ntds.dit

The *OS Info* shows a version of the found Operating System, its owner and installation date, the last logged-in user, and the Windows product key if found.

Choosing a Windows account



Resetting SAM user account password (step 3 of 4)

In order to proceed the decryption, select a user account you want to reset/change the data for.

User name	User RID	Last sign-in	Status
DefaultAccount	000001F7		🔓
HomeGroupUser$	000003F7		🔒
John	000003E9	Facial Recogni...	🔒
WDAGUtilityAccount	000001F8		🔒
Administrator	000001F4		🔒
Guest	000001F5		🔓

Desktop | Documents | Downloads

Legend:
- Administrator
- User
- Guest
- Operator
- Computer account
- 🔒 Password
- 🔓 Password not set
- Account is locked out

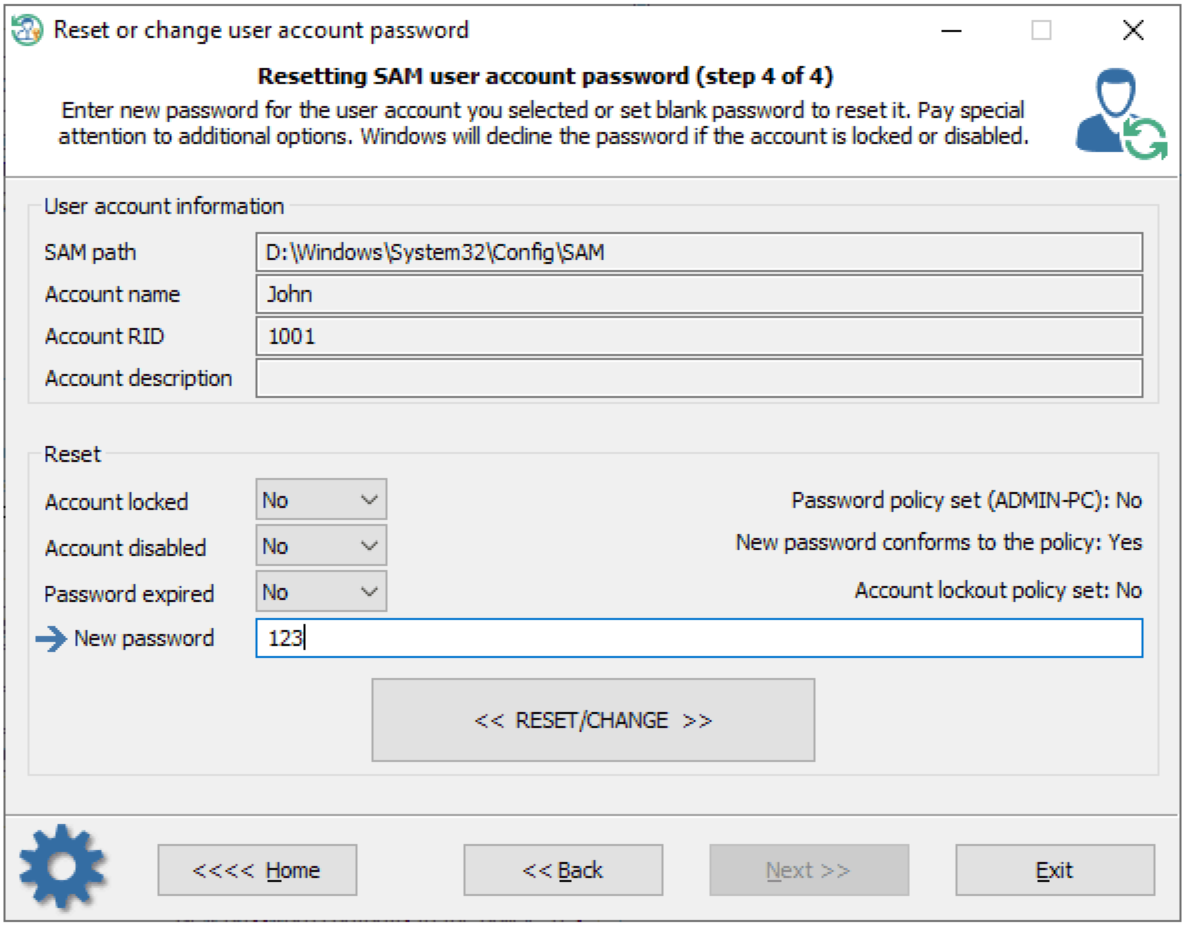
Account locked:	No	Account disabled:	No
Password expired:	Never	No password required:	Yes
Password history present:	No	Microsoft account:	No
Account description:			
Password hint:	5	Secret questions	

The top of the dialog displays the list of user accounts found, their status, and the date of the last logon. By clicking on one of the items, you can view additional information about the account; namely: whether it is locked or disabled, whether the password is required, whether the password history is available, its password hint, etc.

You can also display the selected account's desktop, documents, or download folder.

All Windows 10 versions starting from v17063 have a new security feature, called secret questions. The secret questions is an additional security layer aimed to protect the local accounts against an unauthorized password change. Reset Windows Password can successfully extract and display the secret questions.

Resetting password



Reset or change user account password

Resetting SAM user account password (step 4 of 4)

Enter new password for the user account you selected or set blank password to reset it. Pay special attention to additional options. Windows will decline the password if the account is locked or disabled.

User account information

SAM path	D:\Windows\System32\Config\SAM
Account name	John
Account RID	1001
Account description	

Reset

Account locked	No	Password policy set (ADMIN-PC): No
Account disabled	No	New password conforms to the policy: Yes
Password expired	No	Account lockout policy set: No
New password	123	

To reset the password, leave the '*New password*' field blank and click on the '*Reset/Change*' button. Take a note of the additional options. The account must be not locked, disabled or expired.

Besides that, if local or domain password policies are set, make sure that the new password complies with the length and complexity requirements and does not match any of the passwords used earlier (if password history exists.) Otherwise, you will be unable to logon to the system even if you reset the password successfully.

If you are resetting a password of the built-in Administrator, keep in mind that in order to activate this account and logon to the system, you would need to load the system in Safe mode. To do that, before Windows starts loading, keep pressing the F8 key until the textual system boot selection dialog appears. In that dialog, select the safe mode item. After that, the built-in Administrator account will become active, and you will be able to use it.

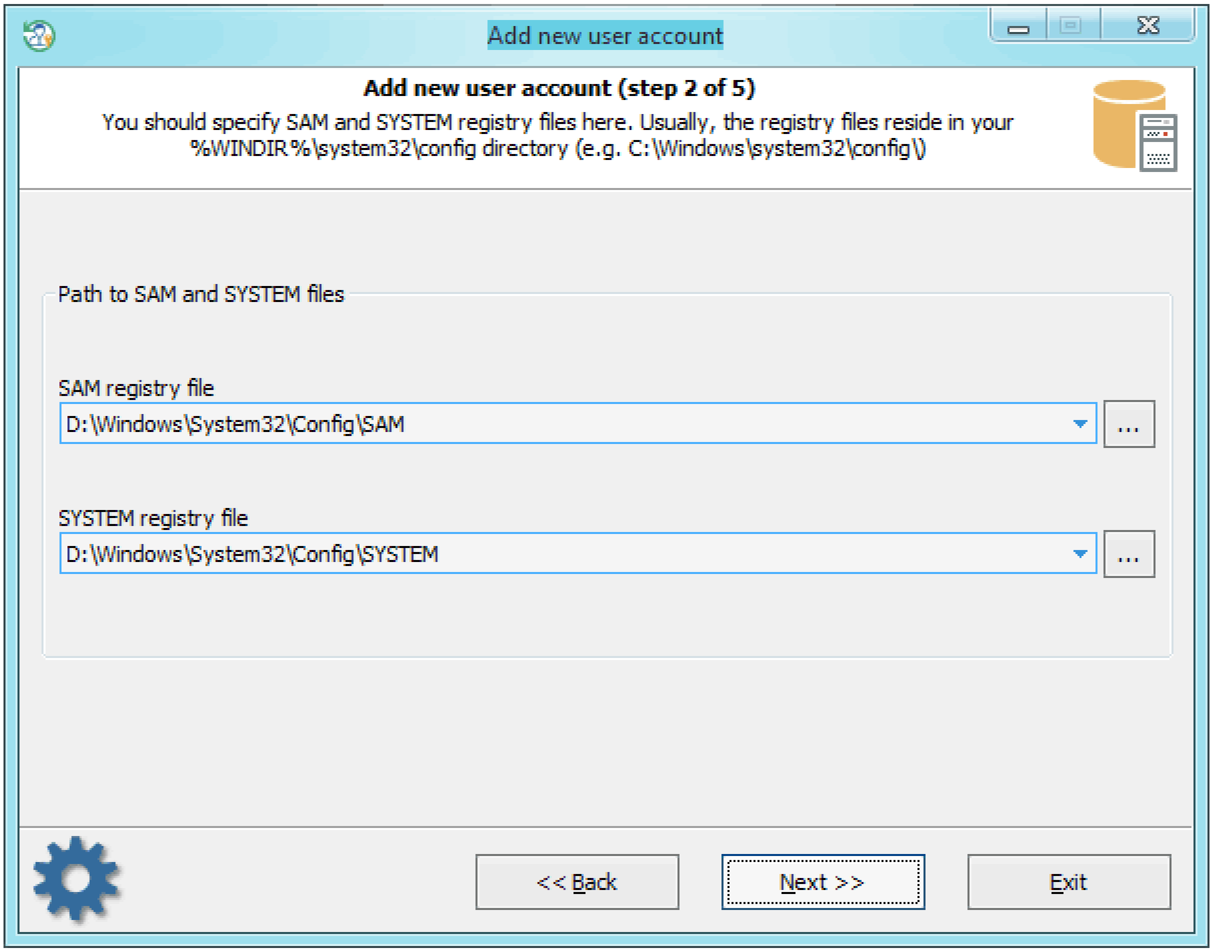
On Windows 8 and later operating systems, click the *Power* button, press and hold the SHIFT key on your keyboard and select *Restart*.

Note that you will have to enter a non-empty password in order to be able to log on LiveID or Microsoft account.

3.2.2 Add new user account

Adding new local account is simple as it is. We tried to arrange it into 3 common steps.

1. Selecting data source



Add new user account

Add new user account (step 2 of 5)

You should specify SAM and SYSTEM registry files here. Usually, the registry files reside in your %WINDIR%\system32\config directory (e.g. C:\Windows\system32\config\)

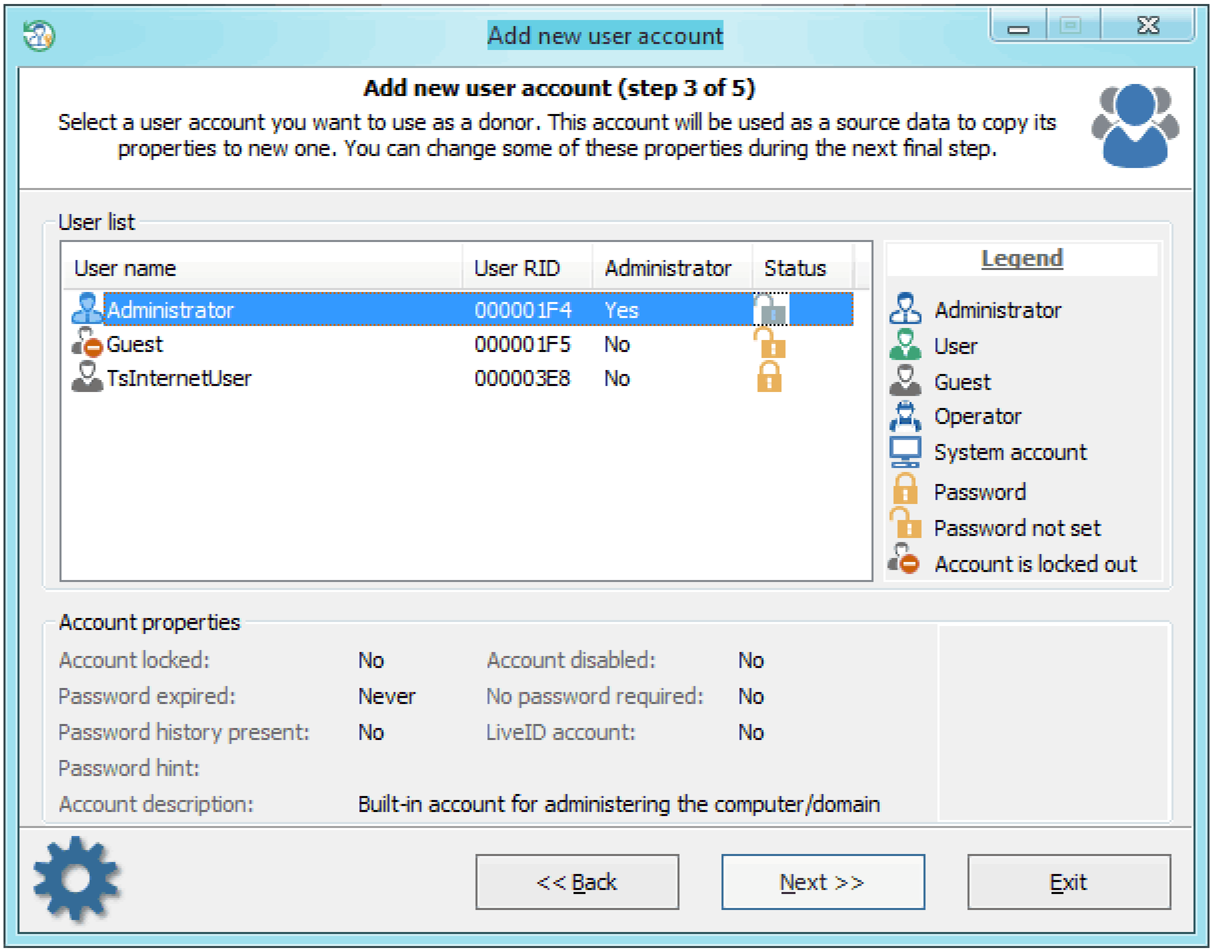
Path to SAM and SYSTEM files

SAM registry file: D:\Windows\System32\Config\SAM

SYSTEM registry file: D:\Windows\System32\Config\SYSTEM

You should select **SAM** and **SYSTEM** files first. The program usually searches for and suggests the files automatically. In case you need to set the files manually for some reason, do know that the registry files are located in the **%WINDIR%\system32\config** directory.

2. Choosing a donor account



Add new user account

Add new user account (step 3 of 5)

Select a user account you want to use as a donor. This account will be used as a source data to copy its properties to new one. You can change some of these properties during the next final step.

User list

User name	User RID	Administrator	Status
Administrator	000001F4	Yes	🔓
Guest	000001F5	No	🔓
TsInternetUser	000003E8	No	🔒

Legend

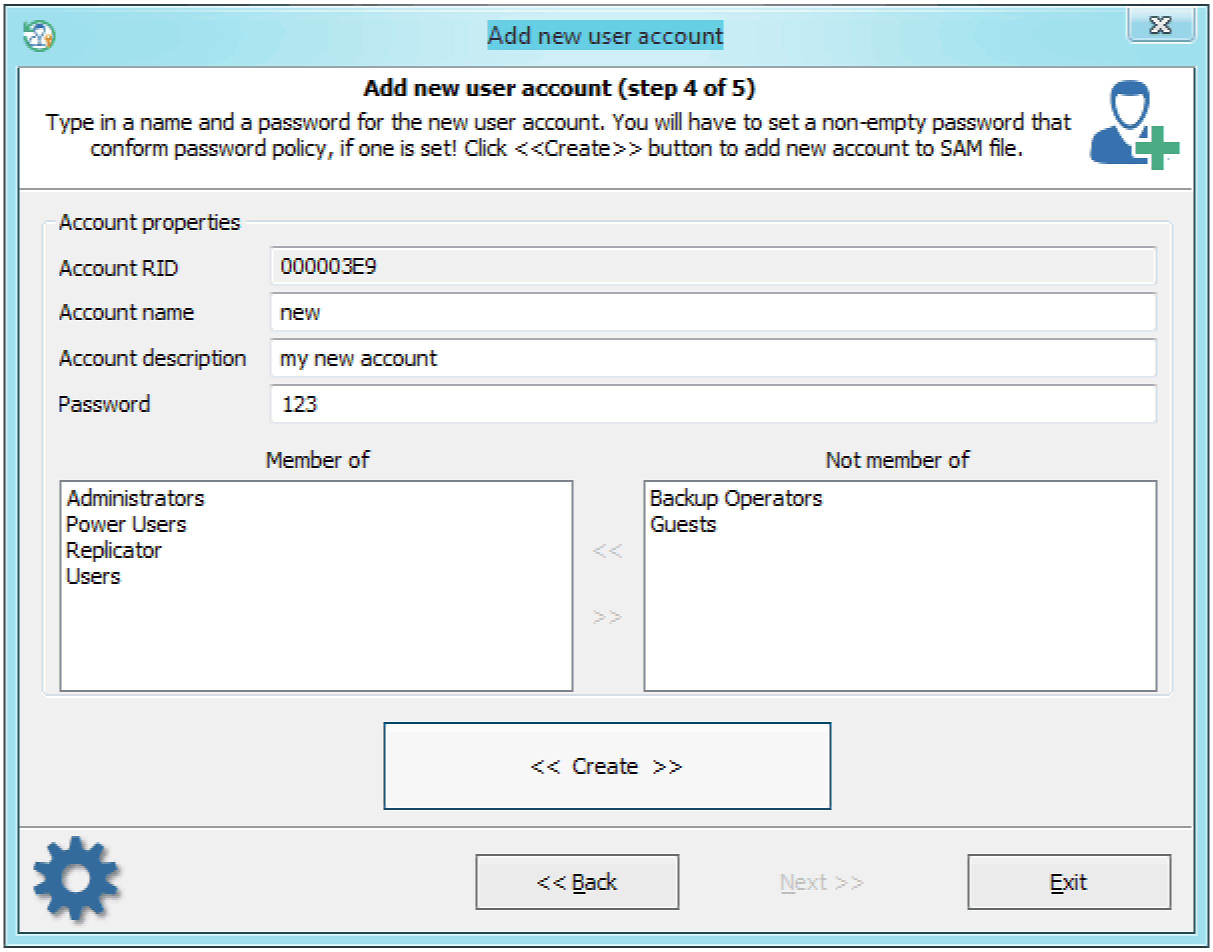
- Administrator
- User
- Guest
- Operator
- System account
- 🔒 Password
- 🔓 Password not set
- Account is locked out

Account properties

Account locked:	No	Account disabled:	No
Password expired:	Never	No password required:	No
Password history present:	No	LiveID account:	No
Password hint:			
Account description:	Built-in account for administering the computer/domain		

Select a user you want to use as a donor account. All properties of the source account will be copied to the newly created one. No problem if the source account is locked or disabled, the program should fix some of its critical properties and set up default flags. For example, if the source account is set to allow logging on to system in certain hours, the program will zero out the restriction.

3. Adding new account



Add new user account

Add new user account (step 4 of 5)

Type in a name and a password for the new user account. You will have to set a non-empty password that conform password policy, if one is set! Click <<Create>> button to add new account to SAM file.

Account properties

Account RID: 000003E9

Account name: new

Account description: my new account

Password: 123

Member of	Not member of
Administrators Power Users Replicator Users	Backup Operators Guests

Now all you need is to set a name, description and a password for the new account. Leave the password field blank to set empty password. Note that if the target OS has password policy set, your new password should conform the policy.

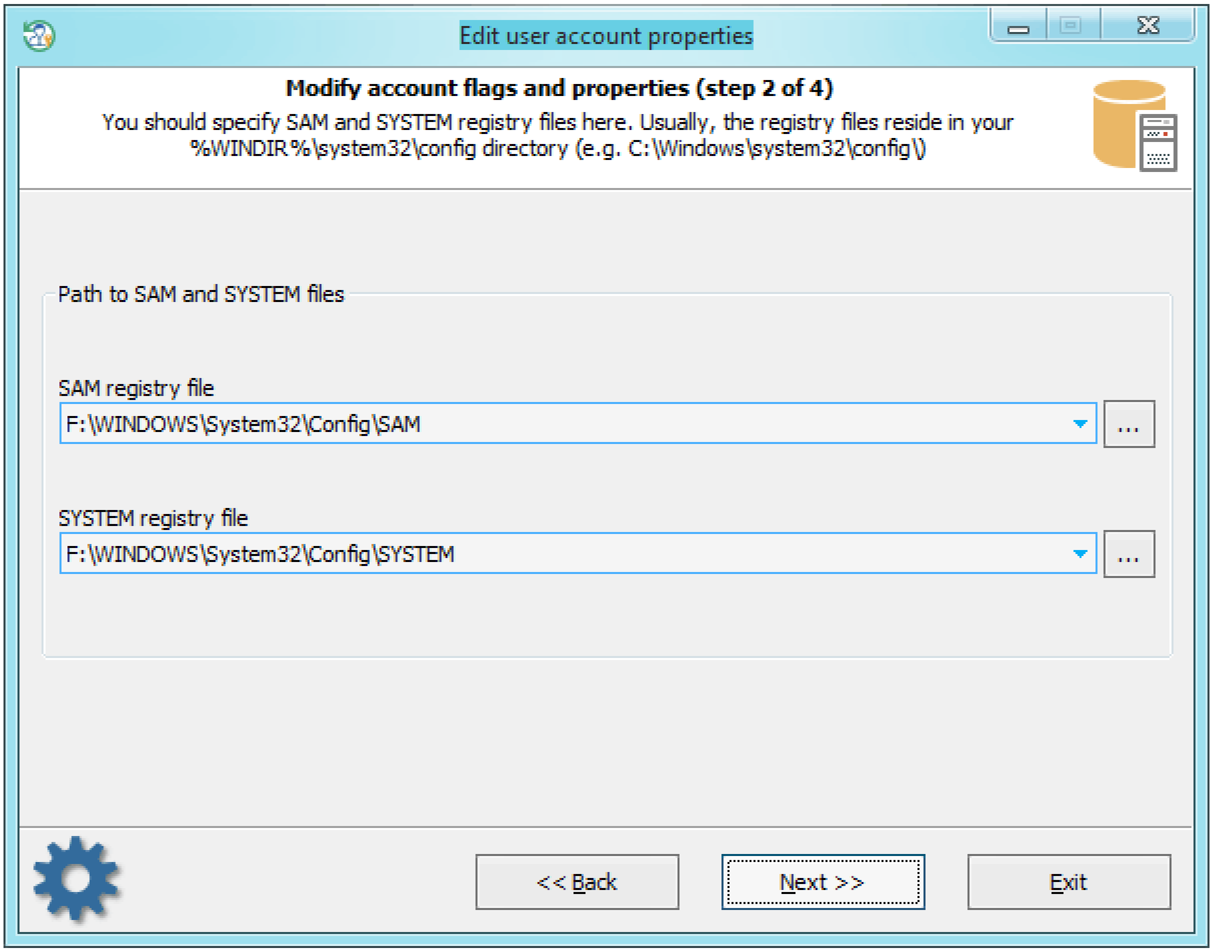
You should pay a special attention setting group membership of the new account. Usually, you should make it a member of 'Administrators' and/or 'Users' group in order to be able to log on locally, if otherwise is not specified by your security policy. Setting an incorrect membership may cause troubles, for example, deleting the account.

After the account is created successfully, you can step back to the main dialog, select 'Edit account properties' mode and set/unset some extended flags, if needed.

3.2.3 Edit user account properties

New version of the program allows you manipulating with extended properties of the target user account, as well as changing Microsoft Live ID account to local account or vice versa. This is an extremely helpful when you need to unlock/enable locked/disabled account, unset the 'password expired' flag, disable the "Smart card logon" if your smart card has lost occasionally, etc. Modifying properties of the problem account is easy pretty much. First you should select the target Operating System's files.

Selecting data source



Modify account flags and properties (step 2 of 4)

You should specify SAM and SYSTEM registry files here. Usually, the registry files reside in your %WINDIR%\system32\config directory (e.g. C:\Windows\system32\config\)

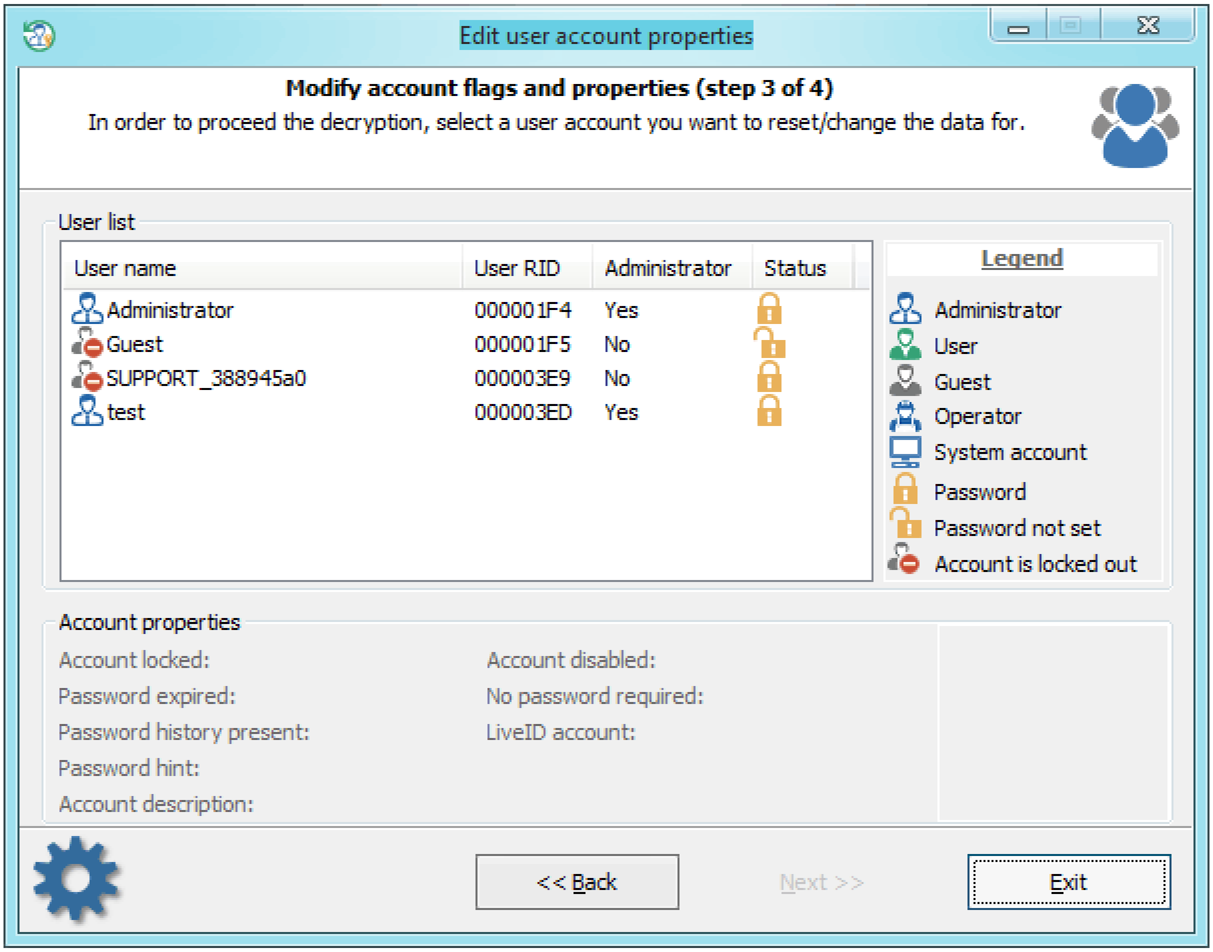
Path to SAM and SYSTEM files

SAM registry file: F:\WINDOWS\System32\Config\SAM

SYSTEM registry file: F:\WINDOWS\System32\Config\SYSTEM

Two files are needed. These are either **SAM** and **SYSTEM** (in case you're modifying a local account) or **NTDS.DIT** and **SYSTEM** (when you need to change the propertied of a domain user). The program automatically searches for these files and suggests the first ones it finds. You can also specify paths to these files manually. They are located in the **%WINDIR%\system32\config** and **%WINDIR%\NTDS** folders. Where %WINDIR% is your windows directory. So the full path to the Active Directory database may look like this: C:\Windows\NTDS\ntds.dit

Choosing a Windows account



Modify account flags and properties (step 3 of 4)

In order to proceed the decryption, select a user account you want to reset/change the data for.

User list

User name	User RID	Administrator	Status
Administrator	000001F4	Yes	🔒
Guest	000001F5	No	🔓
SUPPORT_388945a0	000003E9	No	🔒
test	000003ED	Yes	🔒

Legend

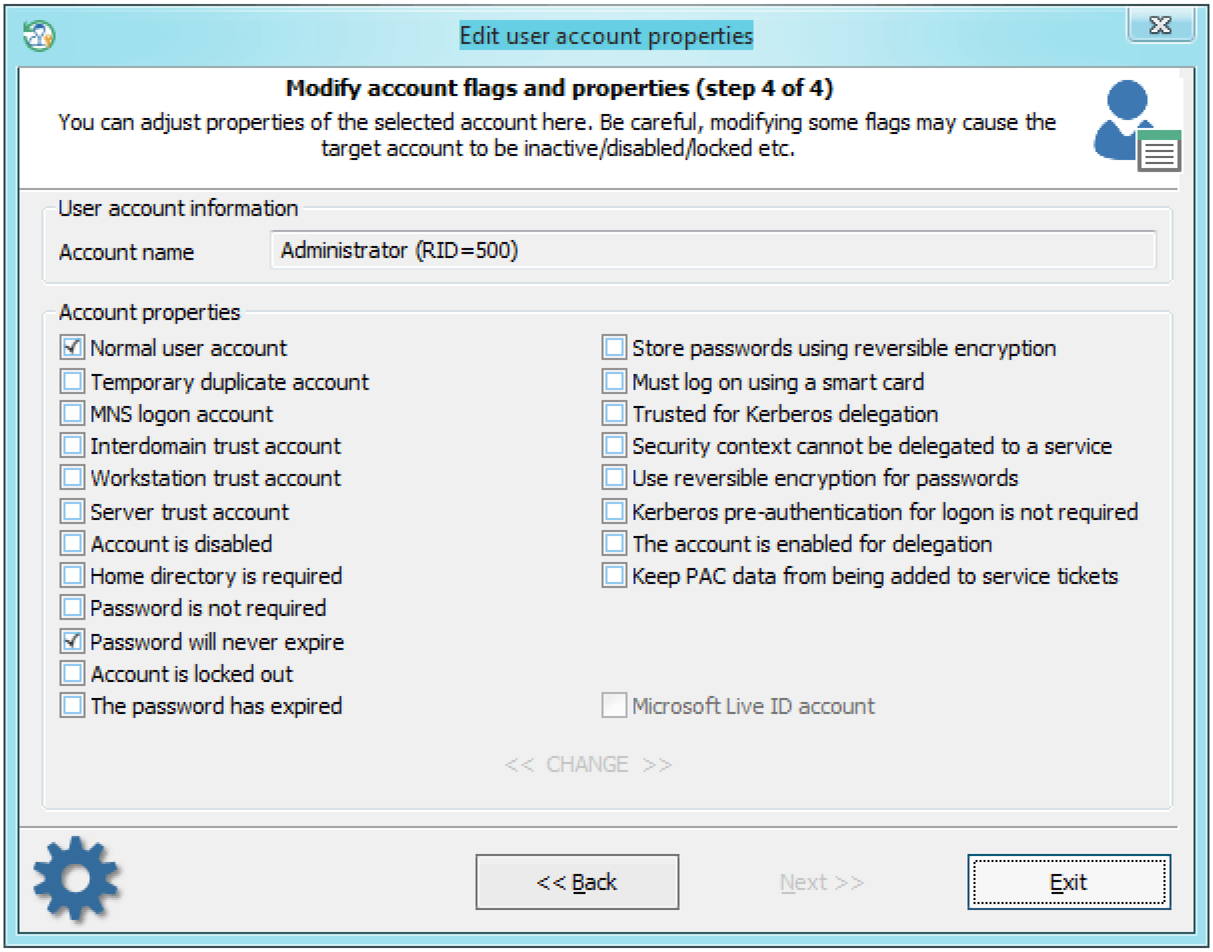
- Administrator
- User
- Guest
- Operator
- System account
- Password
- Password not set
- Account is locked out

Account properties

Account locked:
Password expired:
Password history present:
Password hint:
Account description:
Account disabled:
No password required:
LiveID account:

Once the source files are selected, the program enumerates and displays the list of all found user accounts. Select one you need and click 'Next' button to open the final dialog with the user's properties.

[Changing account properties](#)



Edit user account properties

Modify account flags and properties (step 4 of 4)

You can adjust properties of the selected account here. Be careful, modifying some flags may cause the target account to be inactive/disabled/locked etc.

User account information

Account name: Administrator (RID=500)

Account properties

- ☑ Normal user account
- □ Temporary duplicate account
- □ MNS logon account
- □ Interdomain trust account
- □ Workstation trust account
- □ Server trust account
- □ Account is disabled
- □ Home directory is required
- □ Password is not required
- ☑ Password will never expire
- □ Account is locked out
- □ The password has expired
- □ Store passwords using reversible encryption
- □ Must log on using a smart card
- □ Trusted for Kerberos delegation
- □ Security context cannot be delegated to a service
- □ Use reversible encryption for passwords
- □ Kerberos pre-authentication for logon is not required
- □ The account is enabled for delegation
- □ Keep PAC data from being added to service tickets
- □ Microsoft Live ID account

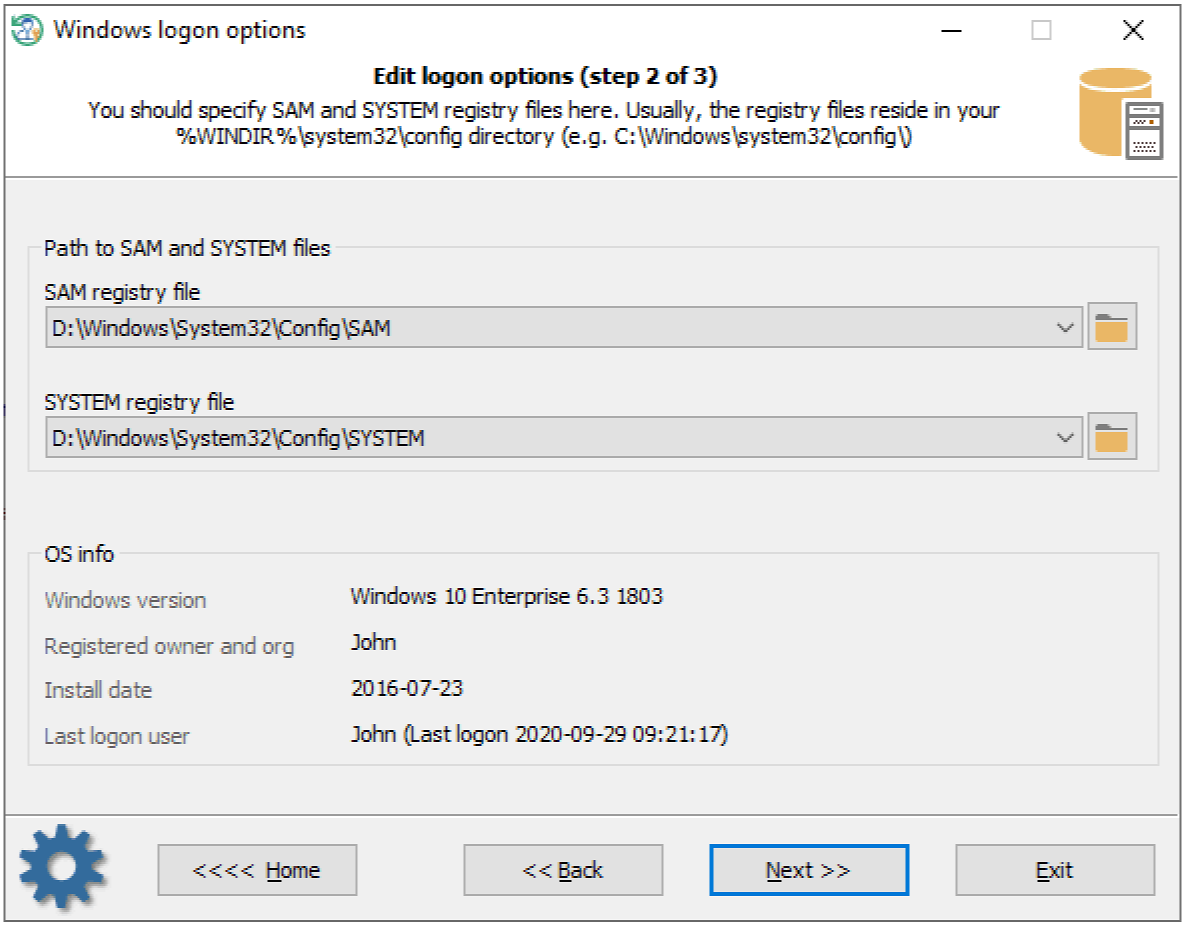
You can set/unset here different flags that control the behavior of the user account.

Be careful, changing some flags may cause the target account to be locked/disabled etc.

3.2.4 Logon policy options

You can use the settings to change the way users log on to Windows. For example, display last logged on user name, assign a default domain for logon, turn on/off passwordless sign-in, etc.

Selecting data source



Windows logon options

Edit logon options (step 2 of 3)

You should specify SAM and SYSTEM registry files here. Usually, the registry files reside in your %WINDIR%\system32\config directory (e.g. C:\Windows\system32\config\)

Path to SAM and SYSTEM files

SAM registry file: D:\Windows\System32\Config\SAM

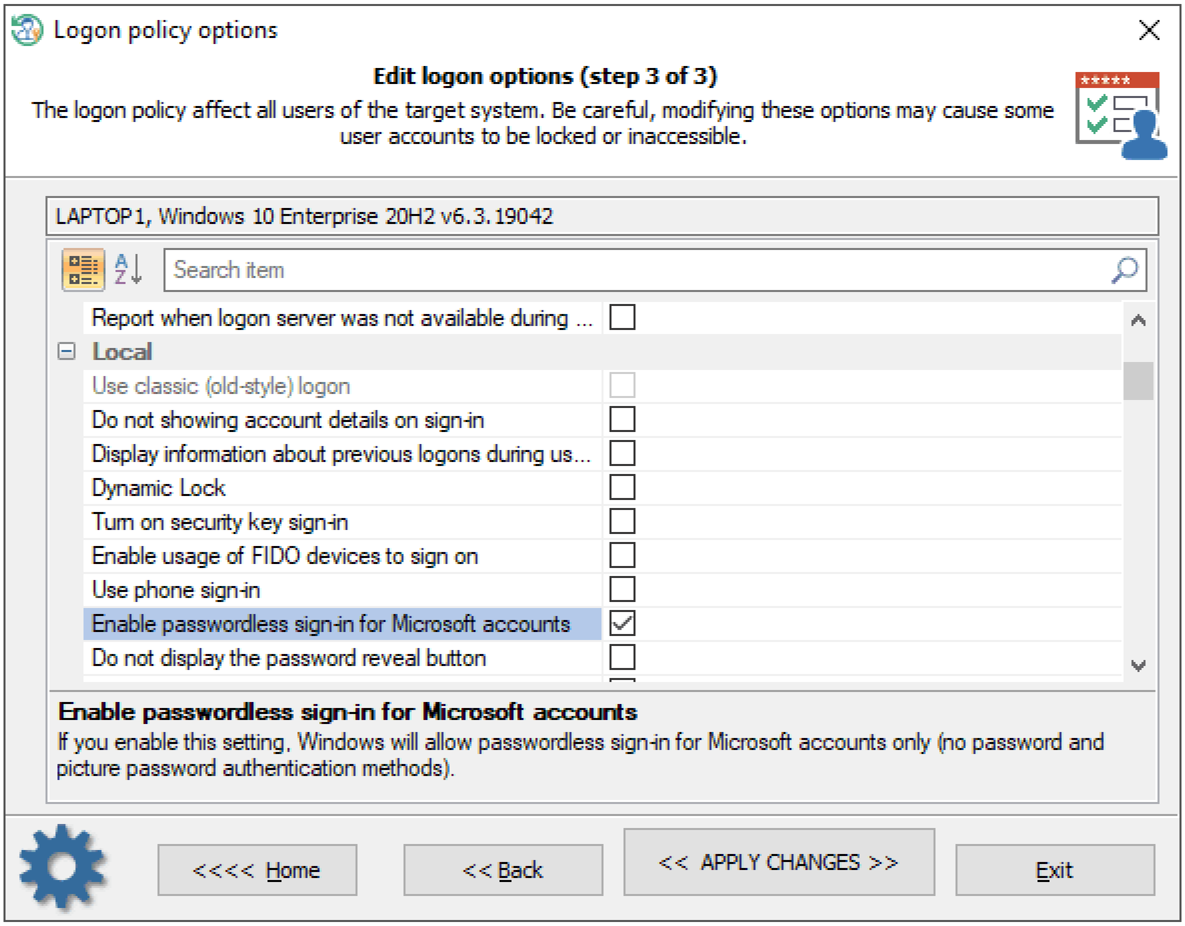
SYSTEM registry file: D:\Windows\System32\Config\SYSTEM

OS info

Windows version	Windows 10 Enterprise 6.3 1803
Registered owner and org	John
Install date	2016-07-23
Last logon user	John (Last logon 2020-09-29 09:21:17)

First, choose SAM and SYSTEM registry files that were found by the program or specify paths to them manually if RWP failed to find ones.

Changing logon policy options



Logon policy options

Edit logon options (step 3 of 3)

The logon policy affect all users of the target system. Be careful, modifying these options may cause some user accounts to be locked or inaccessible.

LAPTOP1, Windows 10 Enterprise 20H2 v6.3.19042

- Report when logon server was not available during ... □
- ⊟ Local
- Use classic (old-style) logon □
- Do not showing account details on sign-in □
- Display information about previous logons during us... □
- Dynamic Lock □
- Turn on security key sign-in □
- Enable usage of FIDO devices to sign on □
- Use phone sign-in □
- Enable passwordless sign-in for Microsoft accounts ☑
- Do not display the password reveal button □

Enable passwordless sign-in for Microsoft accounts
If you enable this setting, Windows will allow passwordless sign-in for Microsoft accounts only (no password and picture password authentication methods).

Once the files are selected, you can alter any available logon options. Click the << APPLY CHANGES >> button to apply and save the changes. The options affect all local users of the target system.

Be careful, modifying these options may cause some accounts to be inaccessible or locked.

The setting of the **Domain** group:

Name	Description
Allow users to select when a password is required when resuming from connected standby	If you enable this setting, a user on a Connected Standby device can change the amount of time after the device's screen turns off before a password is required when waking the device. If you disable this setting, a user cannot change the amount of time after the device's screen turns off before a password is required when waking the device. Instead, a password is required immediately after the screen turns off.
Default domain for logon	Specifies a default logon domain, which might be a different domain than the domain to which the computer is joined.
Do not enumerate connected users on domain-joined computers	If you enable this setting, the Logon UI will not enumerate any connected users on domain-joined computers.
Enumerate local users on domain-joined computers	If you enable this setting, Logon UI will enumerate all local users on domain-joined computers.
Turn off picture password sign-in for domain users	This setting allows you to control whether a domain user can sign in using a picture password.

Turn on convenience PIN sign-in for domain users	If you enable this setting, a domain user can set up and sign in with a convenience PIN. Note: The user's domain password will be cached in the system vault when using this feature.
Report when logon server was not available during user logon	This setting controls whether the logged on user should be notified if the logon server could not be contacted during logon and he has been logged on using previously stored account information.

The setting of the **Local** group:

Name	Description
Use classic (old-style) logon	Always use classic logon interface scheme
Do not showing account details on sign-in	If set, prevents the user from showing account details (email address or user name) on the sign-in screen.
Display information about previous logons during user logon	If you enable this setting, a message appears after the user logs on that displays the date and time of the last successful logon by that user, the date and time of the last unsuccessful logon attempted with that user name, and the number of unsuccessful logons since the last successful logon by that user.
Dynamic Lock	If you enable this setting, Windows will enable dynamic lock for all users on managed devices and users will not be allowed to disable dynamic lock on their accounts.
Turn on security key sign-in	If you enable this setting, users can sign in with external security keys.
Enable usage of FIDO devices to sign on	This setting allows users to use a FIDO device, such as a phone, NFC card, to sign on to a desktop computer running Windows 10.
Use phone sign-in	If you enable this setting, phone sign-in will be enabled, allowing the use of a phone as a companion device for desktop authentication.
Enable passwordless sign-in for Microsoft accounts	If you enable this setting, Windows will allow passwordless sign-in only: both password and picture password authentication methods will be turned off. This option affects Microsoft accounts only.
Do not display the password reveal button	If you enable this setting, the password reveal button will not be displayed after a user types a password in the password entry text box.
Prevent the use of security questions for local accounts	If you turn this setting on, local users won't be able to set up and use security questions to reset their passwords.
Allow companion device for secondary authentication	If you enable or do not configure this setting, users can authenticate to Windows Hello using a companion device. Such as a phone, fitness band, or IoT device.
Software Secure Attention Sequence	This setting controls whether or not software can simulate the Secure Attention Sequence (SAS).
The mode of automatically signing in and locking last interactive user after a restart or cold boot	This setting controls the configuration under which an automatic restart and sign on and lock occurs after a restart or cold boot.
Sign-in and lock last interactive user automatically after a restart	This setting controls whether a device will automatically sign in and lock the last interactive user after the system restarts or after a shutdown and cold boot. This only occurs if the last interactive user didn't sign out before the restart or shutdown.?

The setting of the **Misc** group:

Name	Description
Always use custom logon background	If you enable this policy setting, the logon screen always attempts to load a custom background instead of the Windows-branded logon background.

Show clear logon background	This setting disables the acrylic blur effect on logon background image.
Do not display the Getting Started welcome screen at logon	If you enable this setting, the welcome screen is hidden from the user logging on to the system.
Turn off app notifications on the lock screen	This setting allows you to prevent app notifications from appearing on the lock screen.
Show first sign-in animation	This setting allows you to control whether users see the first sign-in animation when signing in to the computer for the first time.
Turn off Windows Startup sound	Turn off Windows sounds during authentication
Do not process the legacy run list	This setting ignores the customized run list (programs and services that the system starts).
Do not process the run once list	If you enable this setting, the system ignores the list of additional programs and documents that are started automatically the next time the system starts. The customized run-once lists are stored in the registry in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\runOnce.
Hide entry points for Fast User Switching	This setting allows you to hide the Switch User interface in the Logon UI, the Start menu and the Task Manager.
Block all consumer Microsoft account user authentication	If this setting is enabled, all applications and services on the device are prevented from using Microsoft accounts for authentication.
Default credential provider	Assign a specified credential provider as the default credential provider.
Exclude credential providers	This setting allows the administrator to exclude the specified credential providers from use during authentication.

The setting of the **Network** group:

Name	Description
Always wait for the network at computer startup and logon	Determines whether computers wait for the network to be fully initialized during startup and user logon. By default, computers do not wait for the network to be fully initialized at startup and logon.
Do not display network selection UI	If you enable this setting, the PC's network connectivity state cannot be changed without signing into Windows.

The setting of the **Biometrics** group:

Name	Description
Allow domain users to log on using biometrics	If you enable or do not configure this setting, Windows allows domain users to log on to a domain-joined computer using biometrics.
Allow users to log on using biometrics	If you enable or do not configure this setting, all users can log on to a local Windows-based computer and can elevate permissions with UAC using biometrics.
Allow the use of biometrics	If you enable or do not configure this setting, the Windows Biometric Service is available, and users can run applications that use biometrics on Windows.
Configure enhanced anti-spoofing	If you enable this setting, Windows requires all users on managed devices to use enhanced anti-spoofing for Windows Hello face authentication. This disables Windows Hello face authentication on devices that do not support enhanced anti-spoofing.
Specify timeout for fast user switching events	This setting specifies the number of seconds a pending fast user switch event will remain active before the switch is initiated. By default, a fast user switch event is active for 10 seconds before becoming inactive.

The setting of the **PIN** group:

Name	Description
PIN expiration	This setting specifies the period of time in days (between 1 and 730) that a PIN can be used before the system requires the user to change it.
PIN history	This setting specifies the number of past PINs that can be associated to a user account that can't be reused. The value must be between 0 to 50 PINs.
Maximum PIN length	Maximum PIN length configures the maximum number of characters allowed for the PIN. The largest number you can configure for this policy setting is 127.
Minimum PIN length	Minimum PIN length configures the minimum number of characters required for the PIN. The lowest number you can configure for this policy setting is 4.
Require digits	If you enable or do not configure this setting, Windows requires users to include at least one digit in their PIN.
Require lowercase letters	If you enable this setting, Windows requires users to include at least one lowercase letter in their PIN.
Require special characters	If you enable this policy setting, Windows requires users to include at least one special character in their PIN.
Require uppercase letters	If you enable this policy setting, Windows requires users to include at least one uppercase letter in their PIN.

The setting of the **Windows Hello** group:

Name	Description
Allow enumeration of emulated smart card for all users	Windows prevents users on the same computer from enumerating provisioned Windows Hello for Business credentials for other users. If you enable this setting, Windows allows all users of the computer to enumerate all Windows Hello for Business credentials, but still require each user to provide their own factors for authentication.
Device unlock factors A	First unlock factor credential providers
Device unlock factors B	Second unlock factor credential providers
Device unlock rules	Signal rules for device unlock
Dynamic lock factors	If you enable this setting, these signal rules will be evaluated to detect user absence and automatically lock the device.
Dynamic lock rules	Signal rules for dynamic lock
Turn off smart card emulation	If you enable this setting, Windows Hello for Business provisions Windows Hello for Business credentials that are not compatible with smart card applications.
Use a hardware security device	If you enable this setting, Windows Hello for Business provisioning only occurs on devices with usable 1.2 or 2.0 TPMs. You can optionally exclude security devices, which prevents Windows Hello for Business provisioning from using those devices.
Do not use the tpm1.2 security devices	Exclude TPM 1.2 security devices.|
Use biometrics	If you enable or do not configure this setting, Windows Hello for Business allows the use biometric gestures.
Use certificate for on-premises authentication	If you enable this setting, Windows Hello for Business enrolls a sign-in certificate that is used for on-premises authentication.
Use PIN Recovery	If you enable this setting, Windows Hello for Business uses the PIN recovery service.
Use Windows Hello for Business certificates as smart card certificates	If you enable this setting, applications use Windows Hello for Business certificates as smart card certificates. Biometric factors are unavailable when a user is asked to

	authorize the use of the certificate's private key.
Use Windows Hello for Business	If you enable this setting, the device provisions Windows Hello for Business using keys or certificates for all users.
Do not start Windows Hello provisioning after sign-in	If you enable this setting, Windows Hello for Business does not automatically start provisioning after the user has signed in.

The setting of the **TPM** group:

Name	Description
The level of TPM owner authorization information available to the operating system	This policy setting configures how much of the TPM owner authorization information is stored in the registry of the local computer. Depending on the amount of TPM owner authorization information stored locally, the operating system and TPM-based applications can perform certain TPM actions which require TPM owner authorization without requiring the user to enter the TPM owner password. You can choose to have the operating system store either the full TPM owner authorization value, the TPM administrative delegation blob plus the TPM user delegation blob, or none. If you enable this policy setting, Windows will store the TPM owner authorization in the registry of the local computer according to the operating system managed TPM authentication setting you choose.
Configure the system to clear the TPM if it is not in a ready state.	This policy setting configures the system to prompt the user to clear the TPM if the TPM is detected to be in any state other than Ready. This policy will take effect only if the system's TPM is in a state other than Ready, including if the TPM is "Ready, with reduced functionality". The prompt to clear the TPM will start occurring after the next reboot, upon user login only if the logged in user is part of the Administrators group for the system. The prompt can be dismissed, but will reappear after every reboot and login until the policy is disabled or until the TPM is in a Ready state.
Configure the system to use legacy Dictionary Attack Prevention Parameters setting for TPM 2.0	This policy setting configures the TPM to use the Dictionary Attack Prevention Parameters (lockout threshold and recovery time) to the values that were used for Windows 10 Version 1607 and below. Setting this policy will take effect only if a) the TPM was originally prepared using a version of Windows after Windows 10 Version 1607 and b) the System has a TPM 2.0. Note that enabling this policy will only take effect after the TPM maintenance task runs (which typically happens after a system restart). Once this policy has been enabled on a system and has taken effect (after a system restart), disabling it will have no impact and the system's TPM will remain configured using the legacy Dictionary Attack Prevention parameters, regardless of the value of this group policy. The only way for the disabled setting of this policy to take effect on a system where it was once enabled is to a) disable it from group policy and b)clear the TPM on the system.
Ignore the default list of blocked TPM commands	If you enable this policy setting, Windows will ignore the computer's default list of blocked TPM commands and will only block those TPM commands specified by Group Policy or the local list.
Ignore the local list of blocked TPM commands	If you enable this policy setting, Windows will ignore the computer's local list of blocked TPM commands and will only block those TPM commands specified by Group Policy or the default list.
Standard User Individual Lockout Threshold	This policy setting allows you to manage the maximum number of authorization failures for each standard user for the Trusted Platform Module (TPM). If the number of authorization failures for the user within the duration for Standard User Lockout Duration equals this value, the standard user is prevented from sending commands to the Trusted Platform Module (TPM) that require authorization. This setting helps administrators prevent the TPM hardware from entering a lockout mode because it slows the speed standard users can send commands requiring authorization to the TPM. If this value is not configured, a default value of 4 is used.

Standard User Lockout Duration	This policy setting allows you to manage the duration in minutes for counting standard user authorization failures for Trusted Platform Module (TPM) commands requiring authorization. If the number of TPM commands with an authorization failure within the duration equals a threshold, a standard user is prevented from sending commands requiring authorization to the TPM. If this value is not configured, a default value of 480 minutes (8 hours) is used.
Standard User Total Lockout Threshold	This policy setting allows you to manage the maximum number of authorization failures for all standard users for the Trusted Platform Module (TPM). If the total number of authorization failures for all standard users within the duration for Standard User Lockout Duration equals this value, all standard users are prevented from sending commands to the Trusted Platform Module (TPM) that require authorization. This setting helps administrators prevent the TPM hardware from entering a lockout mode because it slows the speed standard users can send commands requiring authorization to the TPM. If this value is not configured, a default value of 9 is used.
Turn on TPM backup to Active Directory Domain Services (1 of 2)|	If you enable this option along with one below, TPM owner information will be automatically and silently backed up to AD DS when you use Windows to set or change a TPM owner password.
Turn on TPM backup to Active Directory Domain Services (2 of 2)|	If you enable this option along with one above, TPM owner information will be automatically and silently backed up to AD DS when you use Windows to set or change a TPM owner password.

The setting of the **Local security** group:

Name	Description
Accounts: Limit local account use of blank passwords to console logon only	This security setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If enabled, local accounts that are not password protected will only be able to log on at the computer's keyboard.
Audit: Audit the access of global system objects	This security setting determines whether to audit the access of global system objects. If this policy is enabled, it causes system objects, such as mutexes, events, semaphores and DOS devices, to be created with a default system access control list (SACL). Only named objects are given a SACL; SACLs are not given to objects without names. If the Audit object access audit policy is also enabled, access to these system objects is audited.
Audit: Audit the use of Backup and Restore privilege	This security setting determines whether to audit the use of all user privileges, including Backup and Restore, when the Audit privilege use policy is in effect. Enabling this option when the Audit privilege use policy is also enabled generates an audit event for every file that is backed up or restored.0 - Disabled, 1 - Enabled
Audit: Force audit policy subcategory settings to override audit policy category settings	Windows Vista and later versions of Windows allow audit policy to be managed in a more precise way using audit policy subcategories. Setting audit policy at the category level will override the new subcategory audit policy feature. Group Policy only allows audit policy to be set at the category level, and existing group policy may override the subcategory settings of new machines as they are joined to the domain or upgraded to Windows Vista or later versions. To allow audit policy to be managed using subcategories without requiring a change to Group Policy, there is a new registry value in Windows Vista and later versions, SCENoApplyLegacyAuditPolicy, which prevents the application of category-level audit policy from Group Policy and from the Local Security Policy administrative tool.
Audit: Shut down system immediately if unable to log security audits	This security setting determines whether the system shuts down if it is unable to log security events. If this security setting is enabled, it causes the system to stop if a security audit cannot be logged for any reason. Typically, an event fails to be logged

	when the security audit log is full and the retention method that is specified for the security log is either Do Not Overwrite Events or Overwrite Events by Days.
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	This policy setting determines which users or groups can access DCOM application remotely or locally. This setting is used to control the attack surface of the computer for DCOM applications.
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	This policy setting determines which users or groups can launch or activate DCOM applications remotely or locally. This setting is used to control the attack surface of the computer for DCOM applications
Devices: Allow undock without having to log on	This security setting determines whether a portable computer can be undocked without having to log on. If this policy is enabled, logon is not required and an external hardware eject button can be used to undock the computer. If disabled, a user must log on and have the Remove computer from docking station privilege to undock the computer.
Devices: Allowed to format and eject removable media	This security setting determines who is allowed to format and eject removable NTFS media. 0 - Only administrators of the computer, 1 - Only administrators and power users, 2 - Only administrators and the local current user.
Devices: Prevent users from installing printer drivers	For a computer to print to a shared printer, the driver for that shared printer must be installed on the local computer. This security setting determines who is allowed to install a printer driver as part of connecting to a shared printer. If this setting is enabled, only Administrators can install a printer driver as part of connecting to a shared printer. If this setting is disabled, any user can install a printer driver as part of connecting to a shared printer.
Devices: Restrict CD-ROM access to locally logged-on user only	This security setting determines whether a CD-ROM is accessible to both local and remote users simultaneously. If this policy is enabled, it allows only the interactively logged-on user to access removable CD-ROM media. If this policy is enabled and no one is logged on interactively, the CD-ROM can be accessed over the network. 1- Enabled, 2 - Disabled.
Devices: Restrict floppy access to locally logged-on user only	This security setting determines whether removable floppy media are accessible to both local and remote users simultaneously. If this policy is enabled, it allows only the interactively logged-on user to access removable floppy media. 1- Enabled, 2 - Disabled.
Devices: Unsigned driver installation behavior	This security setting determines what happens when an attempt is made to install a device driver (by means of Setup API) that has not been tested by the Windows Hardware Quality Lab (WHQL).The options are: 0 - Silently succeed, 1- Warn but allow installation, 2 - Do not allow installation
Domain controller: Allow server operators to schedule tasks	This security setting determines if Server Operators are allowed to submit jobs by means of the AT schedule facility.
Domain controller: LDAP server signing requirements	This security setting determines whether the LDAP server requires signing to be negotiated with LDAP clients.
Domain controller: Refuse machine account password changes	This security setting determines whether domain controllers will refuse requests from member computers to change computer account passwords. By default, member computers change their computer account passwords every 30 days. If enabled, the domain controller will refuse computer account password change requests.
Domain member: Digitally encrypt or sign secure channel data (always)	This security setting determines whether all secure channel traffic initiated by the domain member must be signed or encrypted.
Domain member: Digitally encrypt secure channel data (when possible)	This security setting determines whether a domain member attempts to negotiate encryption for all secure channel traffic that it initiates.

Domain member: Digitally sign secure channel data (when possible)	This security setting determines whether a domain member attempts to negotiate signing for all secure channel traffic that it initiates.
Domain member: Disable machine account password changes	Determines whether a domain member periodically changes its computer account password. If this setting is enabled, the domain member does not attempt to change its computer account password. If this setting is disabled, the domain member attempts to change its computer account password as specified by the setting for Domain Member: Maximum age for machine account password, which by default is every 30 days.
Domain member: Require strong (Windows 2000 or later) session key	This security setting determines whether 128-bit key strength is required for encrypted secure channel data.
Interactive logon: Do not display last user name	This security setting determines whether the name of the last user to log on to the computer is displayed in the Windows logon screen. If this policy is enabled, the name of the last user to successfully log on is not displayed in the Logon Screen.
Interactive Logon: Display user information when session is locked	Interactive Logon: Display user information when session is locked.
Interactive logon: Do not require CTRL+ALT+DEL	This security setting determines whether pressing CTRL+ALT+DEL is required before a user can log on.
Interactive logon: Message text for users attempting to logon	This security setting specifies a text message that is displayed to users when they log on. This text is often used for legal reasons, for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.
Interactive logon: Message title for users attempting to logon	This security setting allows the specification of a title to appear in the title bar of the window that contains the Interactive logon: Message text for users attempting to log on.
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	All previous users' logon information is cached locally so that, in the event that a domain controller is unavailable during subsequent logon attempts, they are able to log on. In this policy setting, a value of 0 disables logon caching. Any value above 50 only caches 50 logon attempts.
Interactive logon: Prompt user to change password before expiration	Determines how far in advance (in days) users are warned that their password is about to expire. With this advance warning, the user has time to construct a password that is sufficiently strong.
Interactive logon: Require Domain Controller authentication to unlock workstation	Logon information must be provided to unlock a locked computer. For domain accounts, this security setting determines whether a domain controller must be contacted to unlock a computer. If this setting is disabled, a user can unlock the computer using cached credentials. If this setting is enabled, a domain controller must authenticate the domain account that is being used to unlock the computer.
Interactive logon: Require smart card	This security setting requires users to log on to a computer using a smart card.
Interactive logon: Smart card removal behavior	This security setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. 0 - No Action, 1 - Lock workstation, 2 - Force logoff, 3 - Disconnect if a remote Remote Desktop Services session
Microsoft network client: Digitally sign communications (always)	This security setting determines whether packet signing is required by the SMB client component. The server message block (SMB) protocol provides the basis for Microsoft file and print sharing and many other networking operations, such as remote Windows administration. To prevent man-in-the-middle attacks that modify SMB packets in transit, the SMB protocol supports the digital signing of SMB packets. This policy setting determines whether SMB packet signing must be negotiated before further communication with an SMB server is permitted.

Microsoft network client: Digitally sign communications (if server agrees)	This security setting determines whether the SMB client attempts to negotiate SMB packet signing. The server message block (SMB) protocol provides the basis for Microsoft file and print sharing and many other networking operations, such as remote Windows administration. To prevent man-in-the-middle attacks that modify SMB packets in transit, the SMB protocol supports the digital signing of SMB packets. This policy setting determines whether the SMB client component attempts to negotiate SMB packet signing when it connects to an SMB server.
Microsoft network client: Send unencrypted password to third-party SMB servers	If this security setting is enabled, the Server Message Block (SMB) redirector is allowed to send plaintext passwords to non-Microsoft SMB servers that do not support password encryption during authentication.
Microsoft network server: Amount of idle time required before suspending session	This security setting determines the amount of continuous idle time (in minutes) that must pass in a Server Message Block (SMB) session before the session is suspended due to inactivity. Administrators can use this policy to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished.
Microsoft network server: Digitally sign communications (always)	This security setting determines whether packet signing is required by the SMB server component. The server message block (SMB) protocol provides the basis for Microsoft file and print sharing and many other networking operations, such as remote Windows administration. To prevent ""man-in-the-middle"" attacks that modify SMB packets in transit, the SMB protocol supports the digital signing of SMB packets. This policy setting determines whether SMB packet signing must be negotiated before further communication with an SMB client is permitted.
Microsoft network server: Digitally sign communications (if client agrees)	This security setting determines whether the SMB server will negotiate SMB packet signing with clients that request it. The server message block (SMB) protocol provides the basis for Microsoft file and print sharing and many other networking operations, such as remote Windows administration. To prevent man-in-the-middle attacks that modify SMB packets in transit, the SMB protocol supports the digital signing of SMB packets. This policy setting determines whether the SMB server will negotiate SMB packet signing when an SMB client requests it.
Microsoft network server: Disconnect clients when logon hours expire	This security setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component.
Microsoft network server: Server SPN target name validation level	The server message block (SMB) protocol provides the basis for file and printer sharing and many other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2.
Network access: Do not allow anonymous enumeration of SAM accounts	This security setting determines what additional permissions will be granted for anonymous connections to the computer. Windows allows anonymous users to perform certain activities, such as enumerating the names of domain accounts and network shares. This is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust.
Network access: Do not allow anonymous enumeration of SAM accounts and shares	This security setting determines whether anonymous enumeration of SAM accounts and shares is allowed. Windows allows anonymous users to perform certain activities, such as enumerating the names of domain accounts and network shares. This is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust.
Network access: Do not allow storage of passwords	This security setting determines whether Stored User Names and Passwords saves passwords, credentials, or .NET Passports for later use when it gains domain

and credentials for network authentication	authentication. If it is enabled, this setting prevents the Stored User Names and Passwords from storing passwords and credentials.
Network access: Let Everyone permissions apply to anonymous users	This security setting determines what additional permissions are granted for anonymous connections to the computer.
Network access: Named Pipes that can be accessed anonymously	This security setting determines which communication sessions (pipes) will have attributes and permissions that allow anonymous access.
Network access: Remotely accessible registry paths	This security setting determines which registry keys can be accessed over the network, regardless of the users or groups listed in the access control list (ACL) of the winreg registry key.
Network access: Remotely accessible registry paths and sub-paths	This security setting determines which registry paths and subpaths can be accessed over the network, regardless of the users or groups listed in the access control list (ACL) of the winreg registry key.
Network access: Shares that can be accessed anonymously	This security setting determines which network shares can accessed by anonymous users.
Network access: Sharing and security model for local accounts	This security setting determines how network logons that use local accounts are authenticated. If this setting is set to Classic, network logons that use local account credentials authenticate by using those credentials. The Classic model allows fine control over access to resources. By using the Classic model, you can grant different types of access to different users for the same resource.
Network security: Do not store LAN Manager hash value on next password change	This security setting determines if, at the next password change, the LAN Manager (LM) hash value for the new password is stored. The LM hash is relatively weak and prone to attack, as compared with the cryptographically stronger Windows NT hash. Since the LM hash is stored on the local computer in the security database the passwords can be compromised if the security database is attacked.
Network security: LAN Manager authentication level	This security setting determines which challenge/response authentication protocol is used for network logons.
Network security: LDAP client signing requirements	This security setting determines the level of data signing that is requested on behalf of clients issuing LDAP BIND requests.
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	This security setting allows a client to require the negotiation of 128-bit encryption and/or NTLMv2 session security. These values are dependent on the LAN Manager Authentication Level security setting value.
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	This security setting allows a server to require the negotiation of 128-bit encryption and/or NTLMv2 session security. These values are dependent on the LAN Manager Authentication Level security setting value.
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	This policy setting allows you to deny or audit outgoing NTLM traffic from this Windows 7 or this Windows Server 2008 R2 computer to any Windows remote server.
Network security: Restrict NTLM: Incoming NTLM traffic	This policy setting allows you to deny or allow incoming NTLM traffic.
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	This policy setting allows you to audit incoming NTLM traffic.
Network security: Restrict NTLM: NTLM authentication in this domain	This policy setting allows you to deny or allow NTLM authentication within a domain from this domain controller. This policy does not affect interactive logon to this domain controller.

Network security: Restrict NTLM: Audit NTLM authentication in this domain	This policy setting allows you to audit NTLM authentication in a domain from this domain controller.
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	This policy setting allows you to create an exception list of remote servers to which clients are allowed to use NTLM authentication if the "Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers" policy setting is configured.
Network security: Restrict NTLM: Add server exceptions in this domain	This policy setting allows you to create an exception list of servers in this domain to which clients are allowed to use NTLM pass-through authentication if the "Network Security: Restrict NTLM: Deny NTLM authentication in this domain" is set.
Network security: Allow LocalSystem NULL session fallback	Allow NTLM to fall back to NULL session when used with LocalSystem.
Network security: Allow PKU2U authentication requests to this computer to use online identities	This policy will be turned off by default on domain joined machines. This would disallow the online identities to be able to authenticate to the domain joined machine in Windows 7.
Network security: Configure encryption types allowed for Kerberos	This policy setting allows you to set the encryption types that Kerberos is allowed to use. If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications.
Recovery console: Allow automatic administrative logon	This security setting determines if the password for the Administrator account must be given before access to the system is granted. If this option is enabled, the Recovery Console does not require you to provide a password, and it automatically logs on to the system.
Recovery console: Allow floppy copy and access to all drives and all folders	Enabling this security option makes the Recovery Console SET command available, which allows you to set the following Recovery Console environment variables.
Shutdown: Allow system to be shut down without having to log on	This security setting determines whether a computer can be shut down without having to log on to Windows. When this policy is enabled, the Shut Down command is available on the Windows logon screen.
Shutdown: Clear virtual memory pagefile	This security setting determines whether the virtual memory pagefile is cleared when the system is shut down.
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	For the Schannel Security Service Provider (SSP), this security setting disables the weaker Secure Sockets Layer (SSL) protocols and supports only the Transport Layer Security (TLS) protocols as a client and as a server (if applicable). If this setting is enabled, Transport Layer Security/Secure Sockets Layer (TLS/SSL) Security Provider uses only the FIPS 140 approved cryptographic algorithms: 3DES and AES for encryption, RSA or ECC public key cryptography for the TLS key exchange and authentication, and only the Secure Hashing Algorithm (SHA1, SHA256, SHA384, and SHA512) for the TLS hashing requirements.
System cryptography: Force strong key protection for user keys stored on the computer	This security setting determines if users' private keys require a password to be used.
System objects: Default owner for objects created by members of the Administrators group	This security setting determines which security principal (SID) will be assigned the OWNER of objects when the object is created by a member of the Administrators Group.
System objects: Require case insensitivity for non-Windows subsystems	This security setting determines whether case insensitivity is enforced for all subsystems. The Win32 subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as POSIX.

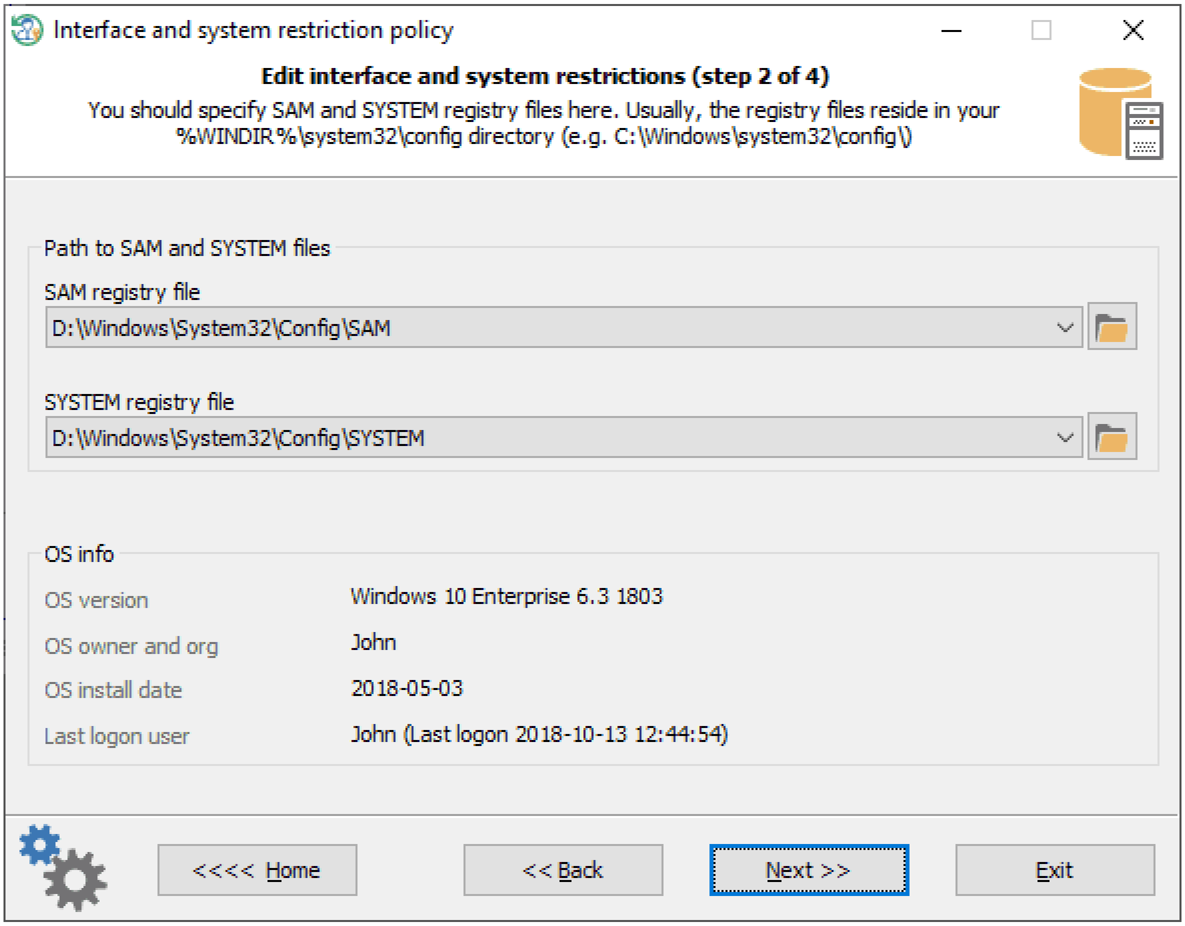
System objects: Strengthen default permissions of internal system objects (e.g., Symbolic Links)	This security setting determines the strength of the default discretionary access control list (DACL) for objects.
System settings: Optional subsystems	This security setting determines which subsystems can optionally be started up to support your applications. With this security setting, you can specify as many subsystems to support your applications as your environment demands.
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	This security setting determines if digital certificates are processed when a user or process attempts to run software with an .exe file name extension. This security settings is used to enable or disable certificate rules, a type of software restriction policies rule. With software restriction policies, you can create a certificate rule that will allow or disallow software that is signed by Authenticode to run, based on the digital certificate that is associated with the software. In order for certificate rules to take effect, you must enable this security setting.
User Account Control: Admin Approval Mode for the Built-in Administrator account	This security setting determines the behavior of Admin Approval mode for the Built-in Administrator account.
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	This security setting determines the behavior of the elevation prompt for administrators.
User Account Control: Behavior of the elevation prompt for standard users	This security setting determines the behavior of the elevation prompt for standard users.
User Account Control: Detect application installations and prompt for elevation	This security setting determines the behavior of application installation detection for the entire system.
User Account Control: Only elevate executables that are signed and validated	This security setting will enforce PKI signature checks on any interactive application that requests elevation of privilege. Enterprise administrators can control the admin application allowed list thru the population of certificates in the local computers Trusted Publisher Store.
User Account Control: Only elevate UIAccess applications that are installed in secure locations	This security setting will enforce the requirement that applications that request execution with a UIAccess integrity level (via a marking of UIAccess=true in their application manifest), must reside in a secure location on the file system.
User Account Control: Run all administrators in Admin Approval Mode	This security setting determines the behavior of all UAC policies for the entire system.
User Account Control: Switch to the secure desktop when prompting for elevation	This security setting determines whether the elevation request will prompt on the interactive users desktop or the Secure Desktop.
User Account Control: Virtualize file and registry write failures to per-user locations	This security setting enables the redirection of legacy application write failures to defined locations in both the registry and file system. This feature mitigates those applications that historically ran as administrator and wrote runtime application data back to either %ProgramFiles%, %Windir%; %Windir%\system32 or HKLM\Software\....
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	This security setting controls whether User Interface Accessibility (UIAccess or UIA) programs can automatically disable the secure desktop for elevation prompts being used by a standard user. If you enable this setting, UIA programs including Windows Remote Assistance can automatically disable the secure desktop for elevation

	prompts. Unless you have also disabled elevation prompts, the prompts will appear on the interactive user's desktop instead of the secure desktop.

3.2.5 Interface and system restriction policy

You can use this feature to change or reset different interface and system restrictions for the selected user. For example, allow/disallow access to specific Windows applications, lock/unlock the Run Dialog box, enable/disable certain control panel settings, allow/prevent access to the command prompt or the Windows registry, allow/prohibit access to CD-ROM or removable disks, etc.

Choosing Windows registry files



Interface and system restriction policy

Edit interface and system restrictions (step 2 of 4)

You should specify SAM and SYSTEM registry files here. Usually, the registry files reside in your %WINDIR%\system32\config directory (e.g. C:\Windows\system32\config\)

Path to SAM and SYSTEM files

SAM registry file: D:\Windows\System32\Config\SAM

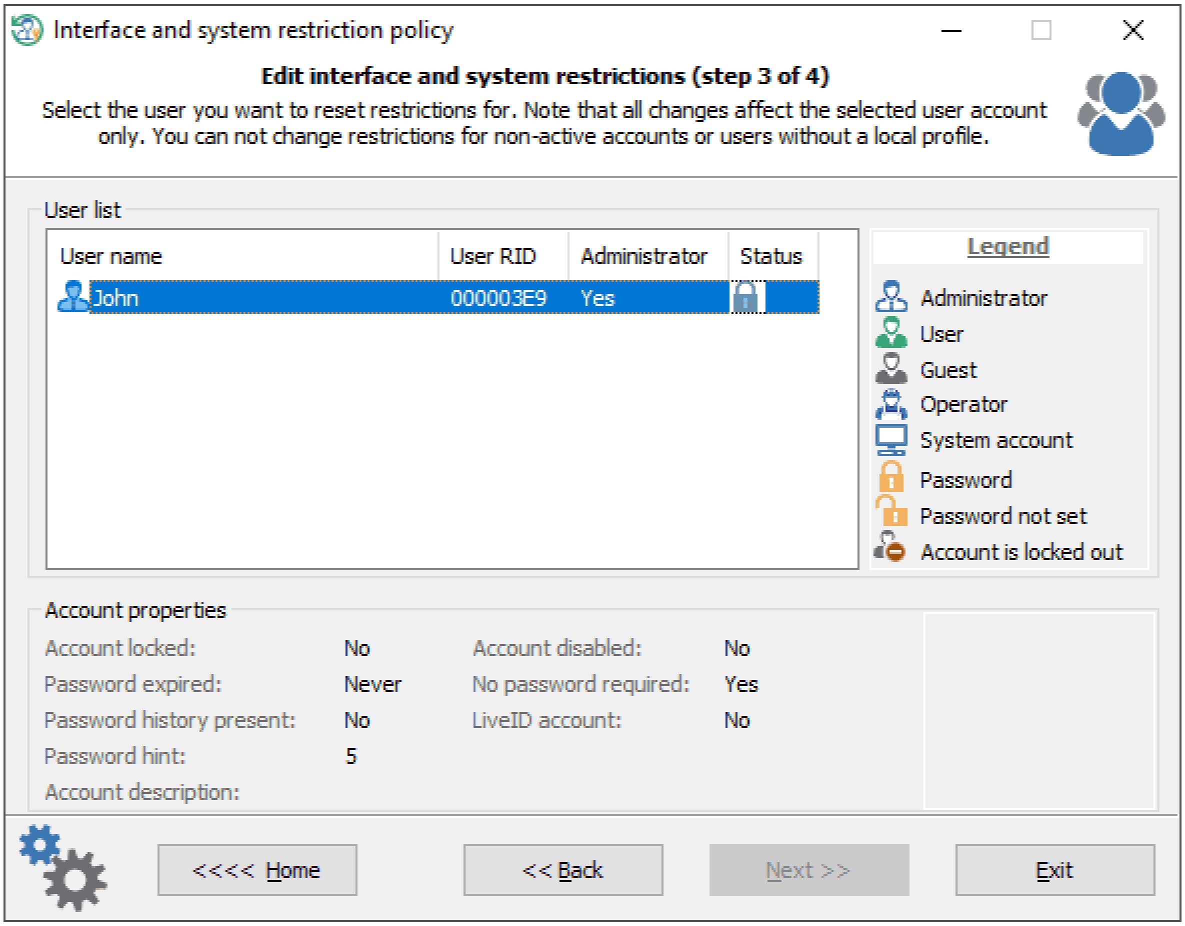
SYSTEM registry file: D:\Windows\System32\Config\SYSTEM

OS info

OS version	Windows 10 Enterprise 6.3 1803
OS owner and org	John
OS install date	2018-05-03
Last logon user	John (Last logon 2018-10-13 12:44:54)

Choose the SAM and SYSTEM registry files found by the program, or specify the path to them manually.

Selecting user account



Interface and system restriction policy

Edit interface and system restrictions (step 3 of 4)

Select the user you want to reset restrictions for. Note that all changes affect the selected user account only. You can not change restrictions for non-active accounts or users without a local profile.

User list

User name	User RID	Administrator	Status
John	000003E9	Yes	🔒

Legend

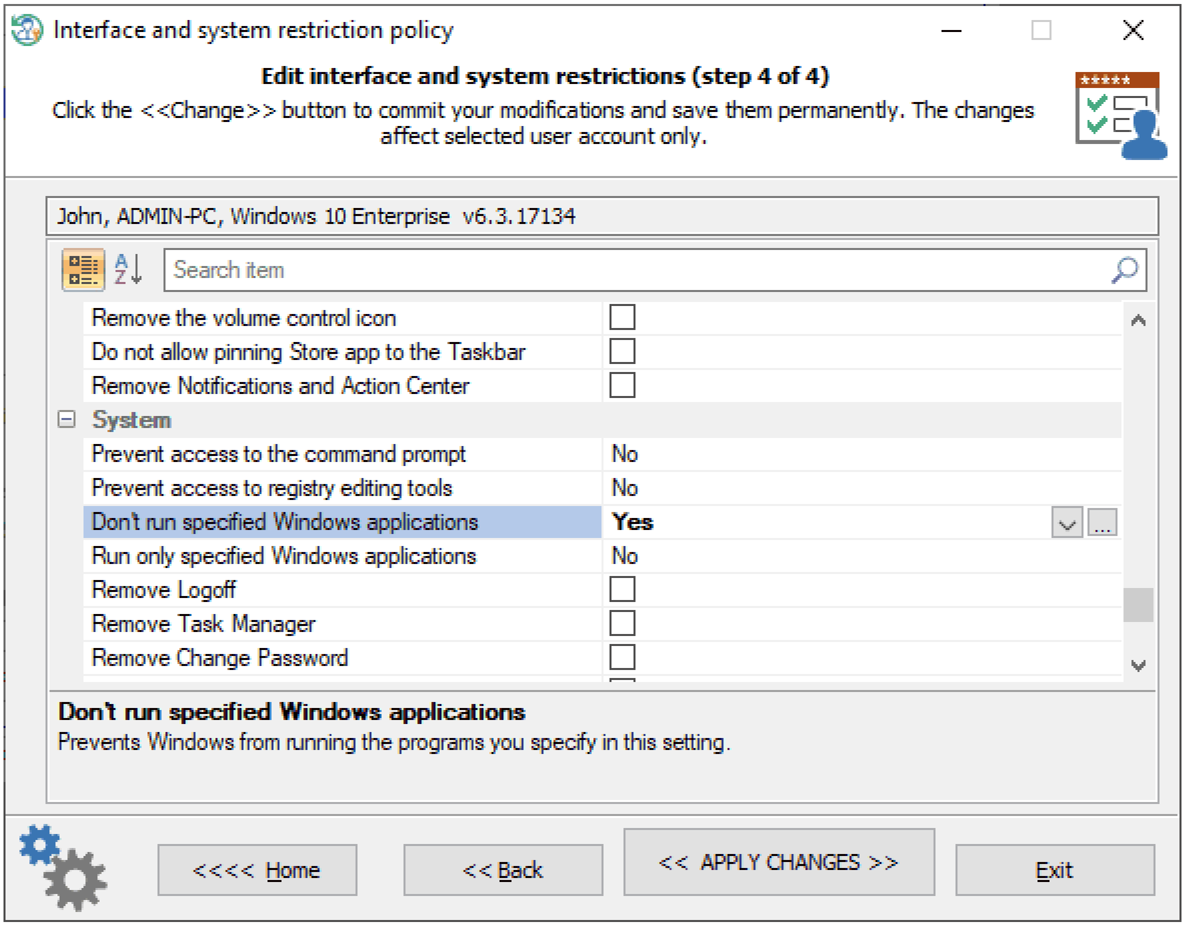
- Administrator
- User
- Guest
- Operator
- System account
- Password
- Password not set
- Account is locked out

Account properties

Account locked:	No	Account disabled:	No
Password expired:	Never	No password required:	Yes
Password history present:	No	LiveID account:	No
Password hint:	5		
Account description:			

Select the user you want to change or reset the restrictions for. The program displays only active accounts that have a local profile.

Changing interface and system restrictions for selected user



Interface and system restriction policy

Edit interface and system restrictions (step 4 of 4)

Click the <<Change>> button to commit your modifications and save them permanently. The changes affect selected user account only.

John, ADMIN-PC, Windows 10 Enterprise v6.3.17134

Remove the volume control icon	□
Do not allow pinning Store app to the Taskbar	□
Remove Notifications and Action Center	□
System	
Prevent access to the command prompt	No
Prevent access to registry editing tools	No
Don't run specified Windows applications	**Yes**
Run only specified Windows applications	No
Remove Logoff	□
Remove Task Manager	□
Remove Change Password	□

Don't run specified Windows applications

Prevents Windows from running the programs you specify in this setting.

Once the user is selected, you can alter the interface and system options available for the user account. Click the << *APPLY CHANGES* >> button to commit the changes.

The options affect selected user account only.

Short description of the interface and system options.

Control panel restrictions:

Name	Description
Hide specified Control Panel items	This option allows you to display or hide specified Control Panel items, such as Mouse, System, or Personalization, from the Control Panel window and the Start screen. The option affects the Start screen and Control Panel window, as well as other ways to access Control Panel items, such as shortcuts in Help and Support or command lines that use control.exe. This policy has no effect on items displayed in PC settings. If you enable this setting, you can select specific items not to display on the Control Panel window and the Start screen.
Show only specified Control Panel items	This option controls which Control Panel items such as Mouse, System, or Personalization, are displayed on the Control Panel window and the Start screen. The only items displayed in Control Panel are those you specify in this setting. This option affects the Start screen and Control Panel, as well as other ways to access Control Panel items such as shortcuts in Help and Support or command lines that use control.exe. This policy has no effect on items displayed in PC settings. For example, enter Microsoft.Mouse, Microsoft.System, or Microsoft.Personalization.

Prohibit access to Control Panel and PC settings	Disables all Control Panel programs and the PC settings app. This option prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.
Settings Page Visibility	Specifies the list of pages to show or hide from the System Settings app. This policy allows an administrator to block a given set of pages from the System Settings app. Blocked pages will not be visible in the app, and if all pages in a category are blocked the category will be hidden as well. Example: showonly:about,bluetooth hide:bluetooth
Disable the Display Control Panel	If you enable this setting, the Display Control Panel does not run. When users try to start Display, a message appears explaining that a setting prevents the action.
Hide Settings tab	Removes the Settings tab from Display in Control Panel
Prevent changing theme	This option disables the theme gallery in the Personalization Control Panel.
Prevent changing visual style for windows and buttons	Prevents users or applications from changing the visual style of the windows and buttons displayed on their screens.
Enable screen saver	If you disable this setting, screen savers do not run. Also, this option disables the Screen Saver section of the Screen Saver dialog in the Personalization or Display Control Panel. As a result, users cannot change the screen saver options.
Prevent changing color and appearance	Disables the Color (or Window Color) page in the Personalization Control Panel, or the Color Scheme dialog in the Display Control Panel on systems where the Personalization feature is not available. This option prevents users from using Control Panel to change the window border and taskbar color (on Windows 8), glass color (on Windows Vista and Windows 7), system colors, or color scheme of the desktop and windows.
Prevent changing desktop background	Prevents users from adding or changing the background design of the desktop. If you enable this setting, none of the Desktop Background settings can be changed by the user.
Prevent changing desktop icons	Prevents users from changing the desktop icons. If you enable this setting, none of the desktop icons can be changed by the user.
Prevent changing mouse pointers	If you enable this setting, none of the mouse pointer scheme settings can be changed by the user.
Prevent changing screen saver	This option prevents users from using Control Panel to add, configure, or change the screen saver on the computer. It does not prevent a screen saver from running.
Prevent changing sounds	If you enable this setting, none of the Sound Scheme settings can be changed by the user.
Password protect the screen saver	If you enable this setting, all screen savers are password protected. If you disable this setting, password protection cannot be set on any screen saver.
Browse the network to find printers	Allows users to use the Add Printer Wizard to search the network for shared printers.
Browse a common web site to find printers	Adds a link to an Internet or intranet Web page to the Add Printer Wizard.
Turn off Windows default printer management	This preference allows you to change default printer management. If you enable this setting, Windows will not manage the default printer.
Prevent addition of printers	Prevents users from using familiar methods to add local and network printers. If this option is enabled, it removes the Add Printer option from the Start menu. (To find the Add Printer option, click Start, click Printers, and then click Add Printer.) This option also removes Add Printer from the Printers folder in Control Panel.
Prevent deletion of printers	If this option is enabled, it prevents users from deleting local and network printers. If a user tries to delete a printer, such as by using the Delete option in Printers in Control Panel, a message appears explaining that a setting prevents the action.

Hide "Set Program Access and Computer Defaults" page	This option removes the Set Program Access and Defaults page from the Programs Control Panel. As a result, users cannot view or change the associated page.
Hide "Get Programs" page	Prevents users from viewing or installing published programs from the network. If this option is enabled, users cannot view the programs that have been published by the system administrator, and they cannot use the "Get Programs" page to install published programs. Enabling this feature does not prevent users from installing programs by using other methods. Users will still be able to view and installed assigned (partially installed) programs that are offered on the desktop or on the Start menu.
Hide "Installed Updates" page	This option prevents users from accessing "Installed Updates" page from the "View installed updates" task.
Hide "Programs and Features" page	This option prevents users from accessing "Programs and Features" to view, uninstall, change, or repair programs that are currently installed on the computer.
Hide the Programs Control Panel	This option prevents users from using the Programs Control Panel in Category View and Programs and Features in Classic View.
Hide "Windows Features"	This option prevents users from accessing the "Turn Windows features on or off" task from the Programs Control Panel in Category View, Programs and Features in Classic View, and Get Programs. As a result, users cannot view, enable, or disable various Windows features and services.
Hide "Windows Marketplace"	This option prevents users from access the "Get new programs from Windows Marketplace" task from the Programs Control Panel in Category View, Programs and Features in Classic View, and Get Programs.
Hide Regional and Language Options administrative options	This option removes the Administrative options from the Region settings control panel. Administrative options include interfaces for setting system locale and copying settings to the default user. This option does not, however, prevent an administrator or another application from changing these values programmatically.
Hide the geographic location option	This option removes the option to change the user's geographical location (GeoID) from the Region settings control panel.
Hide the select language group options	This option removes the option to change the user's menus and dialogs (UI) language from the Language and Regional Options control panel.
Hide user locale selection and customization options	This option removes the regional formats interface from the Region settings control panel.

Desktop restrictions:

Name	Description
Hide Network Locations icon on desktop	Removes the Network Locations icon from the desktop.
Remove the Desktop Cleanup Wizard	Prevents users from using the Desktop Cleanup Wizard.
Remove Computer icon on the desktop	This option hides Computer from the desktop and from the new Start menu. It also hides links to Computer in the Web view of all Explorer windows, and it hides Computer in the Explorer folder tree pane. If the user navigates into Computer via the "Up" button while this option is enabled, they view an empty Computer folder. This option allows administrators to restrict their users from seeing Computer in the shell namespace, allowing them to present their users with a simpler desktop environment.
Remove Properties from the Documents icon context menu	This option hides the Properties menu command on the shortcut menu for the My Documents icon.

Prevent adding, dragging, dropping and closing the Taskbar's toolbars	Prevents users from manipulating desktop toolbars. If you enable this setting, users cannot add or remove toolbars from the desktop. Also, users cannot drag toolbars on to or off of docked toolbars.
Remove Recycle Bin icon from desktop	Removes most occurrences of the Recycle Bin icon.
Hide Internet Explorer icon on desktop	Removes the Internet Explorer icon from the desktop and from the Quick Launch bar on the taskbar.
Hide and disable all items on the desktop	Removes icons, shortcuts, and other default and user-defined items from the desktop, including Briefcase, Recycle Bin, Computer, and Network Locations.
Remove Properties from the Recycle Bin context menu	Removes the Properties option from the Recycle Bin context menu.
Remove Properties from the Computer icon context menu	This option hides Properties on the context menu for Computer.
Hide Active Directory folder	Hides the Active Directory folder in Network Locations.
Prohibit adjusting desktop toolbars	Prevents users from adjusting the length of desktop toolbars. Also, users cannot reposition items or toolbars on docked toolbars.
Remove My Documents icon on the desktop	Removes most occurrences of the My Documents icon.
Enable Active Desktop	Enables Active Desktop and prevents users from disabling it.
Disable Active Desktop	Disables Active Desktop and prevents users from enabling it.
Prohibit changes	Prevents the user from enabling or disabling Active Desktop or changing the Active Desktop configuration.
Prohibit adding items	Prevents users from adding Web content to their Active Desktop.
Prohibit closing items	Prevents users from removing Web content from their Active Desktop.
Prohibit editing items	Prevents users from changing the properties of Web content items on their Active Desktop.
Prohibit deleting items	Prevents users from deleting Web content from their Active Desktop.
Disable all items	Removes Active Desktop content and prevents users from adding Active Desktop content.
Add/delete items	Adds and deletes specified Web content items.

Network restrictions:

Name	Description
Prohibit connecting and disconnecting a remote access connection	Determines whether users can connect and disconnect remote access connections.
Prohibit deletion of remote access connections	Determines whether users can delete remote access connections.
Prohibit renaming private remote access connections	Determines whether users can rename their private remote access connections.
Ability to rename all user remote access connections	Determines whether non-administrators can rename all-user remote access connections.
Prohibit access to the Remote Access Preferences item on the Advanced menu	Determines whether the Remote Access Preferences item on the Advanced menu in Network Connections folder is enabled.

Prohibit access to properties of a LAN connection	Determines whether users can change the properties of a LAN connection.
Prohibit TCP/IP advanced configuration	Determines whether users can configure advanced TCP/IP settings.
Prohibit access to the Advanced Settings item on the Advanced menu	Determines whether the Advanced Settings item on the Advanced menu in Network Connections is enabled for administrators.
Ability to rename LAN connections	Determines whether non-administrators can rename a LAN connection.
Prohibit adding and removing components for a LAN or remote access connection	Determines whether administrators can add and remove network components for a LAN or remote access connection. This option has no effect on non-administrators.
Ability to delete all user remote access connections	Determines whether users can delete all user remote access connections.
Prohibit changing properties of a private remote access connection	Determines whether users can view and change the properties of their private remote access connections.
Ability to change properties of an all user remote access connection	Determines whether a user can view and change the properties of remote access connections that are available to all users of the computer.
Prohibit access to properties of components of a remote access connection	Determines whether users can view and change the properties of components used by a private or all-user remote access connection.
Enable Windows 2000 Network Connections settings for Administrators	Determines whether settings that existed in Windows 2000 Server family will apply to Administrators.
Prohibit access to properties of components of a LAN connection	Determines whether Administrators and Network Configuration Operators can change the properties of components used by a LAN connection.
Ability to Enable/Disable a LAN connection	Determines whether users can enable/disable LAN connections.
Prohibit viewing of status for an active connection	Determines whether users can view the status for an active connection.
Ability to rename LAN connections or remote access connections available to all users	Determines whether users can rename LAN or all user remote access connections.
Prohibit Enabling/Disabling components of a LAN connection	Determines whether administrators can enable and disable the components used by LAN connections.
Prohibit access to the New Connection Wizard	Determines whether users can use the New Connection Wizard, which creates new network connections.
Prohibit user configuration of Offline Files	Prevents users from enabling, disabling, or changing the configuration of Offline Files.
Remove "Work offline" command	This option removes the "Work offline" command from Explorer, preventing users from manually changing whether Offline Files is in online mode or offline mode.
Remove "Make Available Offline" command	This option prevents users from making network files and folders available offline.
Prohibit access of the Windows Connect Now wizards	This option prohibits access to Windows Connect Now (WCN) wizards.

Start menu and taskbar restrictions:

Name	Description
Remove the "Undock PC" button from the Start Menu	If you enable this setting, the "Undock PC" button is removed from the simple Start Menu, and your PC cannot be undocked.
Remove user folder link from Start Menu	If you enable this option the start menu will not show a link to the user's storage folder.
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	This option prevents users from performing the following commands from the Start menu or Windows Security screen: Shut Down, Restart, Sleep, and Hibernate. This option does not prevent users from running Windows-based programs that perform these functions.
Remove user's folders from the Start Menu	Hides all folders on the user-specific (top) section of the Start menu. Other items appear, but folders are hidden.
Remove programs on Settings menu	This option allows you to remove programs on Settings menu. If you enable this setting, the Control Panel, Printers, and Network and Connection folders are removed from Settings on the Start menu, and from Computer and File Explorer. It also prevents the programs represented by these folders (such as Control.exe) from running.
Remove See More Results / Search Everywhere link	If you enable this policy, a "See more results" / "Search Everywhere" link will not be shown when the user performs a search in the start menu search box.
Remove Favorites menu from Start Menu	Prevents users from adding the Favorites menu to the Start menu or classic Start menu. If you enable this setting, the Display Favorites item does not appear in the Advanced Start menu options box.
Show QuickLaunch on Taskbar	This option controls whether the QuickLaunch bar is displayed in the Taskbar.
Add the Run command to the Start Menu	If you enable this setting, the Run command is added to the Start menu.
Remove Recorded TV link from Start Menu	This option allows you to remove the Recorded TV link from the Start Menu.
Disable context menus in the Start Menu	This allows you to prevent users from being able to open context menus in the Start Menu.
Remove All Programs list from the Start menu	If you enable this setting, the Start Menu will either collapse or remove the all apps list from the Start menu.
Lock the Taskbar	This option affects the taskbar, which is used to switch between running applications.
Hide the notification area	This option affects the notification area (previously called the "system tray") on the taskbar.
Remove Clock from the system notification area	Prevents the clock in the system notification area from being displayed.
Show "Run as different user" command on Start	This option shows or hides the "Run as different user" command on the Start application bar.
Remove access to the context menus for the taskbar	This option allows you to remove access to the context menus for the taskbar.
Remove Run menu from Start Menu	Allows you to remove the Run command from the Start menu, Internet Explorer, and Task Manager.
Remove Documents icon from Start Menu	This option allows you to remove the Documents icon from the Start menu and its submenus.
Remove the People Bar from the taskbar	This allows you to remove the People Bar from the taskbar and disables the My People experience.

Remove Help menu from Start Menu	This option allows you to remove the Help command from the Start menu.
Prevent changes to Taskbar and Start Menu Settings	This option allows you to prevent changes to Taskbar and Start Menu Settings.
Remove Downloads link from Start Menu	This option allows you to remove the Downloads link from the Start Menu.
Remove Videos link from Start Menu	This option allows you to remove the Videos link from the Start Menu.
Remove frequent programs list from the Start Menu	If you enable this setting, the frequently used programs list is removed from the Start menu.
Remove Games link from Start Menu	If you enable this option the start menu will not show a link to the Games folder.
Remove Search link from Start Menu	This option allows you to remove the Search link from the Start menu, and disables some File Explorer search elements. Note that this does not remove the search box from the new style Start menu.
Prevent users from customizing their Start Screen	This option allows you to prevent users from changing their Start screen layout.
Remove common program groups from Start Menu	Removes items in the All Users profile from the Programs menu on the Start menu.
Prevent users from uninstalling applications from Start	If you enable this setting, users cannot uninstall apps from Start.
Remove Network Connections from Start Menu	This option allows you to remove Network Connections from the Start Menu.
Remove pinned programs list from the Start Menu	If you enable this setting, the "Pinned Programs" list is removed from the Start menu. Users cannot pin programs to the Start menu.
Add Logoff to the Start Menu	This option only applies to the classic version of the start menu and does not affect the new style start menu.
Remove Default Programs link from the Start menu	This option allows you to remove the Default Programs link from the Start menu.
Remove Recent Items menu from Start Menu	Removes the Recent Items menu from the Start menu. Removes the Documents menu from the classic Start menu.
Remove Music icon from Start Menu	This option allows you to remove the Music icon from Start Menu.
Remove "Recently added" list from Start Menu	This option allows you to prevent the Start Menu from displaying a list of recently installed applications.
Remove Logoff on the Start Menu	This option allows you to removes the "Log Off <username>" item from the Start menu and prevents users from restoring it.
Remove Homegroup link from Start Menu	If you enable this option the Start menu will not show a link to Homegroup. It also removes the homegroup item from the Start Menu options. As a result, users cannot add the homegroup link to the Start Menu.
Remove Search Computer link	If you enable this policy, the "See all results" link will not be shown when the user performs a search in the start menu search box.
Add Search Internet link to Start Menu	If you enable this policy, a "Search the Internet" link is shown when the user performs a search in the start menu search box. This button launches the default browser with the search terms.
Remove Network icon from Start Menu	This option allows you to remove the Network icon from Start Menu.

Remove links and access to Windows Update	This option allows you to remove links and access to Windows Update.
Show additional calendar	By default, the calendar is set according to the locale of the operating system, and users can show an additional calendar. For zh-CN and zh-SG locales, an additional calendar shows the lunar month and date and holiday names in Simplified Chinese (Lunar) by default. For zh-TW, zh-HK, and zh-MO locales, an additional calendar shows the lunar month and date and holiday names in Traditional Chinese (Lunar) by default.
Prevent users from rearranging toolbars	This option allows you to prevent users from rearranging toolbars.
Lock all taskbar settings	This option allows you to lock all taskbar settings.
Remove the battery meter	This option allows you to remove the battery meter from the system control area.
Remove pinned programs from the Taskbar	This option allows you to remove pinned programs from the taskbar.
Remove the Security and Maintenance icon	This option allows you to remove Security and Maintenance from the system control area.
Do not allow pinning programs to the Taskbar	This option allows you to control pinning programs to the Taskbar.
Prevent users from adding or removing toolbars	This option allows you to prevent users from adding or removing toolbars.
Prevent users from moving taskbar to another screen dock location	This option allows you to prevent users from moving taskbar to another screen dock location.
Remove the networking icon	This option allows you to remove the networking icon from the system control area.
Prevent users from resizing the taskbar	This option allows you to prevent users from resizing the taskbar.
Show Windows Store apps on the taskbar	This option allows users to see Windows Store apps on the taskbar.
Remove the volume control icon	This option allows you to remove the volume control icon from the system control area.
Do not allow pinning Store app to the Taskbar	This option allows you to control pinning the Store app to the Taskbar.
Remove Notifications and Action Center	This option removes Notifications and Action Center from the notification area on the taskbar.

System restrictions:

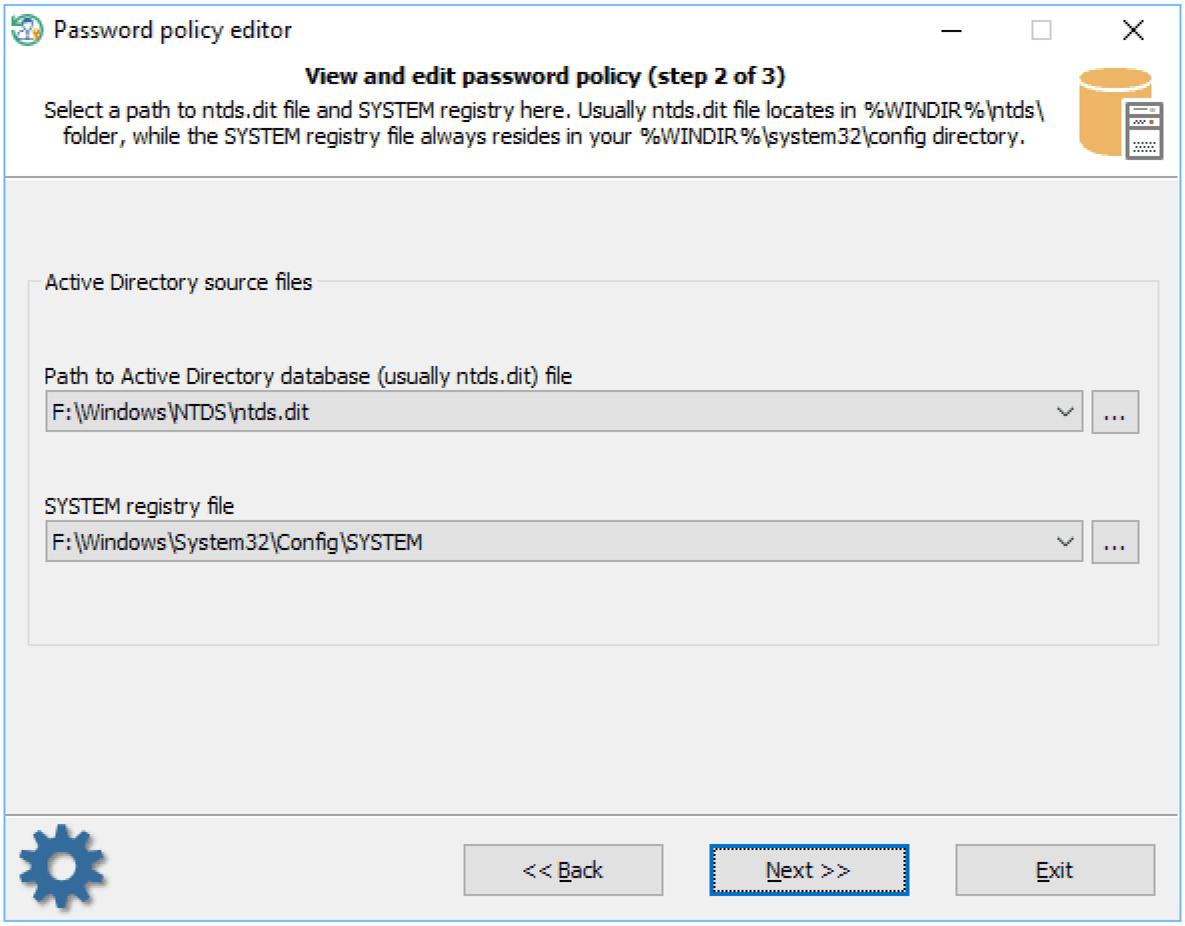
Name	**Description**
Prevent access to the command prompt	This option prevents users from running the interactive command prompt, Cmd.exe. This option also determines whether batch files (.cmd and .bat) can run on the computer. If you enable this option and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.
Prevent access to registry editing tools	Disables the Windows registry editor Regedit.exe. If you enable this option and the user tries to start Regedit.exe, a message appears explaining that a setting prevents the action.
Don't run specified Windows applications	Prevents Windows from running the programs you specify in this setting.
Run only specified Windows applications	Limits the Windows programs that users have permission to run on the computer.
Remove Logoff	This option disables or removes all menu items and buttons that log the user off the system. If you enable this setting, users will not see the Log off menu item when they

	press Ctrl+Alt+Del. This will prevent them from logging off unless they restart or shutdown the computer, or clicking Log off from the Start menu.
Remove Task Manager	This option prevents users from starting Task Manager. If you enable this setting, users will not be able to access Task Manager. If users try to start Task Manager, a message appears explaining that a policy prevents the action.
Remove Change Password	This option prevents users from changing their Windows password on demand. If you enable this setting, the 'Change Password' button on the Windows Security dialog box will not appear when you press Ctrl+Alt+Del.
Remove Lock Computer	This option prevents users from locking the system. If you enable this setting, users cannot lock the computer from the keyboard using Ctrl+Alt+Del.
All Removable Storage classes: Deny all access	Configure access to all removable storage classes.
Removable Disks: Deny read access	This option denies read access to removable disks.
Removable Disks: Deny write access	This option denies write access to removable disks.
CD and DVD: Deny read access	This option denies read access to the CD and DVD removable storage class.
CD and DVD: Deny write access	This option denies write access to the CD and DVD removable storage class.
WPD Devices: Deny read access	This option denies read access to removable disks, which may include media players, cellular phones, auxiliary displays, and CE devices.
WPD Devices: Deny write access	This option denies write access to removable disks, which may include media players, cellular phones, auxiliary displays, and CE devices.
Floppy Drives: Deny read access	This option denies read access to the Floppy Drives removable storage class, including USB Floppy Drives.
Floppy Drives: Deny write access	This option denies write access to the Floppy Drives removable storage class, including USB Floppy Drives.
Tape Drives: Deny read access	This option denies read access to the Tape Drive removable storage class.
Tape Drives: Deny write access	This option denies write access to the Tape Drive removable storage class.

3.2.6 Password policy editor

Sometimes to functioning security settings properly, it is vitally required to set up workstation's or domain's password policy. For example, if you want to to deny domain users to log on to a system without supplying strong passwords, you should restricted it through the domain password policy. However that would be quite a problem if you cannot log on to the workstation or to the domain as an administrator. The new RWP's password policy editor can get around the problem and allows changing various password policy's properties on any Windows system without logging on to the system.

Selecting data source



Password policy editor

View and edit password policy (step 2 of 3)

Select a path to ntds.dit file and SYSTEM registry here. Usually ntds.dit file locates in %WINDIR%\ntds\ folder, while the SYSTEM registry file always resides in your %WINDIR%\system32\config directory.

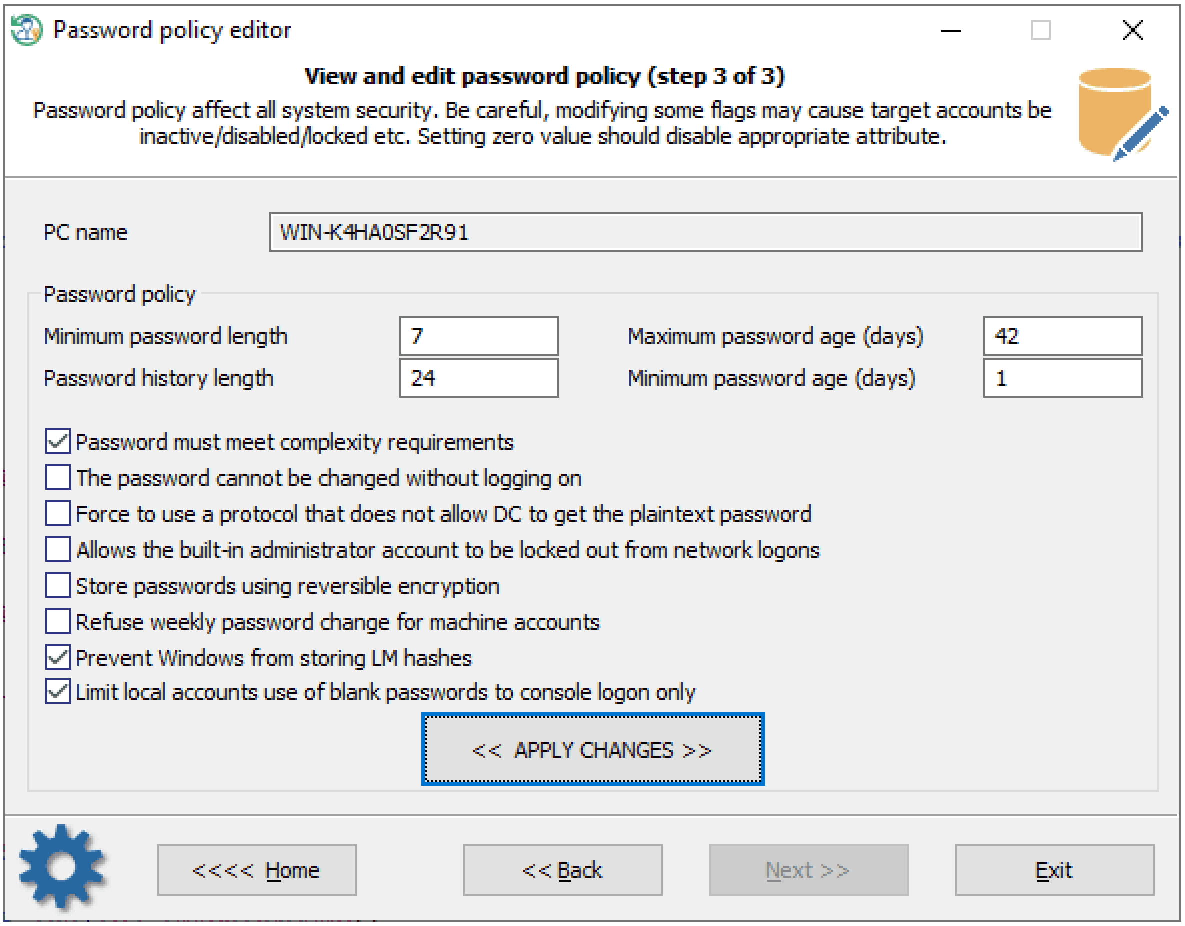
Active Directory source files

Path to Active Directory database (usually ntds.dit) file: F:\Windows\NTDS\ntds.dit

SYSTEM registry file: F:\Windows\System32\Config\SYSTEM

First of all, you will need to feed the program with two system files:
- either **SAM** and **SYSTEM,** in case you' want to modify password policy of a workstation or a standalone PC;
- or **NTDS.DIT** and **SYSTEM,** when you need to change the password policy properties of a domain.
The program should try to find the files automatically. You can however provide the paths manually.

Changing password policy



Password policy editor

View and edit password policy (step 3 of 3)

Password policy affect all system security. Be careful, modifying some flags may cause target accounts be inactive/disabled/locked etc. Setting zero value should disable appropriate attribute.

PC name: WIN-K4HA0SF2R91

Password policy

Minimum password length	7	Maximum password age (days)	42
Password history length	24	Minimum password age (days)	1

☑ Password must meet complexity requirements
☐ The password cannot be changed without logging on
☐ Force to use a protocol that does not allow DC to get the plaintext password
☐ Allows the built-in administrator account to be locked out from network logons
☐ Store passwords using reversible encryption
☐ Refuse weekly password change for machine accounts
☑ Prevent Windows from storing LM hashes
☑ Limit local accounts use of blank passwords to console logon only

Here's the short description of what you can modify in password policy of the target system:

- Minimum password length - minimum length of a valid password, in characters.
- Password history length - number of previous passwords saved in the history list. A user is not allowed to reuse a password from the list.
- Maximum password age - maximum length (in days) that a password can remain the same. Passwords older than this must be changed.
- Minimum password age - minimum length of time before a password can be changed.
- Password must meet complexity requirements - passwords must meet the following minimum requirements: contain no user's account name or a part of it, be at least six characters in length (if otherwise is not set), contain characters from at least three charsets, do not be one used previously (if password history is set).
- The password cannot be changed without logging on - password cannot be changed without logging on. Otherwise, if it has expired, you can change it and then log on.
- Force to use a protocol that does not allow DC to get the plaintext password - forces the client to use a protocol that does not allow the domain controller to get plaintext passwords.
- Allows the built-in administrator account to be locked out from network logons
- Store passwords using reversible encryption - force to store plaintext passwords for all users instead of hashing the passwords.
- Refuse weekly password change for machine accounts - removes the requirement for any machine account to automatically change its password every week.
- Prevent Windows from storing LM hashes. The LAN Manager hash uses an extremely weak encryption algorithm. This setting controls whether a LM hash of the password can be stored in Active Directory and the local SAM database (the next time a new user is created or the password is changed). This setting is on by default on Windows Vista and later OSes.

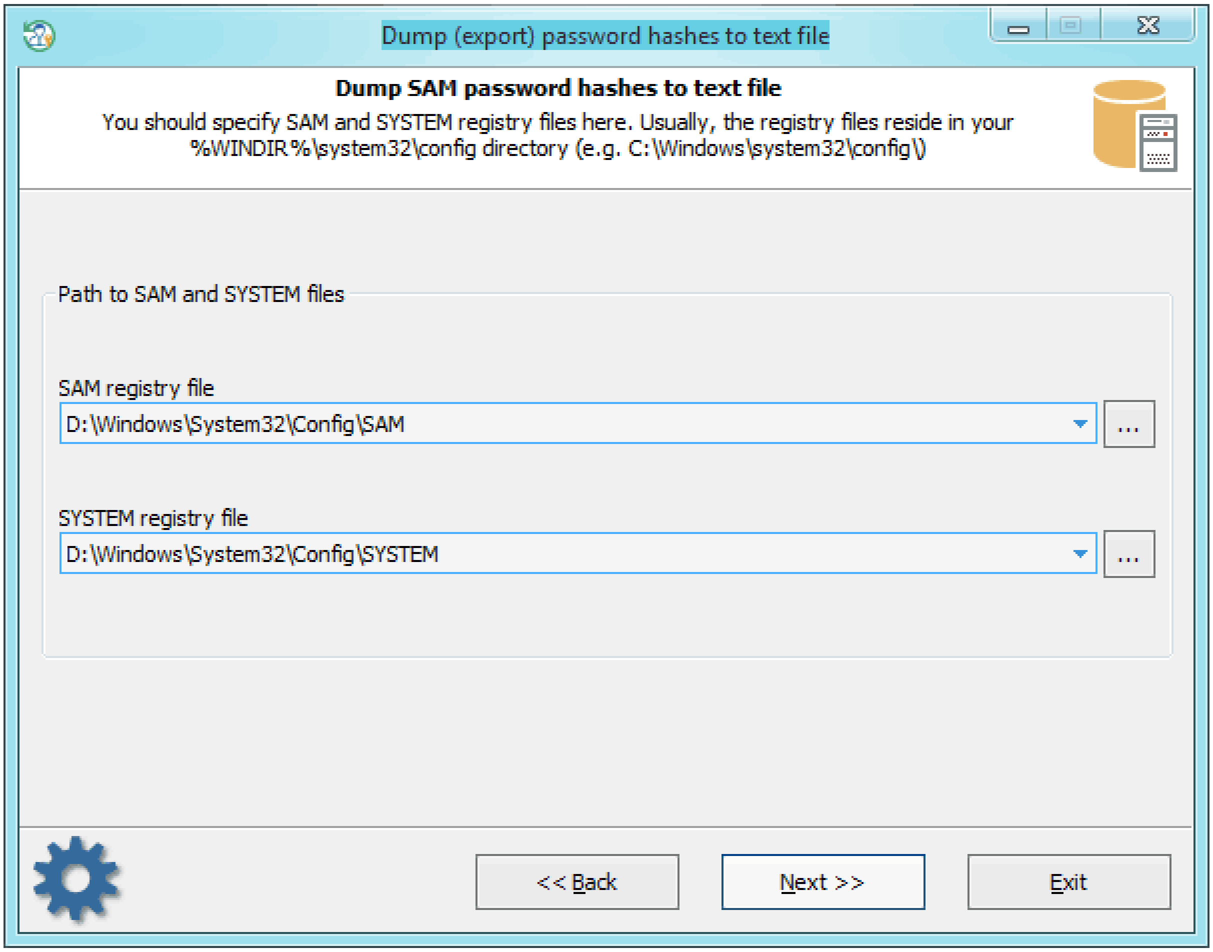
- Limit local accounts to use blank passwords to console logon only. Prevent accounts with blank passwords from existing on a system. However, if a local account with a blank password did exist, enabling this setting will prevent network access, limiting the account to local console logon only.

To disable an editable attribute, just set zero value into its edit box.

Be careful, altering any value of the password policy will affect on all security of the Windows system!

3.2.7 Dump password hashes

Selecting data source



Dump (export) password hashes to text file

Dump SAM password hashes to text file

You should specify SAM and SYSTEM registry files here. Usually, the registry files reside in your %WINDIR%\system32\config directory (e.g. C:\Windows\system32\config\)

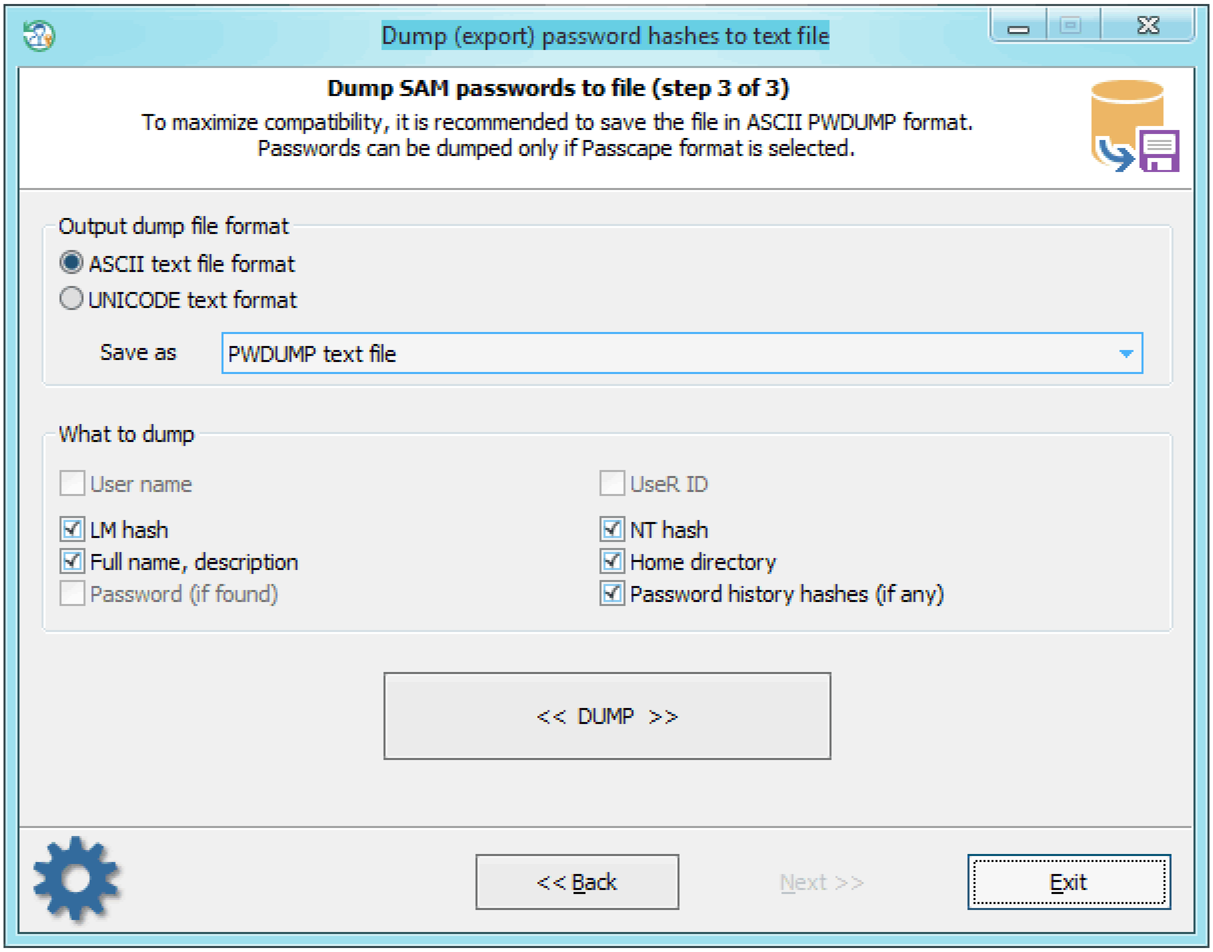
Path to SAM and SYSTEM files

SAM registry file: D:\Windows\System32\Config\SAM

SYSTEM registry file: D:\Windows\System32\Config\SYSTEM

On this step, specify the location of SAM and SYSTEM files. Or, in the case with domain users, – ntds.dit and SYSTEM.

Export password hashes



Dump (export) password hashes to text file

Dump SAM passwords to file (step 3 of 3)

To maximize compatibility, it is recommended to save the file in ASCII PWDUMP format.
Passwords can be dumped only if Passcape format is selected.

Output dump file format

● ASCII text file format
○ UNICODE text format

Save as: PWDUMP text file

What to dump

□ User name	□ UseR ID
☑ LM hash	☑ NT hash
☑ Full name, description	☑ Home directory
□ Password (if found)	☑ Password history hashes (if any)

Select the format and type of the dump file. While generating the dump, you can also delete, if that's no value to you, individual unnecessary attributes of the account. If the Passcape format is selected, you can also dump plaintext passwords (if ones were found). The application scans your computer for the availability of such and, if such are available, maps them to the accounts while saving to the dump file.

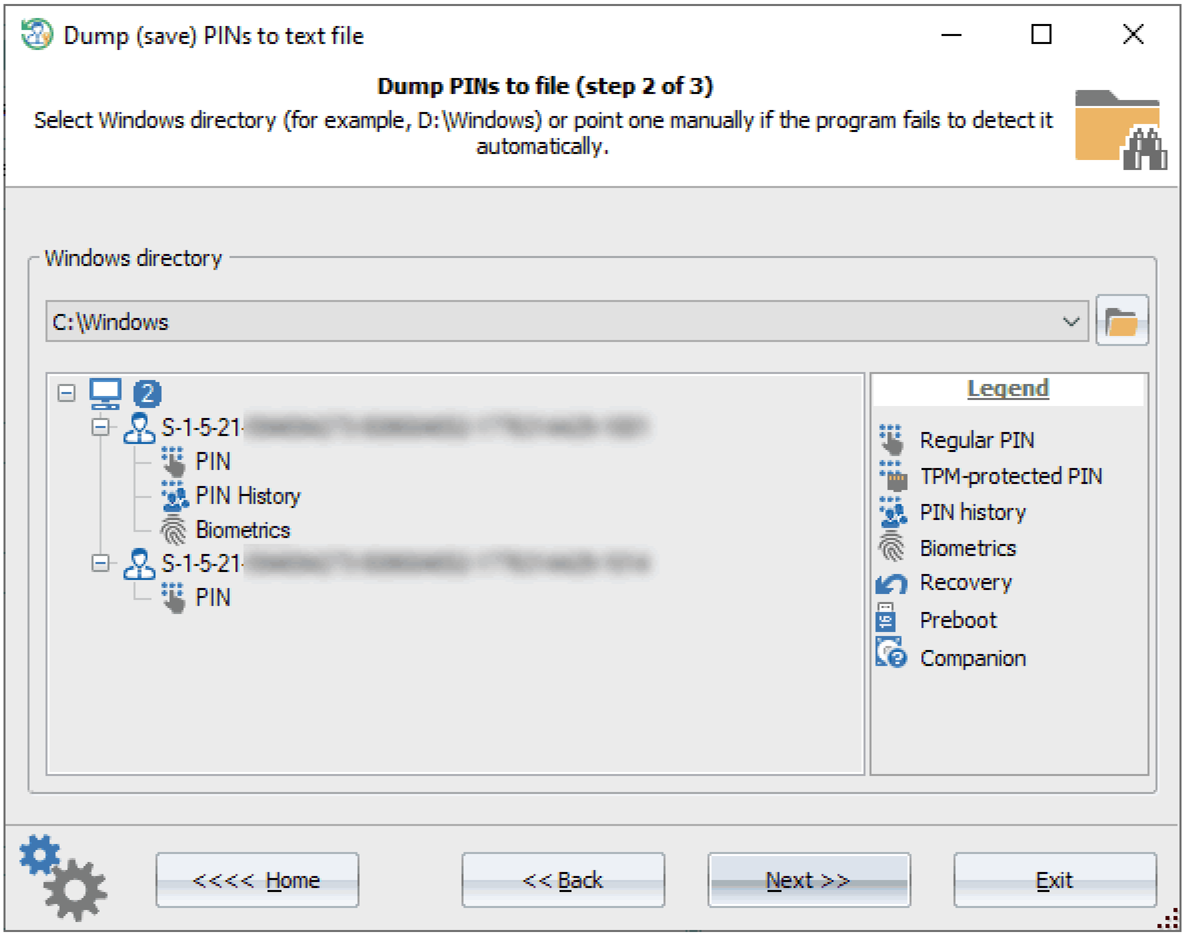
Plaintext passwords are stored in domain when the option '*Store passwords using reversible encryption for all users in the domain*' is set; you can find it in the groups policy console.

Further on, you can use the dump file with different password audit and recovery applications.

Please note also that Reset Windows Password, thanks to the AI attack technology developed by Passcape Software, can decrypt passwords to certain accounts literally instantly, without searching. For details, please refer to the Lookup user passwords section.

3.2.8 Dump Windows Hello PIN

Selecting Windows directory



Dump (save) PINs to text file

Dump PINs to file (step 2 of 3)

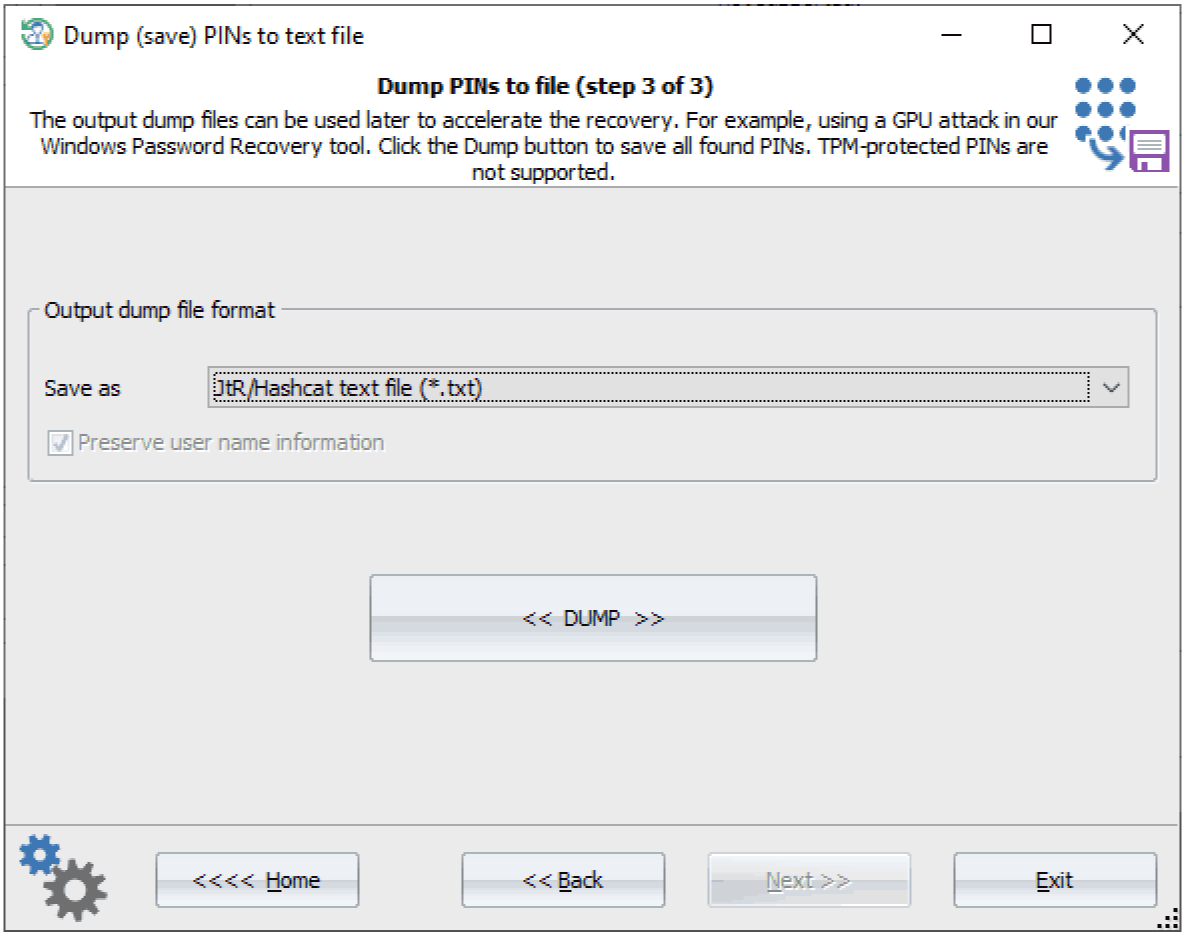
Select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it automatically.

Windows directory: C:\Windows

```
⊟ 2
  ⊟ S-1-5-21-[redacted]
      PIN
      PIN History
      Biometrics
  ⊟ S-1-5-21-[redacted]
      PIN
```

Once the Windows directory is set, the program displays the list of users with detected PIN sign-ins.

Saving Windows PIN


Dump (save) PINs to text file

Dump PINs to file (step 3 of 3)

The output dump files can be used later to accelerate the recovery. For example, using a GPU attack in our Windows Password Recovery tool. Click the Dump button to save all found PINs. TPM-protected PINs are not supported.

Output dump file format

Save as: JtR/Hashcat text file (*.txt)

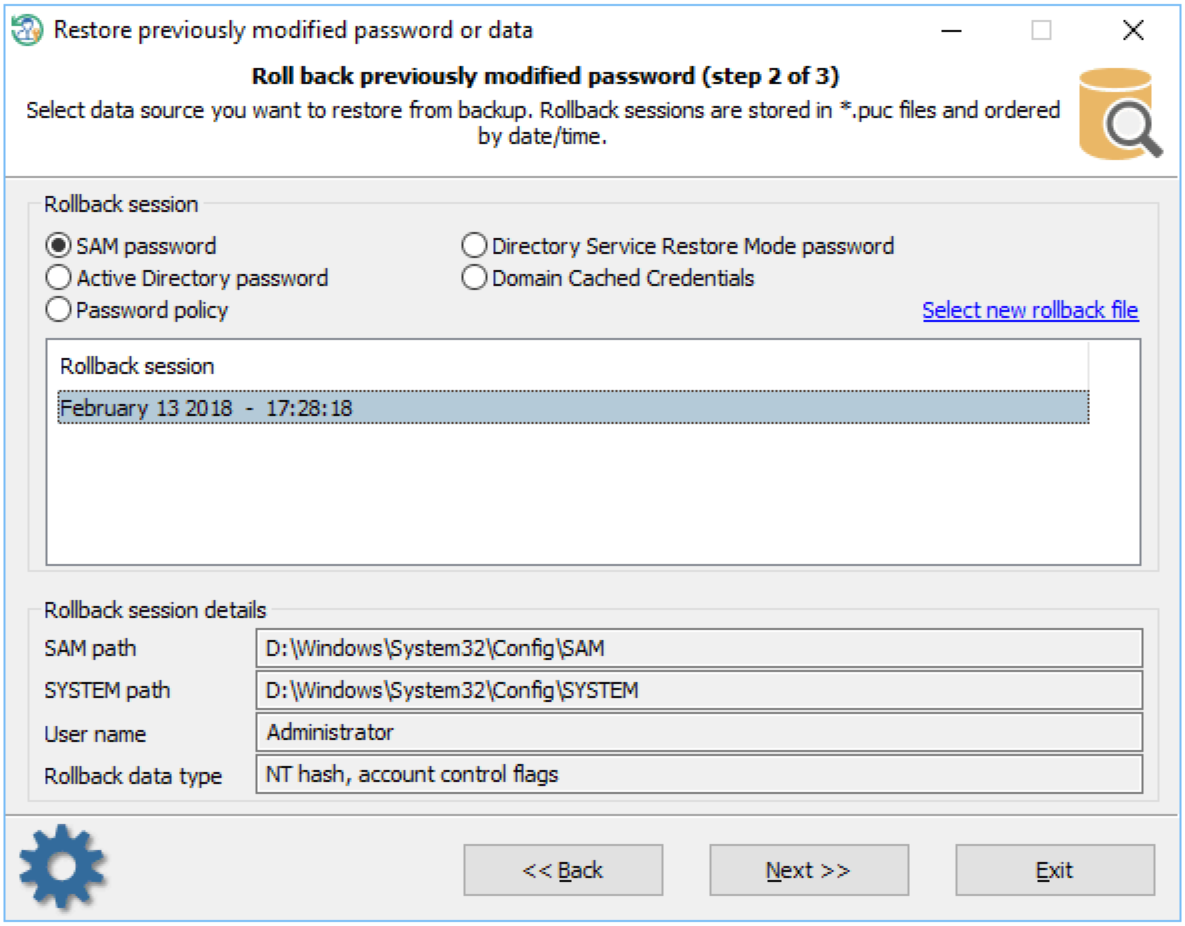
☑ Preserve user name information

The program supports Hashcat (*.txt) and Elcomsoft (*.pin) formats when saving Windows PIN codes. Both formats are identical pretty much.

Later, you can use the saved dumps from within a third-party application. For example, our Windows Password Recovery auditing tool works with both formats and supports GPUs to accelerate the PIN recovery process.

3.2.9 Restoring previous modified password

Choosing a roll-back file



Restore previously modified password or data

Roll back previously modified password (step 2 of 3)

Select data source you want to restore from backup. Rollback sessions are stored in *.puc files and ordered by date/time.

Rollback session

● SAM password
○ Active Directory password
○ Password policy
○ Directory Service Restore Mode password
○ Domain Cached Credentials

Select new rollback file

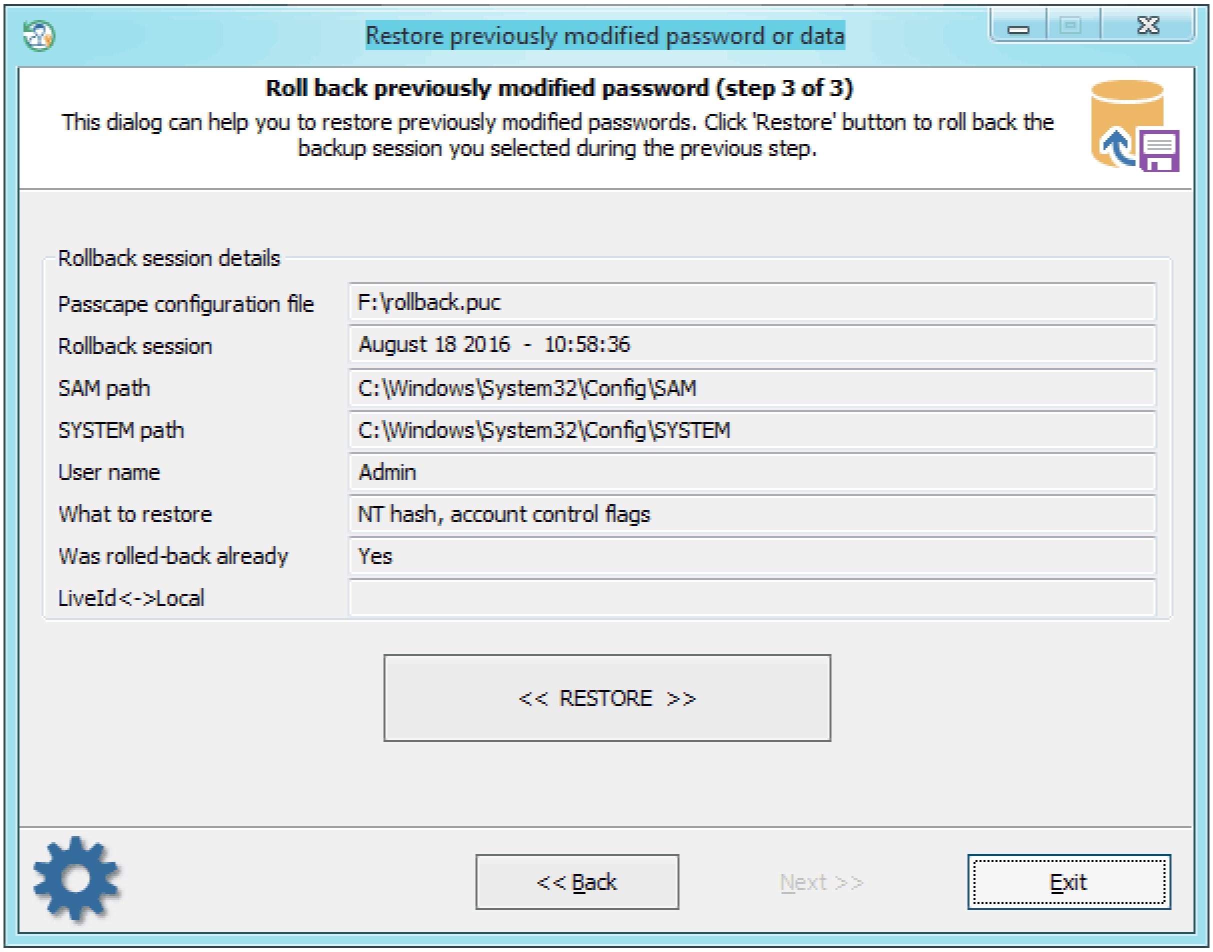
Rollback session
February 13 2018 - 17:28:18

Rollback session details

SAM path	D:\Windows\System32\Config\SAM
SYSTEM path	D:\Windows\System32\Config\SYSTEM
User name	Administrator
Rollback data type	NT hash, account control flags

If for whatsoever reason you need to undo (i.e. restore) the password that was reset or modified earlier, on the second step of the Wizard, provide the application with the *.puc file with the roll-back (undo) sessions. Activate the type of the password to be restored: regular SAM account password, Active Directory, DSRM password or domain cached credentials, password policy flags. After that, select the date when the change was made.

Restoring previously modified password



Roll back previously modified password (step 3 of 3)

This dialog can help you to restore previously modified passwords. Click 'Restore' button to roll back the backup session you selected during the previous step.

Rollback session details

Passcape configuration file	F:\rollback.puc
Rollback session	August 18 2016 - 10:58:36
SAM path	C:\Windows\System32\Config\SAM
SYSTEM path	C:\Windows\System32\Config\SYSTEM
User name	Admin
What to restore	NT hash, account control flags
Was rolled-back already	Yes
LiveId<->Local	

On the last step, the application will offer you to review the details of the undo session; please pay close attention to the last three items:

- Account to be managed.
- Data to be restored. That’s the data you have modified at some point.
- Whether or not this undo session has been used already

Let’s review this situation for an example:

A computer security expert needs to logon to Windows under a certain account. The password for that account is unknown. At the same time, the account password must remain unmodified.

Here is the routine:

- Run Reset Windows Password, select the corresponding account and reset its password. At the same time, save the undo session to a *.puc file (the application will prompt you to do that when you modify the password).
- Close Reset Windows Password and start Windows. Logon under the modified account with the blank password. Do what you need under that account.
- Now you need to restore the old account password. For that purpose, reboot once again and launch Reset Windows Password. On the main menu, select ‘*Restore previously modified password or data*’, enter path to the undo file where you have saved the changes you had made. Move on to the third step and make sure that this is the account you need. Click on the <<Restore>> button, and the old password will be restored.

3.3 Active Directory

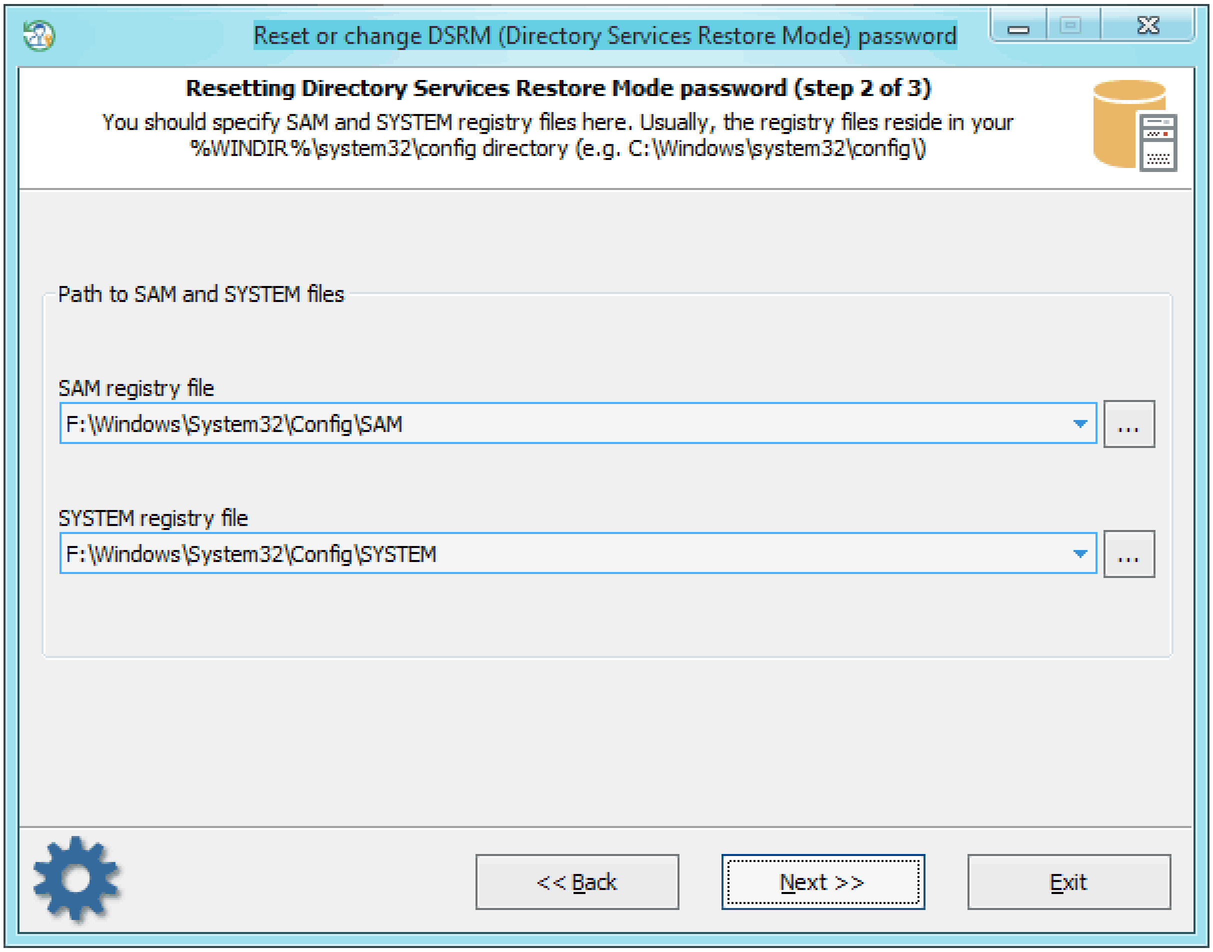
3.3.1 Reset DSRM passwords

What is DSRM

DSRM (known as **Directory Services Repair Mode** or **Directory Services Restore Mode** in versions prior to Windows Server 2012) is a special boot mode of a Windows Server domain controller that is something similar to Safe Mode with Networking, but without Active Directory running. DSRM is used to restore Active Directory from a backup. It is also helpful in different situations and problems with the AD.

To get into DSRM one needs to press the F8 key immediately after BIOS/UEFI POST screen, but before the Windows logo appears. In Windows Server 2012 and later OSes there's **Advanced Boot Options** menu or **Windows Recovery Environment** for that.

Selecting data source



Reset or change DSRM (Directory Services Restore Mode) password

Resetting Directory Services Restore Mode password (step 2 of 3)

You should specify SAM and SYSTEM registry files here. Usually, the registry files reside in your %WINDIR%\system32\config directory (e.g. C:\Windows\system32\config\)

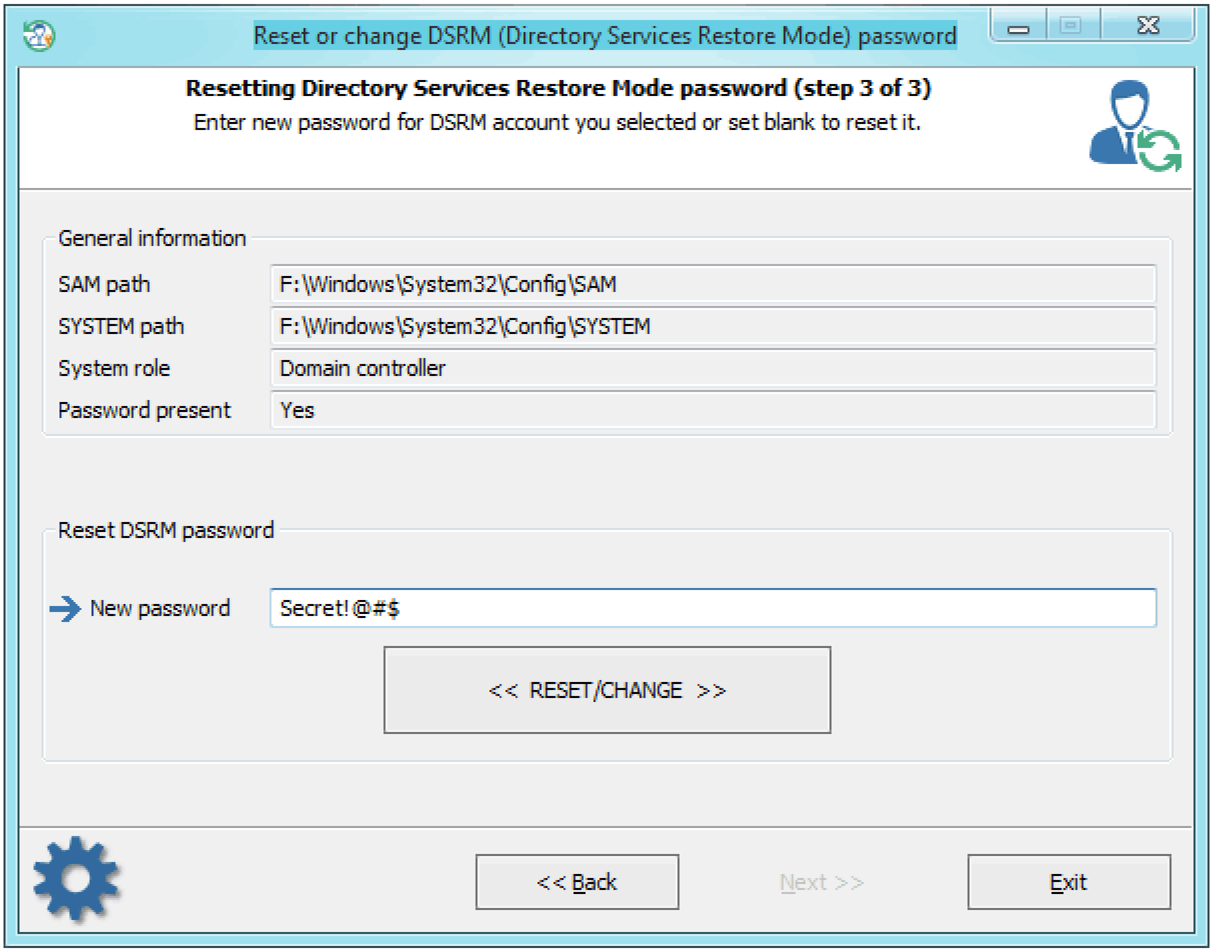
Path to SAM and SYSTEM files

SAM registry file: F:\Windows\System32\Config\SAM

SYSTEM registry file: F:\Windows\System32\Config\SYSTEM

Password recovery process for DSRM account is almost the same as for regular user account. First you'll have to specify the location for **SAM** and **SYSTEM** registry files.

Resetting password



Reset or change DSRM (Directory Services Restore Mode) password

Resetting Directory Services Restore Mode password (step 3 of 3)

Enter new password for DSRM account you selected or set blank to reset it.

General information

SAM path	F:\Windows\System32\Config\SAM
SYSTEM path	F:\Windows\System32\Config\SYSTEM
System role	Domain controller
Password present	Yes

Reset DSRM password

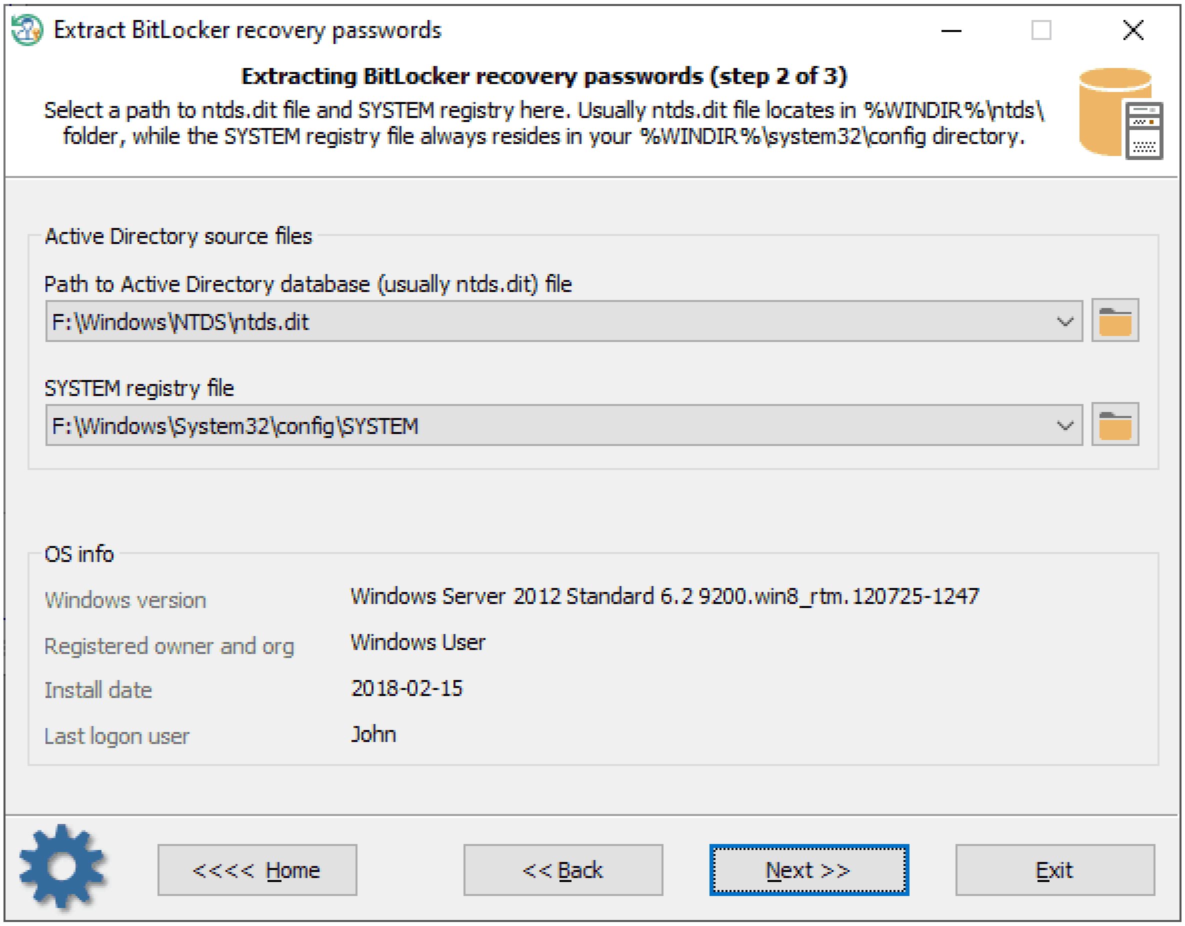
New password: Secret!@#$

Type in a new password or just set the input field blank if you want to reset it. Then confirm the changes by clicking the 'RESET/CHANGE' button. The program may ask you to create a backup file. You can use the backup file later to roll-back the changes.

3.3.2 Extract BitLocker recovery passwords

Often, BitLocker recovery passwords are backed-up in an Active Directory database. This function of the program is designed to extract BitLocker passwords even out of a non-bootable or a non-working domain.

Selecting Active Directory database



Extract BitLocker recovery passwords

Extracting BitLocker recovery passwords (step 2 of 3)

Select a path to ntds.dit file and SYSTEM registry here. Usually ntds.dit file locates in %WINDIR%\ntds\ folder, while the SYSTEM registry file always resides in your %WINDIR%\system32\config directory.

Active Directory source files

Path to Active Directory database (usually ntds.dit) file: F:\Windows\NTDS\ntds.dit

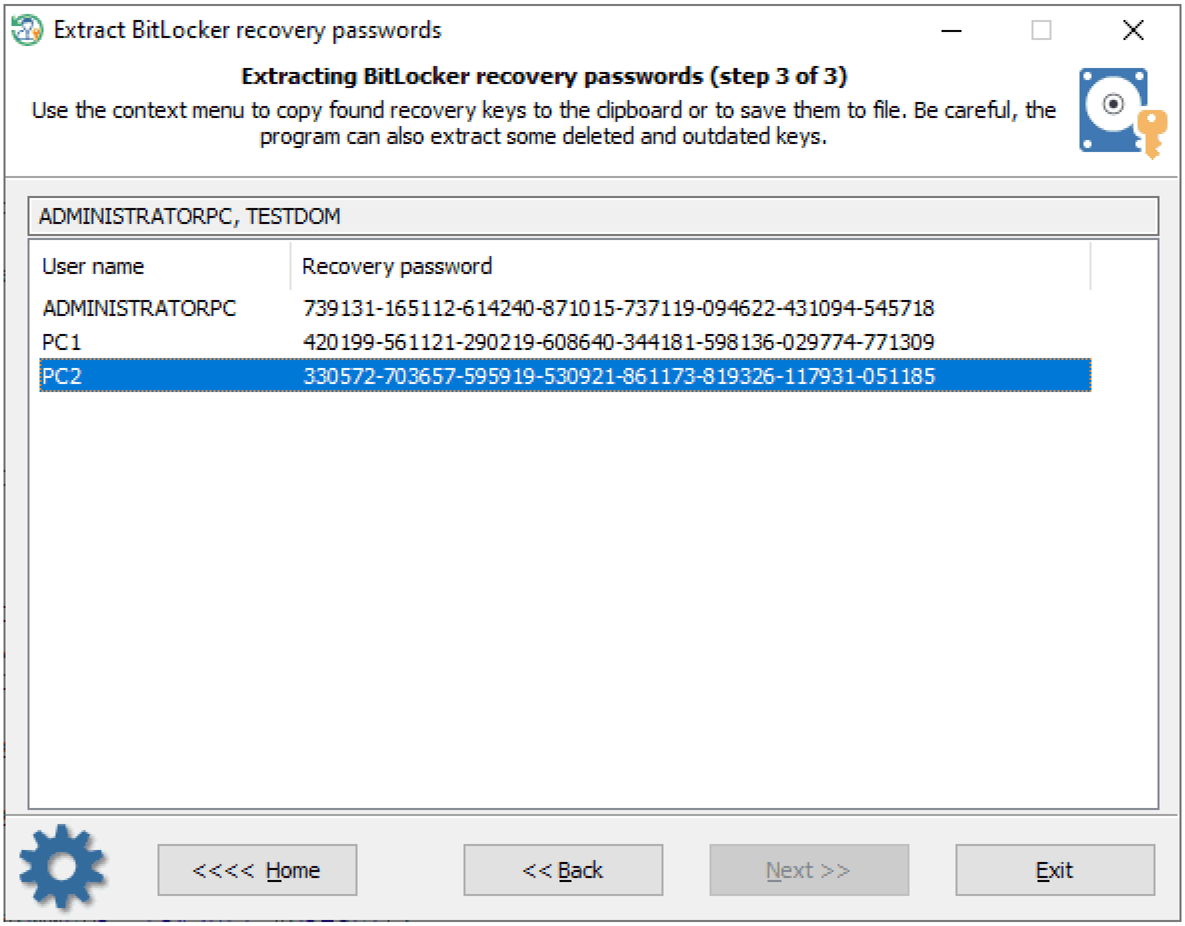
SYSTEM registry file: F:\Windows\System32\config\SYSTEM

OS info

Windows version	Windows Server 2012 Standard 6.2 9200.win8_rtm.120725-1247
Registered owner and org	Windows User
Install date	2018-02-15
Last logon user	John

In the beginning, you have to set up paths for the **SYSTEM** registry and for the **NTDS.DIT** database. The program should locate the paths automatically but you can select them on your own.

Extracting BitLocker recovery passwords



Extract BitLocker recovery passwords

Extracting BitLocker recovery passwords (step 3 of 3)

Use the context menu to copy found recovery keys to the clipboard or to save them to file. Be careful, the program can also extract some deleted and outdated keys.

ADMINISTRATORPC, TESTDOM

User name	Recovery password
ADMINISTRATORPC	739131-165112-614240-871015-737119-094622-431094-545718
PC1	420199-561121-290219-608640-344181-598136-029774-771309
PC2	330572-703657-595919-530921-861173-819326-117931-051185

Be careful, the program can additionally retrieve expired and deleted BitLocker keys, and often there's no way to get the real names of the key owners.

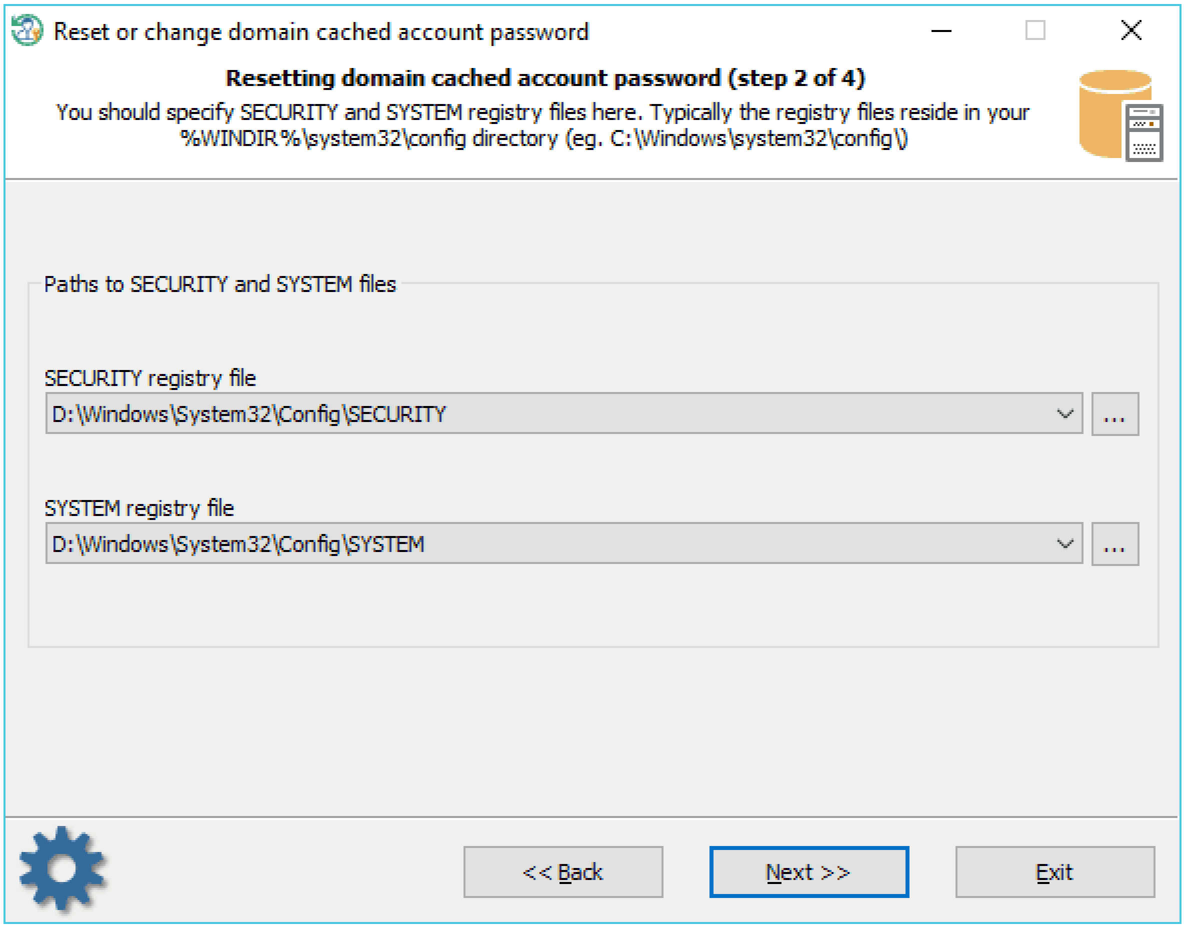
You can copy the required key to the clipboard or save it to a file.

3.4 Domain accounts

3.4.1 Reset domain cached password

When a user logs on to a Windows domain, the user's domain credentials are securely cached and saved to his/her PC. This feature allows users logging on to the domain when the local workstation is disconnected from the network or even if no domain controller is available. To get around the problem of lost or forgotten password for the domain account, you can simply reset your domain cached credentials using Reset Windows Password. The process consists of 3 simple steps.

Selecting registry files



Reset or change domain cached account password

Resetting domain cached account password (step 2 of 4)

You should specify SECURITY and SYSTEM registry files here. Typically the registry files reside in your %WINDIR%\system32\config directory (eg. C:\Windows\system32\config\)

Paths to SECURITY and SYSTEM files

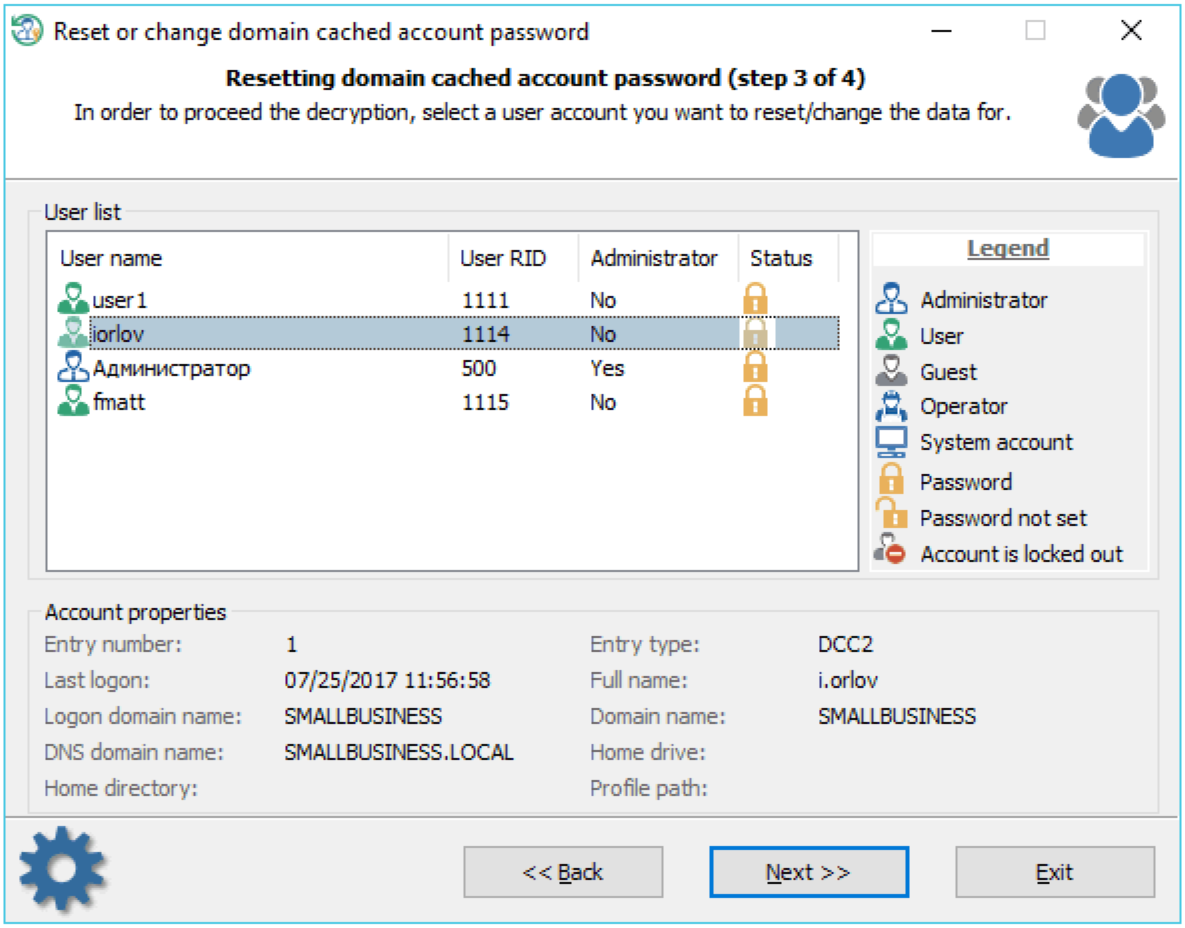
SECURITY registry file: D:\Windows\System32\Config\SECURITY

SYSTEM registry file: D:\Windows\System32\Config\SYSTEM

To reset a domain cached password, you should provide two registry files: **SECURITY** and **SYSTEM**. Both files are located in the **%WINDIR%\system32\config** folder. Where %WINDIR% is your windows directory. Usually, the program takes care of that and suggests the files it found.

Before proceeding to the next recovery step, make sure you selected exactly the files you need.

Selecting domain account



Resetting domain cached account password (step 3 of 4)

In order to proceed the decryption, select a user account you want to reset/change the data for.

User list

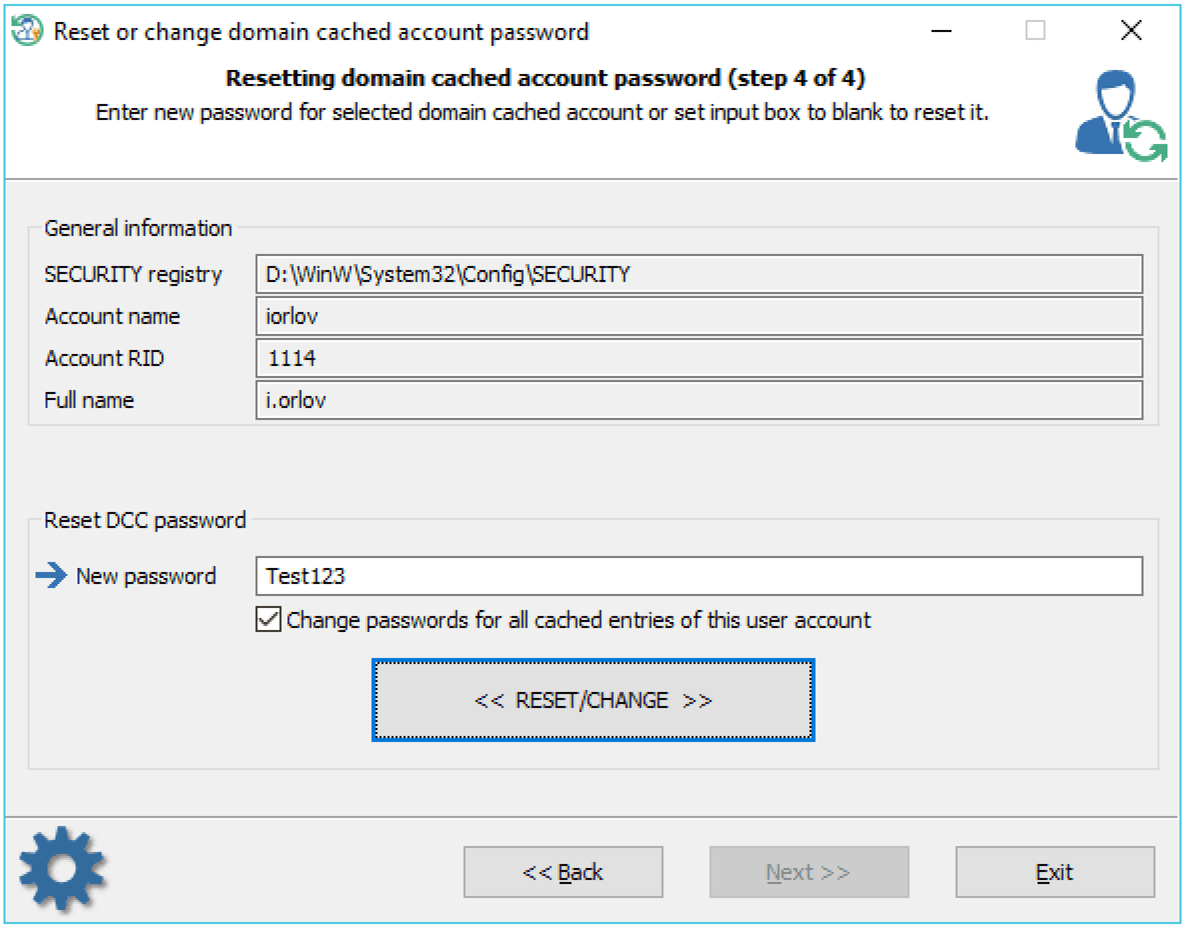
User name	User RID	Administrator	Status
user1	1111	No	🔒
iorlov	1114	No	🔒
Администратор	500	Yes	🔒
fmatt	1115	No	🔒

Account properties

Entry number:	1	Entry type:	DCC2
Last logon:	07/25/2017 11:56:58	Full name:	i.orlov
Logon domain name:	SMALLBUSINESS	Domain name:	SMALLBUSINESS
DNS domain name:	SMALLBUSINESS.LOCAL	Home drive:	
Home directory:		Profile path:	

The upper part of the dialog displays a list of found cached entries with the names of the user accounts. Select one of the entries to view its properties: the full name of the user account, last login date, logon domain, home directory, etc.

Resetting password



Reset or change domain cached account password

Resetting domain cached account password (step 4 of 4)

Enter new password for selected domain cached account or set input box to blank to reset it.

General information

SECURITY registry: D:\WinW\System32\Config\SECURITY

Account name: iorlov

Account RID: 1114

Full name: i.orlov

Reset DCC password

New password: Test123

☑ Change passwords for all cached entries of this user account

To reset the password, leave the '*New password*' input box empty and click the '*RESET/CHANGE*'. Do pay special attention to the additional option. Domain cache is arranged in such a manner that it can contain multiple entries of the same user. If the '*Change password for all cached entries for this user account*' option is set, then the program will try to change/reset passwords of all found entries of the selected account (with the specified RID). Otherwise it will reset the password for the selected entry only. It is recommended to set this option on unless you know what you do.

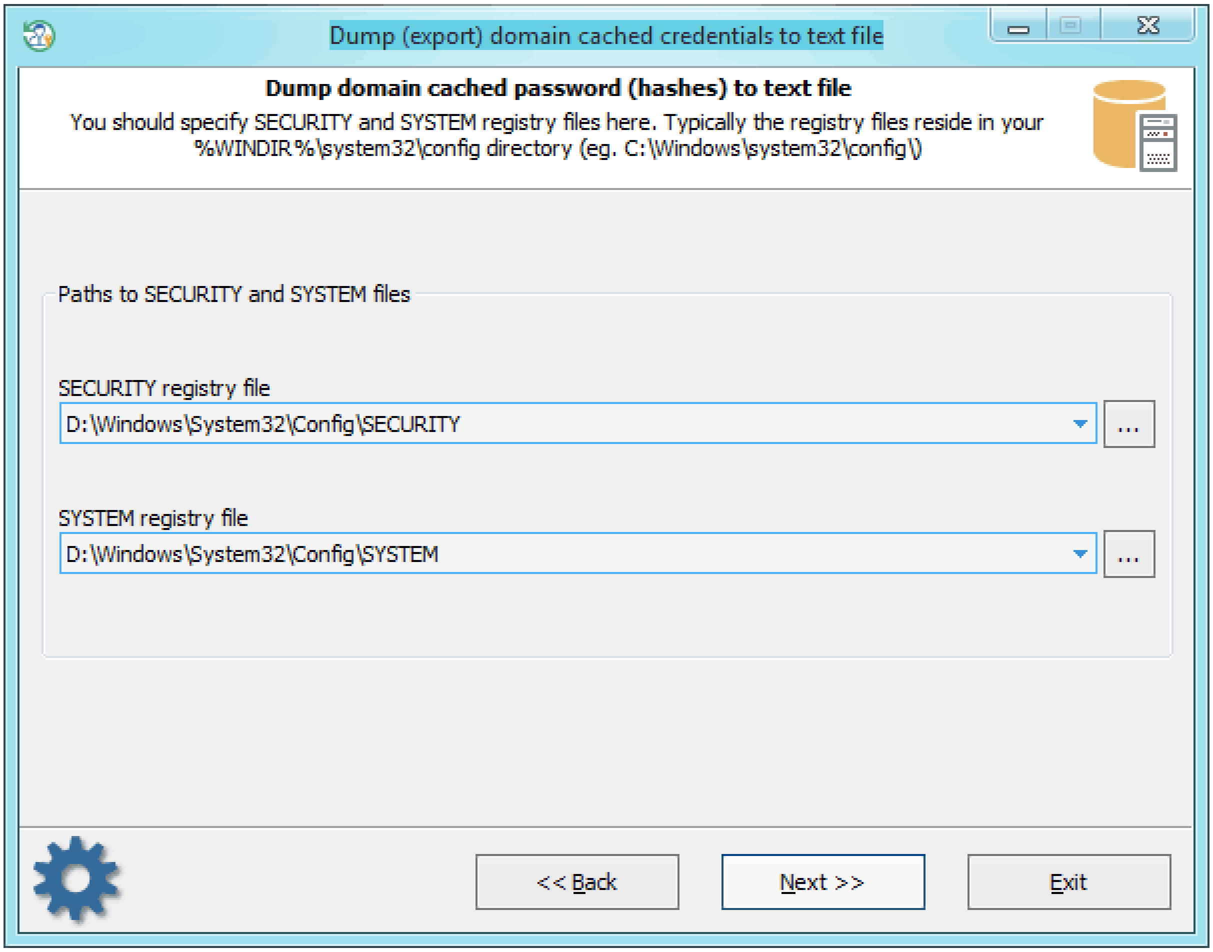
Make sure that your new password meets the domain length and complexity requirements and does not match any of the previously entered passwords (if security policy and password history are used.) Otherwise, Windows may deny access even if the password is successfully modified.

Please note, to log in to your domain account successfully after the cached password is reset, you must temporarily **disable connection to the domain!** Otherwise, Windows will not use the local cached entry but the regular domain credentials instead.

Keep in mind, logging on to the domain with cached credentials gives you access to local resources only.

3.4.2 Dump domain cached passwords

Selecting data source



Dump (export) domain cached credentials to text file

Dump domain cached password (hashes) to text file

You should specify SECURITY and SYSTEM registry files here. Typically the registry files reside in your %WINDIR%\system32\config directory (eg. C:\Windows\system32\config\)

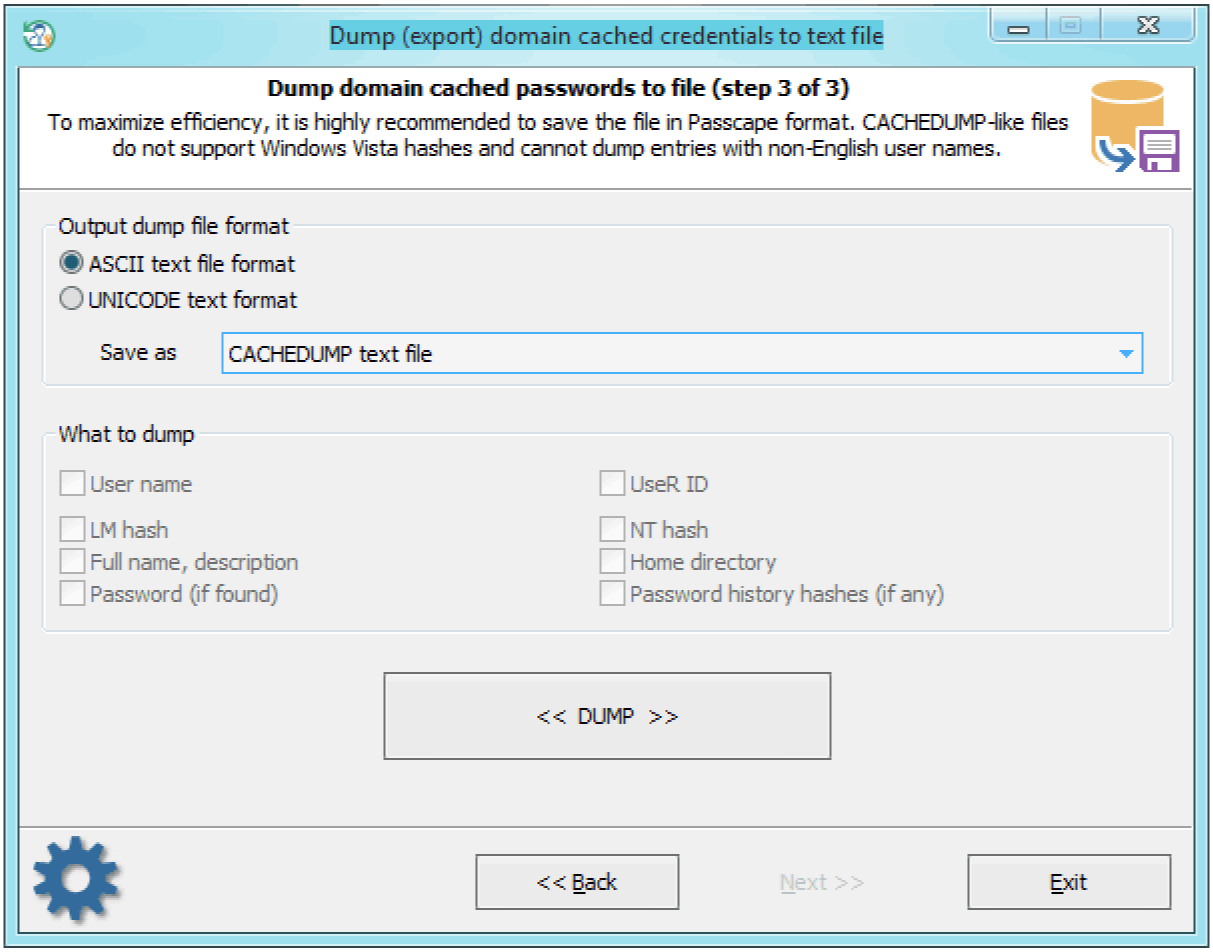
Paths to SECURITY and SYSTEM files

SECURITY registry file: D:\Windows\System32\Config\SECURITY

SYSTEM registry file: D:\Windows\System32\Config\SYSTEM

For decrypting domain cached credentials, the program needs to 'know' the location of two system registry files: SECURITY and SYSTEM. Select them from the list or, if the application was unable to locate them, provide the path to them manually.

Dumping domain cached credentials



Dump (export) domain cached credentials to text file

Dump domain cached passwords to file (step 3 of 3)

To maximize efficiency, it is highly recommended to save the file in Passcape format. CACHEDUMP-like files do not support Windows Vista hashes and cannot dump entries with non-English user names.

Output dump file format

● ASCII text file format
○ UNICODE text format

Save as: CACHEDUMP text file

What to dump

□ User name
□ UseR ID
□ LM hash
□ NT hash
□ Full name, description
□ Home directory
□ Password (if found)
□ Password history hashes (if any)

The final dialog provides just two options:

- **Dump file format**. ASCII is good for all cases, but problems may occur with non-English user names and, respectively, with further analysis and decryption of those hashes. UNICODE supports all languages, but compatibility problems may occur when reading this format in different applications.

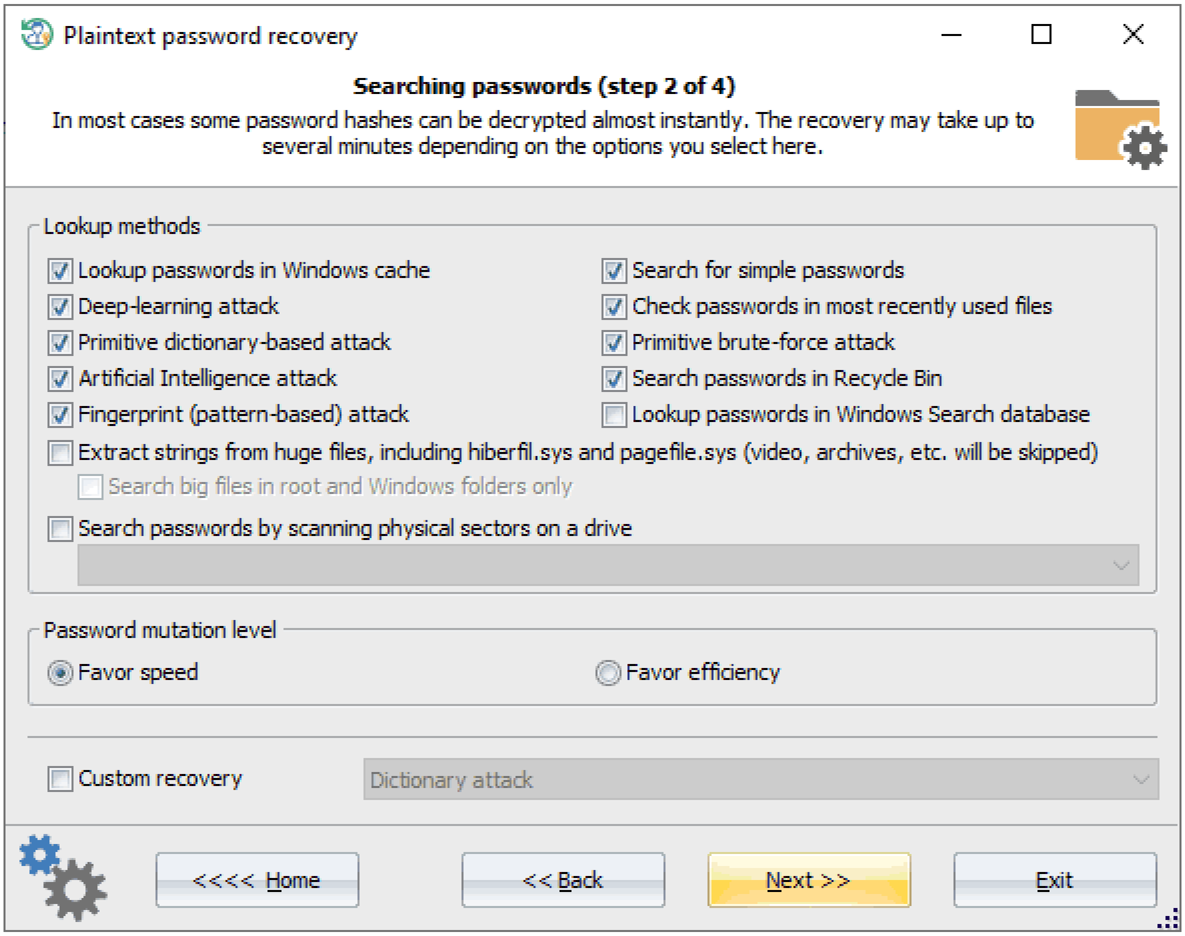
- **Dump file type** can be either CACHEDUMP – a simple but widespread format. No compatibility problems will occur. However, this format imposes a number of restrictions. First, it does not support non-English user names. Respectively, further on, you will be unable to decrypt the account password, as it is bound to the name. Second, the current version of the CACHEDUMP format does not support operating systems Windows Vista and higher.

Passcape format – free from these disadvantages and can be successfully used in password audit and recovery applications like, for example, Network Password Recovery.

3.5 Passwords

3.5.1 Search for logon passwords

Setting search and recovery methods



Plaintext password recovery

Searching passwords (step 2 of 4)

In most cases some password hashes can be decrypted almost instantly. The recovery may take up to several minutes depending on the options you select here.

Lookup methods

☑ Lookup passwords in Windows cache
☑ Deep-learning attack
☑ Primitive dictionary-based attack
☑ Artificial Intelligence attack
☑ Fingerprint (pattern-based) attack
☑ Search for simple passwords
☑ Check passwords in most recently used files
☑ Primitive brute-force attack
☑ Search passwords in Recycle Bin
□ Lookup passwords in Windows Search database
□ Extract strings from huge files, including hiberfil.sys and pagefile.sys (video, archives, etc. will be skipped)
□ Search big files in root and Windows folders only
□ Search passwords by scanning physical sectors on a drive

Password mutation level

● Favor speed ○ Favor efficiency

□ Custom recovery Dictionary attack

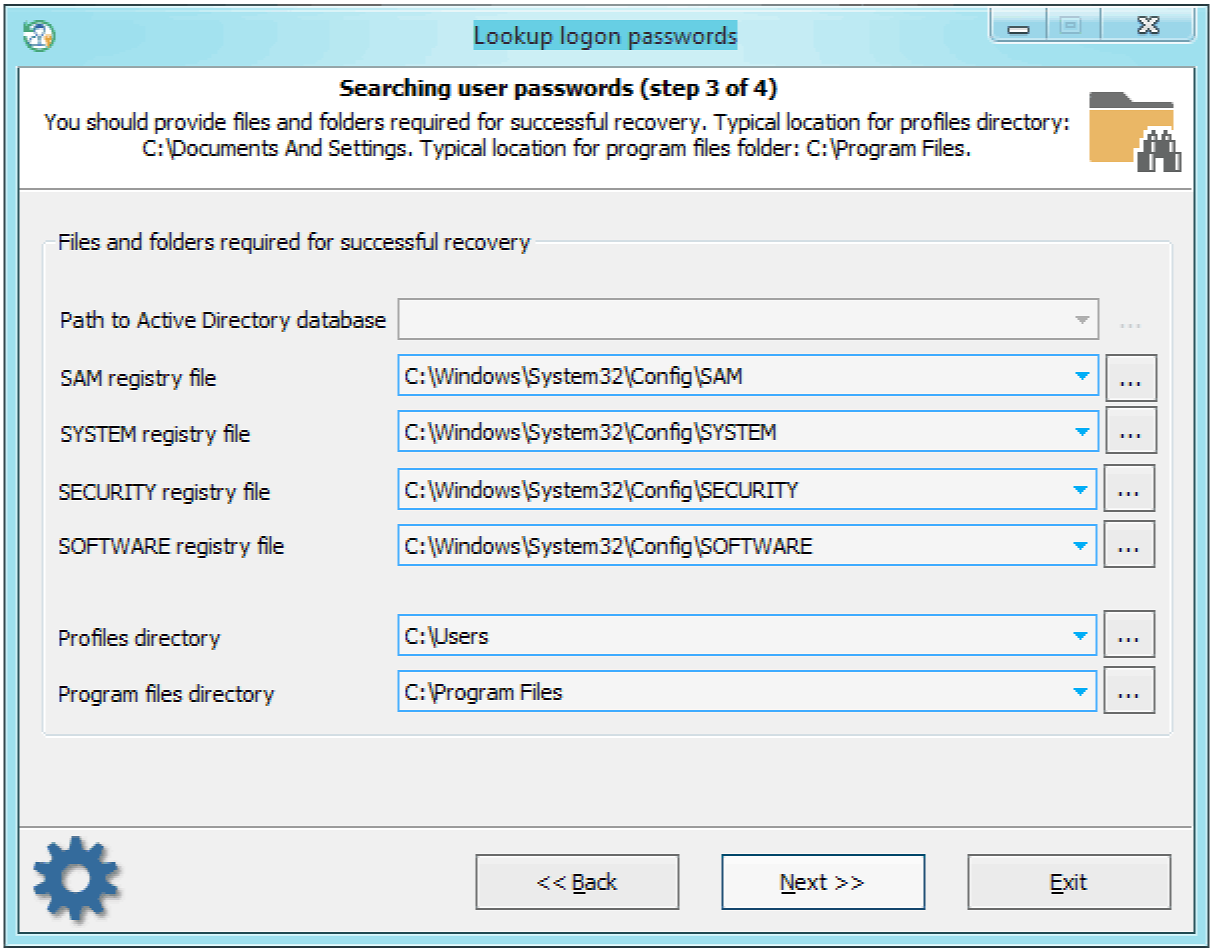
Finding user’s passwords takes 11 steps:

1. Finding information in Windows system cache. This method, in its turn, consists of over a dozen of mini-attacks, during which the program analyzes all kinds of personal data like LSA secrets, VPN, WiFi, DSL, FTP, IM, etc, passwords, e-mail correspondence, sticky notes, Windows clipboard, browser passwords, internet auto-completion and search phrases, Windows Search index, etc. To ensure the system files are not altered, the program does not involve its auto repair function for Windows Search databases that are not in a clean state and silently skips such databases. To check if the Windows Search database is clean or dirty, try to open it from within the Windows Search explorer. The program will prompt to repair the database if it is in a dirty state.
2. Analyzing simple, short passwords, keyboard shortcuts, etc.
3. Password search using deep learning algorithms. Even though these algorithms are cut significantly to meet CPU requirements, they work much better compared to previous ones.
4. Scan, parse and analyze most recently used files of the target system.
5. Primitive dictionary attack. The application checks all passwords from the built-in dictionary for the Light and Standard editions or from several dictionaries (Arabic, Chinese, English, French, German, Portuguese, Russian, Spanish) for the Advanced Edition. If the deep search option is on, simple word mutations will also be taken into account during the search.
6. Primitive brute-force attack.
7. Artificial Intelligence attack. This is our little 'know-how'. The attack analyzes network activity of a user on the computer. Over thirty mini-modules take care of that. Upon the results of the analysis, the application generates user preferences and generates a semantic dictionary for the attack, which it later uses it for finding the password.
8. Look for passwords in deleted files, temporary folders and so on.

9. Primitive Fingerprint attack on some complicated English passwords.
10. Extract strings from huge files: RAM images, hiberfil.sys, pagefile.sys and so on. When this option is set, the program will try to skip files useless in password analysis like video, archives, audio files, etc.
11. Search passwords by reading and analyzing raw sectors of the selected drive. This feature works for both LM and NTLM hashes, looking for both ASCII and UNICODE passwords. If the '*Password mutation level*' is set to '*Favor efficiency*', the program additionally tries to mutate all found passwords, thus walking through all sectors of the target drive may take quite a time. Note that the sector-based scanning algorithm is not effective against drives which have a full-disk encryption set on. Like Bitlocker or TrueCrypt, for example.

To apply a custom recovery method, turn on the 'Custom recovery' option and select one of the available attacks. On the next step you will be prompted to set up various options related to the selected attack.

Selecting data source



Searching user passwords (step 3 of 4)

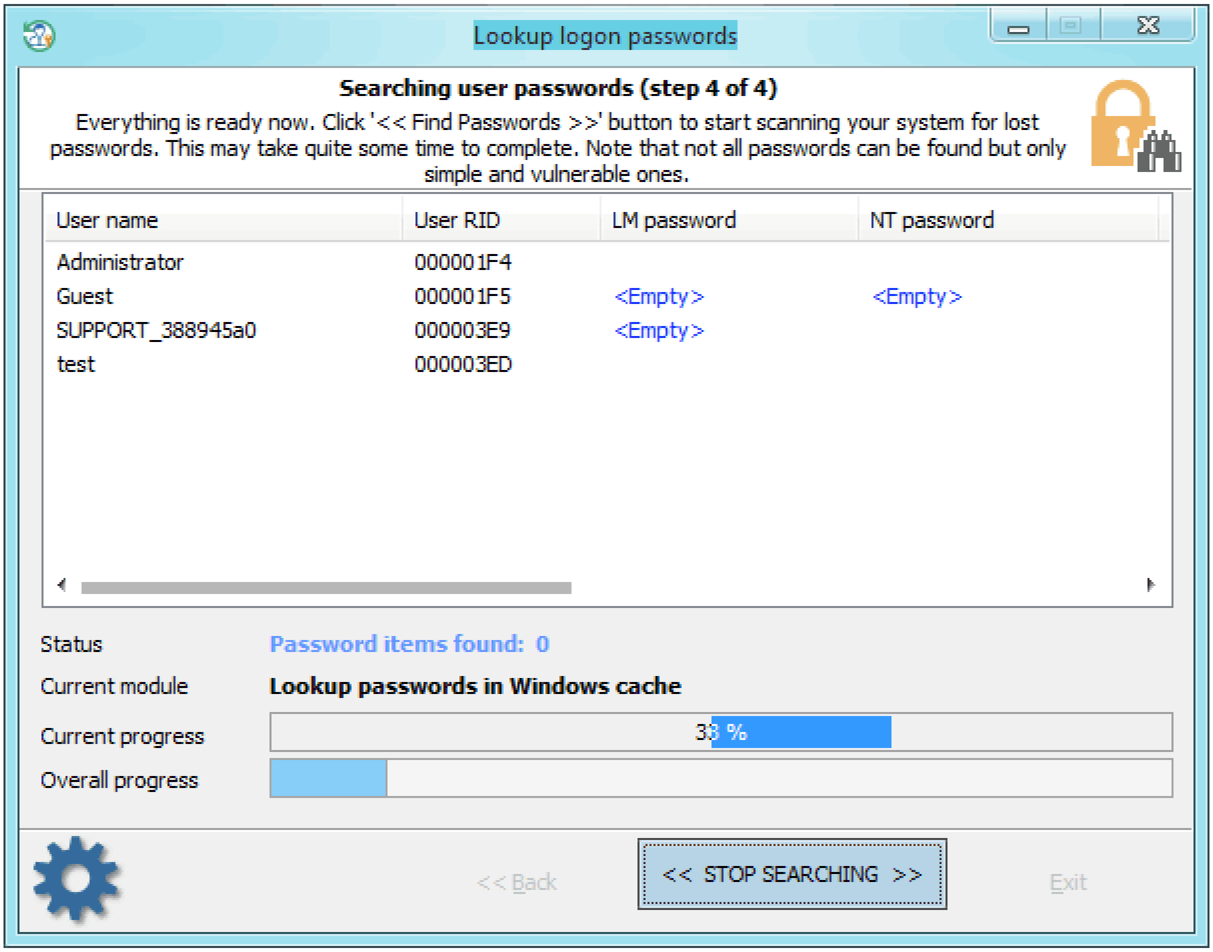
You should provide files and folders required for successful recovery. Typical location for profiles directory: C:\Documents And Settings. Typical location for program files folder: C:\Program Files.

Files and folders required for successful recovery

Path to Active Directory database	
SAM registry file	C:\Windows\System32\Config\SAM
SYSTEM registry file	C:\Windows\System32\Config\SYSTEM
SECURITY registry file	C:\Windows\System32\Config\SECURITY
SOFTWARE registry file	C:\Windows\System32\Config\SOFTWARE
Profiles directory	C:\Users
Program files directory	C:\Program Files

When searching for passwords, special attention is to be paid to entering files and folders required for the analysis process. Without those, password search will be inefficient. The application finds the files automatically, but sometimes, e.g., when the computer has several operating systems installed, you may need to use the 'manual control'. Please also keep in mind that if the computer has 2 or more hard disk drives, the sequence of the letters for these disks can be set totally different than in the original system.

Searching and decrypting passwords



Searching user passwords (step 4 of 4)

Everything is ready now. Click '<< Find Passwords >>' button to start scanning your system for lost passwords. This may take quite some time to complete. Note that not all passwords can be found but only simple and vulnerable ones.

User name	User RID	LM password	NT password
Administrator	000001F4		
Guest	000001F5	<Empty>	<Empty>
SUPPORT_388945a0	000003E9	<Empty>	
test	000003ED		

Status: Password items found: 0
Current module: Lookup passwords in Windows cache
Current progress: 33 %
Overall progress

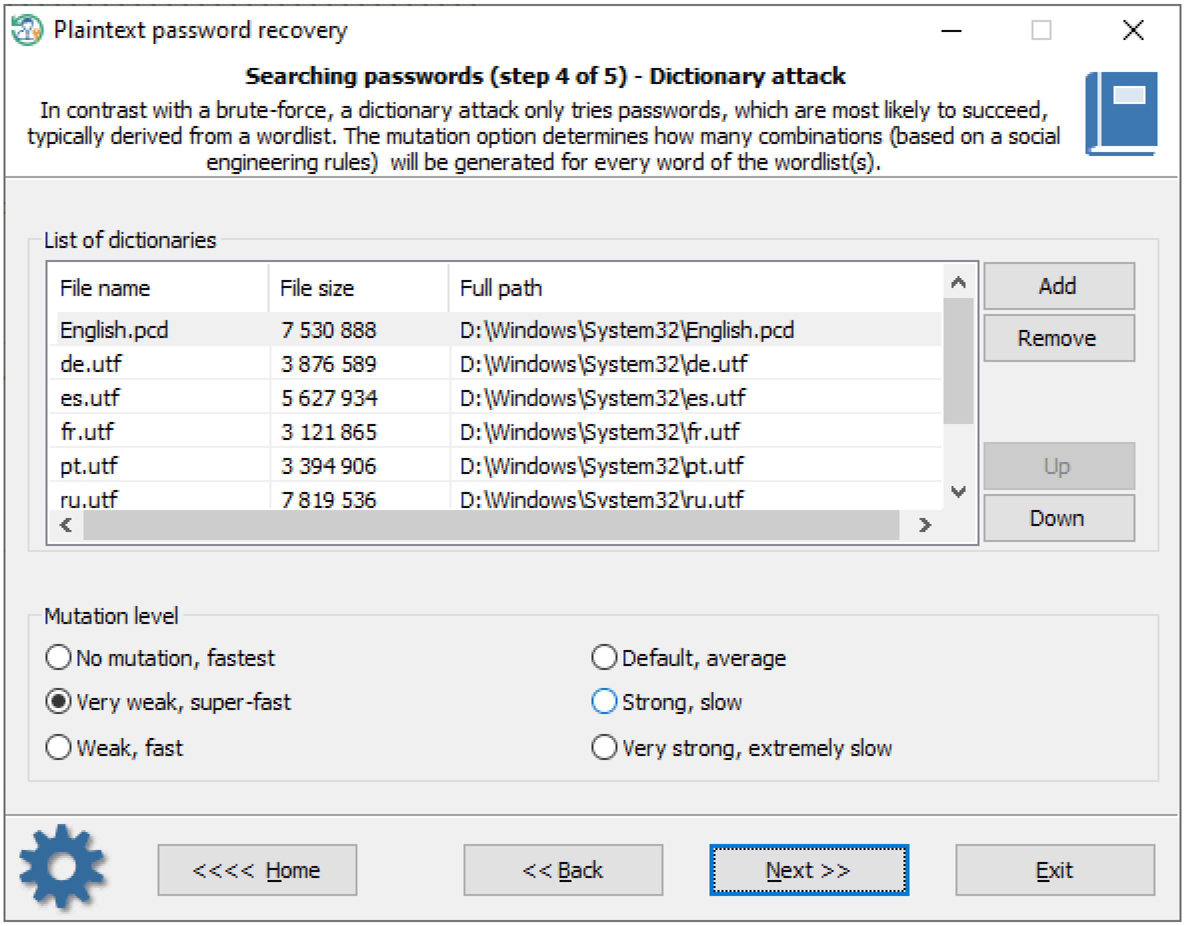
Finding/analyzing passwords can take some time, which depends on attack settings and peculiarities of your system. Completing the search normally takes approximately 10-15 minutes without Passcape table and disk search attacks. The Passcape table attack takes much longer and depends on your CPU and the number of hashes to recover. For example, on a 2-core CPU it takes usually up to 3 minutes for a single hash.

3.5.1.1 Custom recovery

Once the custom recovery option is set, the program can additionally run 3 different attacks to guess the passwords:

- Dictionary attack
- Hybrid attack
- Mask attack

Dictionary attack


Plaintext password recovery

Searching passwords (step 4 of 5) - Dictionary attack

In contrast with a brute-force, a dictionary attack only tries passwords, which are most likely to succeed, typically derived from a wordlist. The mutation option determines how many combinations (based on a social engineering rules) will be generated for every word of the wordlist(s).

List of dictionaries

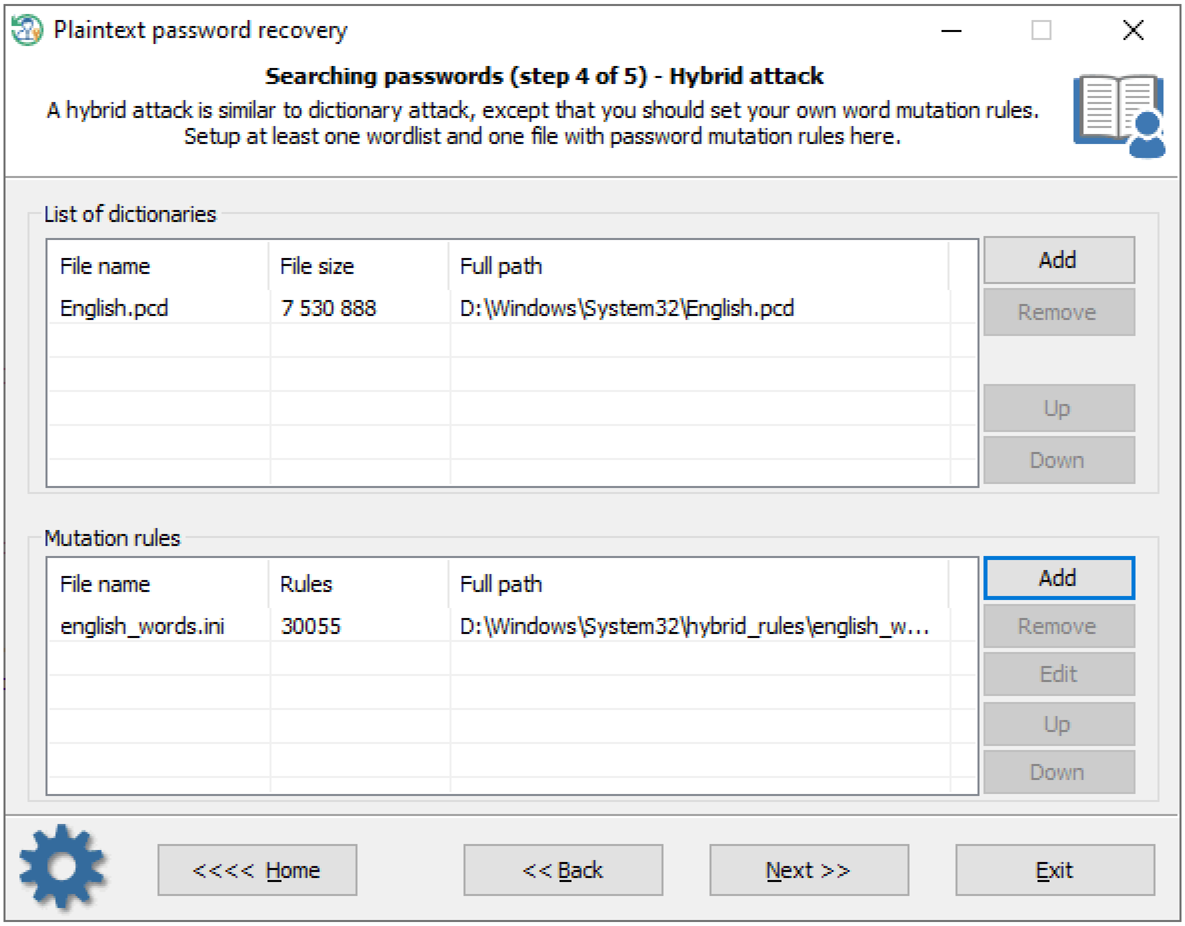
File name	File size	Full path
English.pcd	7 530 888	D:\Windows\System32\English.pcd
de.utf	3 876 589	D:\Windows\System32\de.utf
es.utf	5 627 934	D:\Windows\System32\es.utf
fr.utf	3 121 865	D:\Windows\System32\fr.utf
pt.utf	3 394 906	D:\Windows\System32\pt.utf
ru.utf	7 819 536	D:\Windows\System32\ru.utf

Mutation level

○ No mutation, fastest
● Very weak, super-fast
○ Weak, fast
○ Default, average
○ Strong, slow
○ Very strong, extremely slow

A dictionary attack tries passwords, which are most likely to succeed, typically derived from a wordlist. RWP supports for different types of dictionaries: ASCII, UNICODE, UTF8, as well as encrypted/compressed dictionaries in the native PCD format. You can use both predefined and custom dictionaries. To add your own wordlist, copy one to a USB drive and attach the drive to the target PC. The mutation level determines how many combinations (based on social engineering rules) will be generated for every word of the wordlist(s).

Hybrid attack



Plaintext password recovery

Searching passwords (step 4 of 5) - Hybrid attack

A hybrid attack is similar to dictionary attack, except that you should set your own word mutation rules. Setup at least one wordlist and one file with password mutation rules here.

List of dictionaries

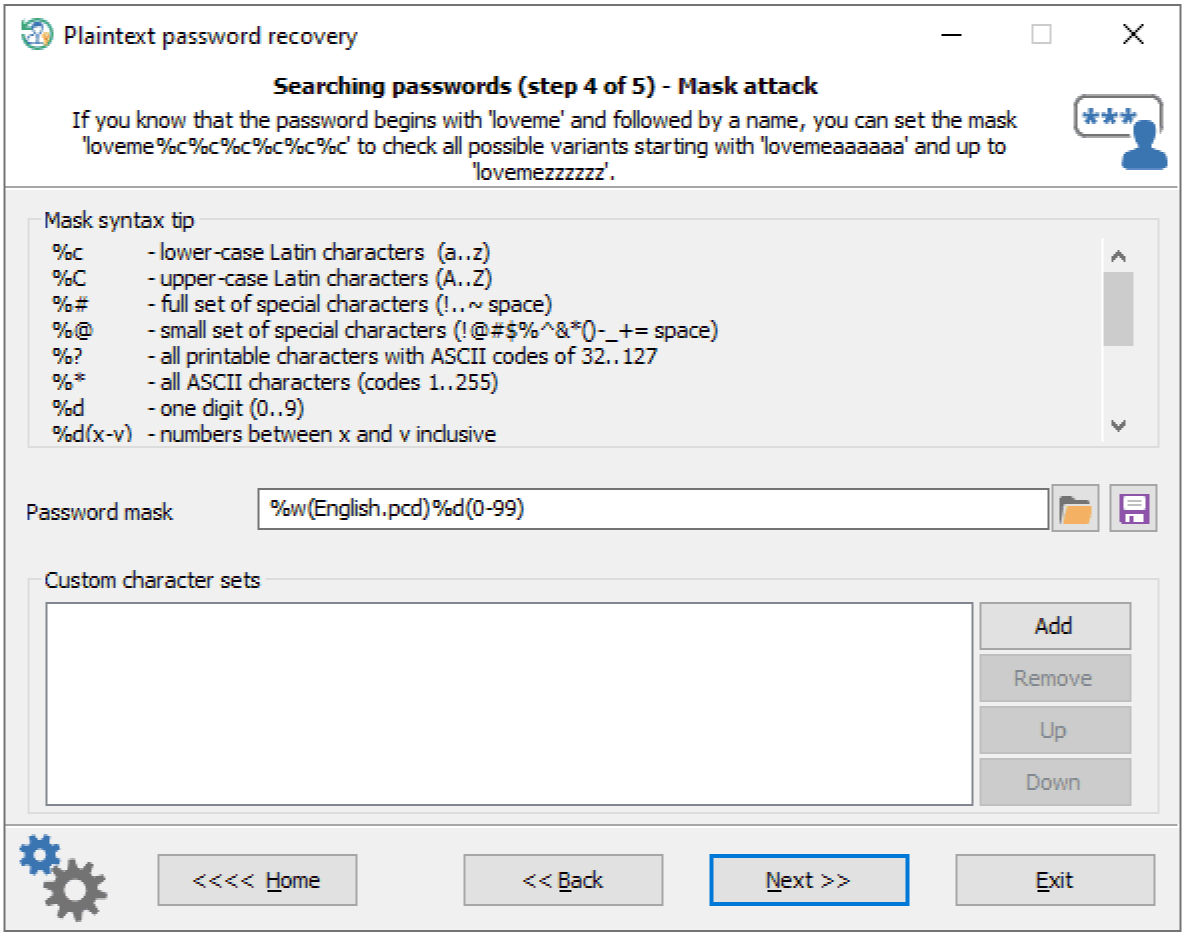
File name	File size	Full path
English.pcd	7 530 888	D:\Windows\System32\English.pcd

Mutation rules

File name	Rules	Full path
english_words.ini	30055	D:\Windows\System32\hybrid_rules\english_w...

A hybrid attack is similar to a dictionary one, except that you can set your own word mutation rules. The program comes with a huge set of rule-files. Just use one that is best for your task. The good thing in a Hybrid attack is that you can additionally create, edit and modify password mutation rules according to your needs.

Mask attack



Plaintext password recovery

Searching passwords (step 4 of 5) - Mask attack

If you know that the password begins with 'loveme' and followed by a name, you can set the mask 'loveme%c%c%c%c%c%c' to check all possible variants starting with 'lovemeaaaaaa' and up to 'lovemezzzzzz'.

Mask syntax tip

%c	- lower-case Latin characters (a..z)
%C	- upper-case Latin characters (A..Z)
%#	- full set of special characters (!..~ space)
%@	- small set of special characters (!@#$%^&*()-_+= space)
%?	- all printable characters with ASCII codes of 32..127
%*	- all ASCII characters (codes 1..255)
%d	- one digit (0..9)
%d(x-y)	- numbers between x and y inclusive

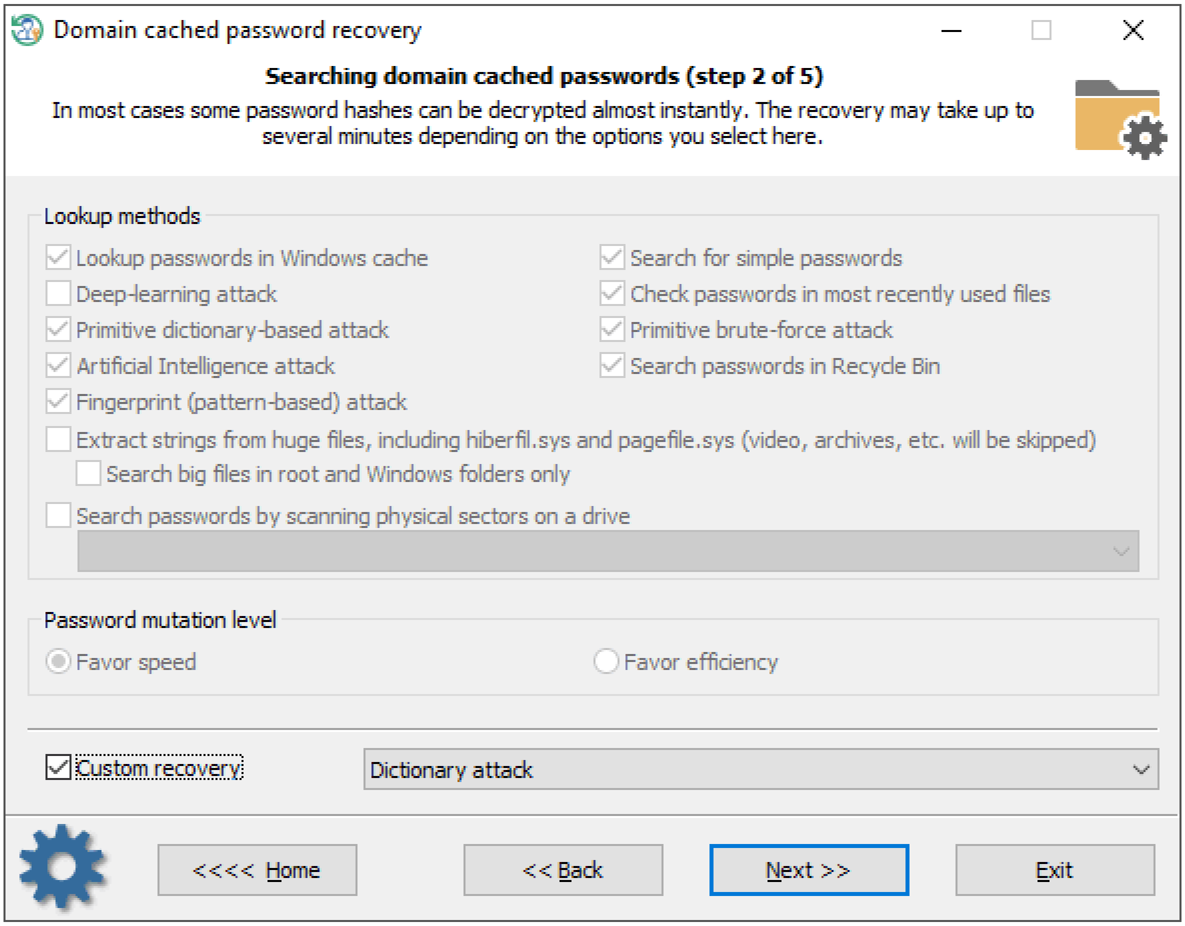
Password mask: %w(English.pcd)%d(0-99)

Custom character sets

A Mask attack is an irreplaceable tool when you know a part of the password or have any specific details about it. For example, if you know that the password consists of 12 characters and starts with 'loveme', obviously it's just enough to guess the last 6 characters of the password. That is what the mask attack is for. In our example, you can set the following mask: loveme%c%c%c%c%c%c
To get more information about how the mask works, please refer to our online documentation.

3.5.2 Search for domain cached passwords

Setting search and recovery options



Domain cached password recovery

Searching domain cached passwords (step 2 of 5)

In most cases some password hashes can be decrypted almost instantly. The recovery may take up to several minutes depending on the options you select here.

Lookup methods

☑ Lookup passwords in Windows cache
☐ Deep-learning attack
☑ Primitive dictionary-based attack
☑ Artificial Intelligence attack
☑ Fingerprint (pattern-based) attack
☑ Search for simple passwords
☑ Check passwords in most recently used files
☑ Primitive brute-force attack
☑ Search passwords in Recycle Bin
☐ Extract strings from huge files, including hiberfil.sys and pagefile.sys (video, archives, etc. will be skipped)
☐ Search big files in root and Windows folders only
☐ Search passwords by scanning physical sectors on a drive

Password mutation level

● Favor speed ○ Favor efficiency

☑ Custom recovery: Dictionary attack

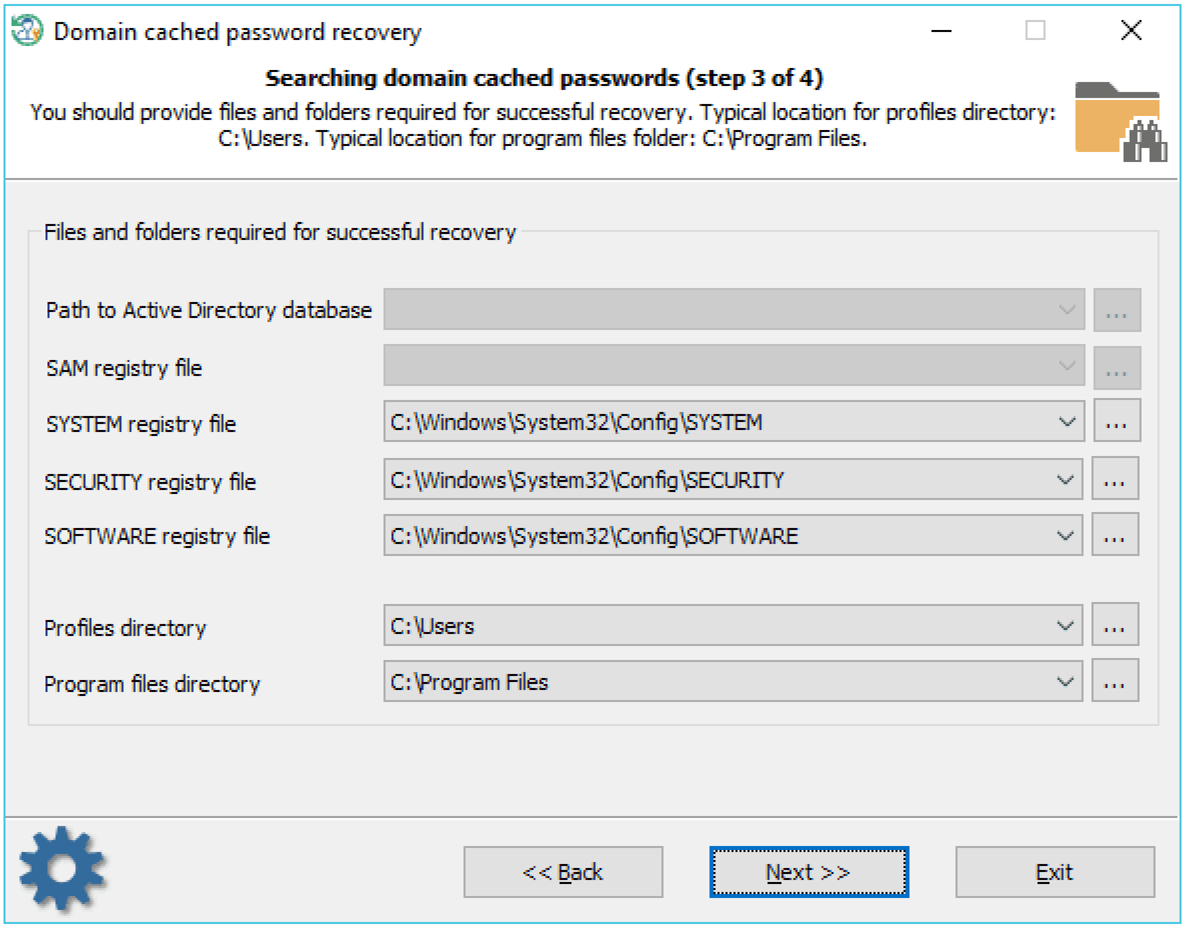
Domain cached password recovery consists of several modules. Each one can be turned on/off separately:

1. Finding information in Windows system cache. This module consists of over a dozen of mini-attacks, during which the program analyzes all kinds of system passwords: LSA secrets, DSL, FTP, LAN, WAN passwords, Internet and email credentials, etc. Later the found passwords are used by the program to check other passwords by generating more complex variations.
2. Analyzing simple, short and numeric passwords, keyboard combinations, etc. Over 20 mini-modules in total.
3. Scanning, reading and analyzing most recently used files of the target system. The program parses the files and creates a list of words (by generating various mutations) to be checked as passwords.
4. Primitive dictionary attack. The application checks all passwords from the built-in dictionary for the Light and Standard editions or from several dictionaries (Arabic, Chinese, English, French, German, Portuguese, Russian, Spanish) for the Advanced Edition. If the deep search option is on, simple word mutations will also be taken into account during the search.
5. Primitive brute-force module that consists of several simple attacks to search for short passwords.
6. Artificial Intelligence module analyzes network activity of users on the target computer. Over thirty mini-modules take care of that. Upon the results of the analysis, the application generates user preferences and creates a semantic dictionary for the attack. Then the dictionary is uses for guessing passwords.
7. Looking for passwords in deleted files, temporary folders, etc.
8. Primitive Fingerprint attack on English passwords. This module may take a lot of time to complete.
9. Extract strings from huge files: RAM images, hiberfil.sys, pagefile.sys and so on. The program can skip files useless in password analysis like video, archives, audio files, etc.
10. Searching for passwords by reading and analyzing raw sectors of the selected drive. If the Password mutation level is set to '*Favor efficiency*', the program additionally tries to mutate all found passwords as well, thus

walking through all sectors of the target drive may take quite a time. This module is not effective for drives which have a full-disk encryption set on. Like Bitlocker or TrueCrypt, for example.

To apply a custom recovery method, turn on the 'Custom recovery' option and select one of the available attacks. On the next step you will be prompted to set up various options related to the selected attack.

Selecting data source



Domain cached password recovery

Searching domain cached passwords (step 3 of 4)

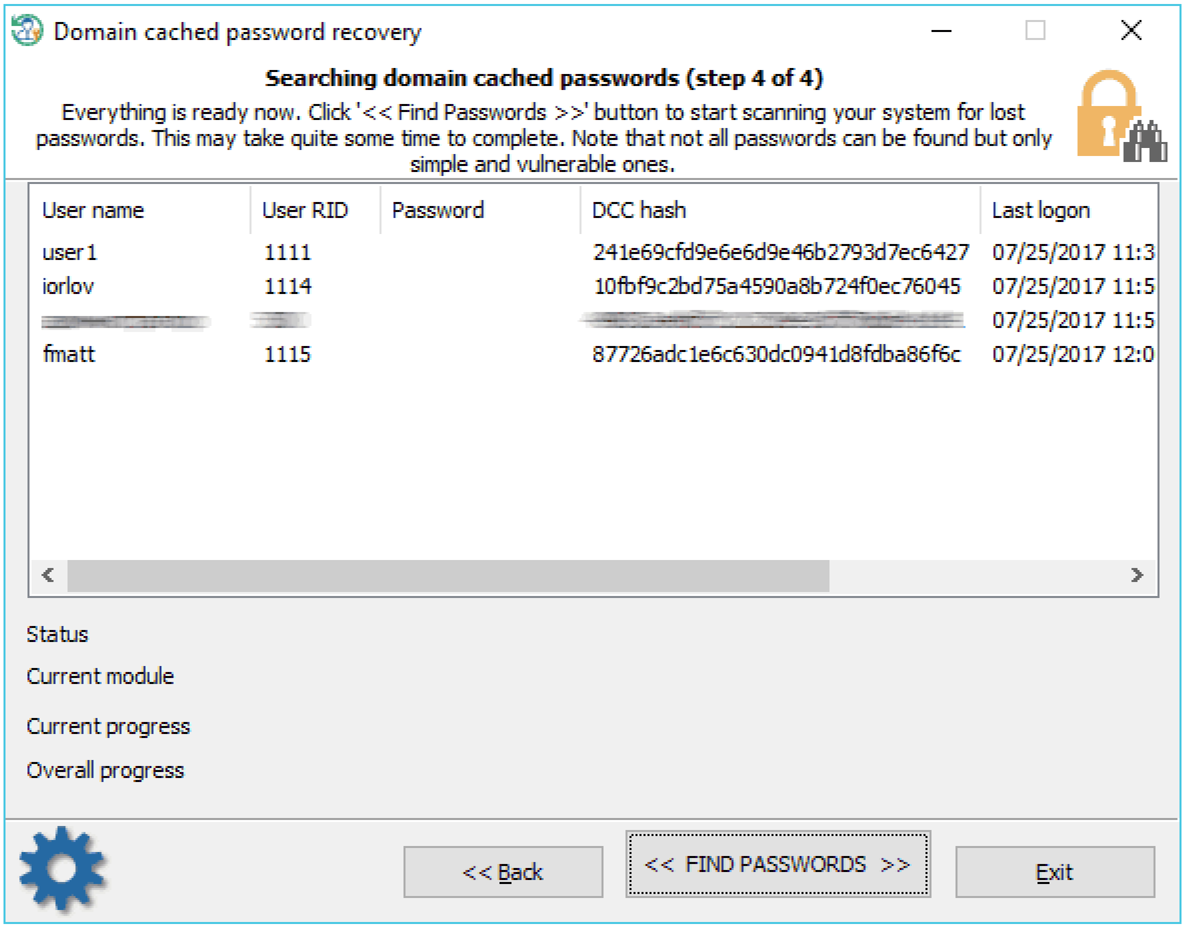
You should provide files and folders required for successful recovery. Typical location for profiles directory: C:\Users. Typical location for program files folder: C:\Program Files.

Files and folders required for successful recovery

Path to Active Directory database	
SAM registry file	
SYSTEM registry file	C:\Windows\System32\Config\SYSTEM
SECURITY registry file	C:\Windows\System32\Config\SECURITY
SOFTWARE registry file	C:\Windows\System32\Config\SOFTWARE
Profiles directory	C:\Users
Program files directory	C:\Program Files

When searching for domain cached passwords, special attention is to be paid to proper setting files and folders required for the process. RWP finds the files automatically, but sometimes, e.g., when the computer has several operating systems installed, you may need to adjust it manually. Also keep in mind that if the target PC has 2 or more hard disk drives, the sequence of the letters for these disks can be set totally different than in the original system.

Searching for domain cached passwords



Searching domain cached passwords (step 4 of 4)

Everything is ready now. Click '<< Find Passwords >>' button to start scanning your system for lost passwords. This may take quite some time to complete. Note that not all passwords can be found but only simple and vulnerable ones.

User name	User RID	Password	DCC hash	Last logon
user1	1111		241e69cfd9e6e6d9e46b2793d7ec6427	07/25/2017 11:3
iorlov	1114		10fbf9c2bd75a4590a8b724f0ec76045	07/25/2017 11:5
[redacted]	[redacted]		[redacted]	07/25/2017 11:5
fmatt	1115		87726adc1e6c630dc0941d8fdba86f6c	07/25/2017 12:0

Status

Current module

Current progress

Overall progress

Domain cached credentials are of two types. DCC type 1 has very weak encryption and was used in Windows 2000, Windows XP and Windows 2003 OSes. Recovery rate can exceed millions or even billions passwords per second. DCC type 2 is used in Windows Vista and later operating systems. Its encryption is much much stronger and quite resistant to cracking. The brute-force speed is only hundreds/thousands passwords per second. Just imagine, guessing an 8 character long password consisting of upper and lower case letters using brute-force attack might take over 1000 years!

Do take into account the following considerations:

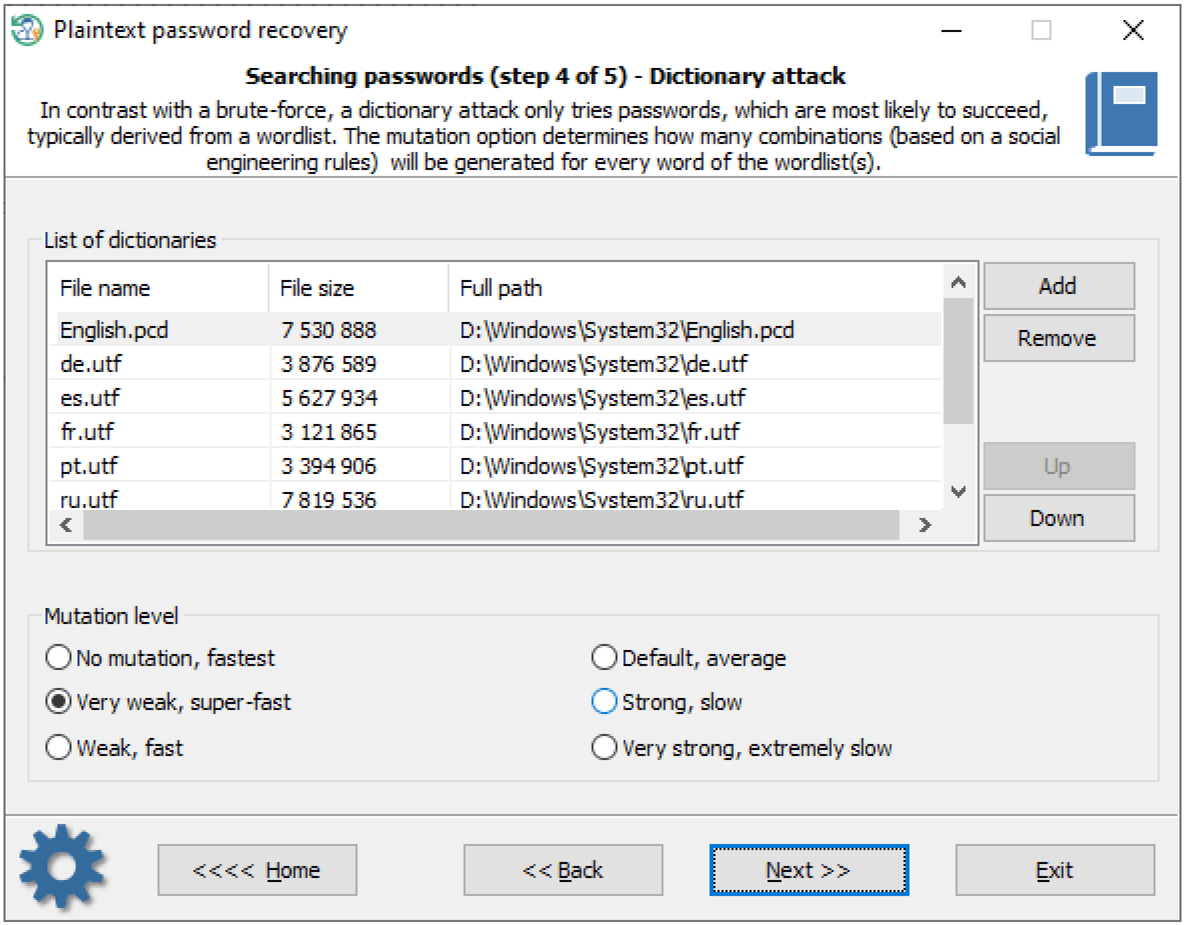
- Process of searching for DCC type 2 is extremely slow. Completing some modules (for example, Fingerprint attack) may take hours or even days.
- To speed up the search, select only account you need the password for. Just right-click the cached entry and select '*Exclude from search all entries except selected*'. Otherwise, the speed of the password recovery will decrease by a multiple of the number of accounts.

3.5.2.1 Custom recovery

Once the custom recovery option is set, the program can additionally run 3 different attacks to guess the passwords:

- Dictionary attack
- Hybrid attack
- Mask attack

Dictionary attack



Plaintext password recovery

Searching passwords (step 4 of 5) - Dictionary attack

In contrast with a brute-force, a dictionary attack only tries passwords, which are most likely to succeed, typically derived from a wordlist. The mutation option determines how many combinations (based on a social engineering rules) will be generated for every word of the wordlist(s).

List of dictionaries

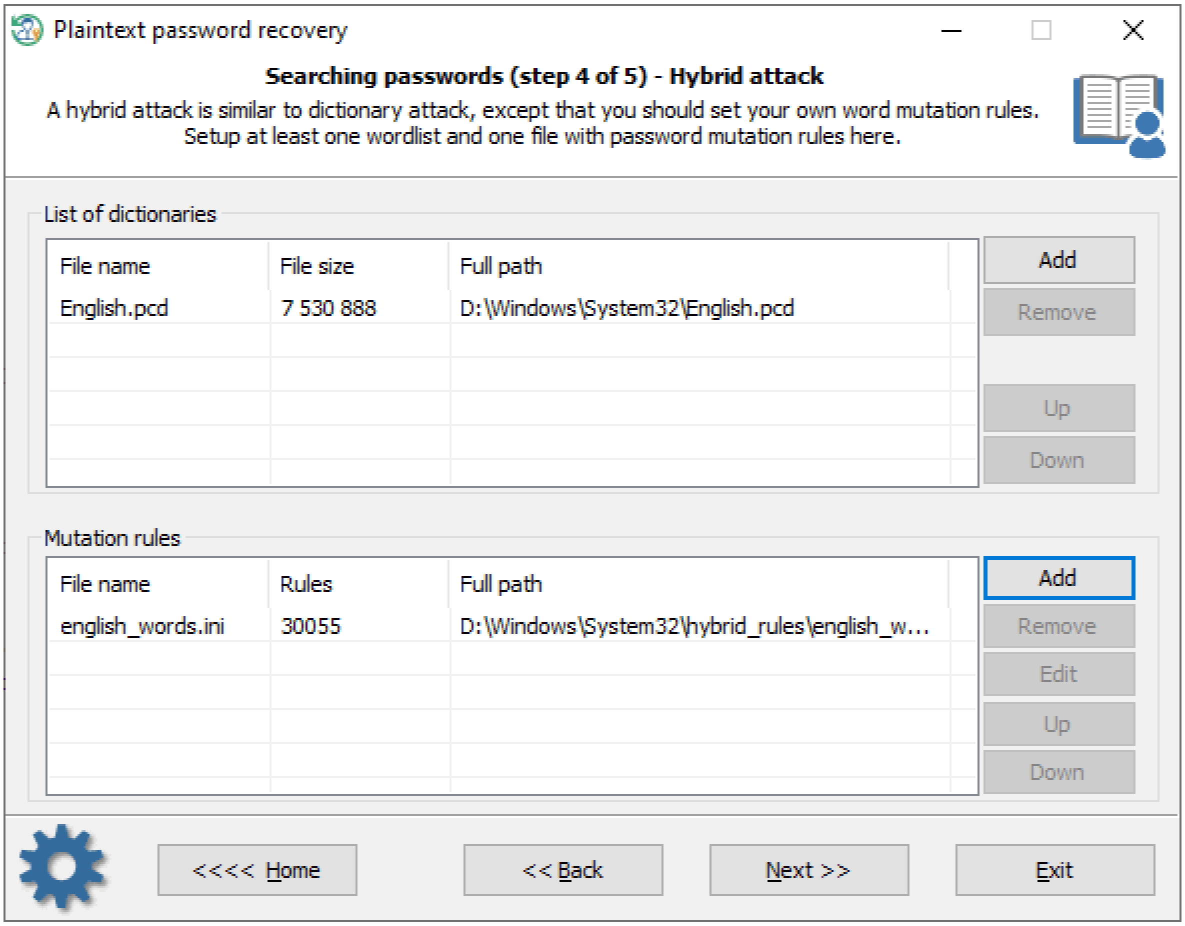
File name	File size	Full path
English.pcd	7 530 888	D:\Windows\System32\English.pcd
de.utf	3 876 589	D:\Windows\System32\de.utf
es.utf	5 627 934	D:\Windows\System32\es.utf
fr.utf	3 121 865	D:\Windows\System32\fr.utf
pt.utf	3 394 906	D:\Windows\System32\pt.utf
ru.utf	7 819 536	D:\Windows\System32\ru.utf

Mutation level

○ No mutation, fastest
● Very weak, super-fast
○ Weak, fast
○ Default, average
○ Strong, slow
○ Very strong, extremely slow

A dictionary attack tries passwords, which are most likely to succeed, typically derived from a wordlist. RWP supports for different types of dictionaries: ASCII, UNICODE, UTF8, as well as encrypted/compressed dictionaries in the native PCD format. You can use both predefined and custom dictionaries. To add your own wordlist, copy one to a USB drive and attach the drive to the target PC. The mutation level determines how many combinations (based on a social engineering rules) will be generated for every word of the wordlist(s).

Hybrid attack



Plaintext password recovery

Searching passwords (step 4 of 5) - Hybrid attack

A hybrid attack is similar to dictionary attack, except that you should set your own word mutation rules. Setup at least one wordlist and one file with password mutation rules here.

List of dictionaries

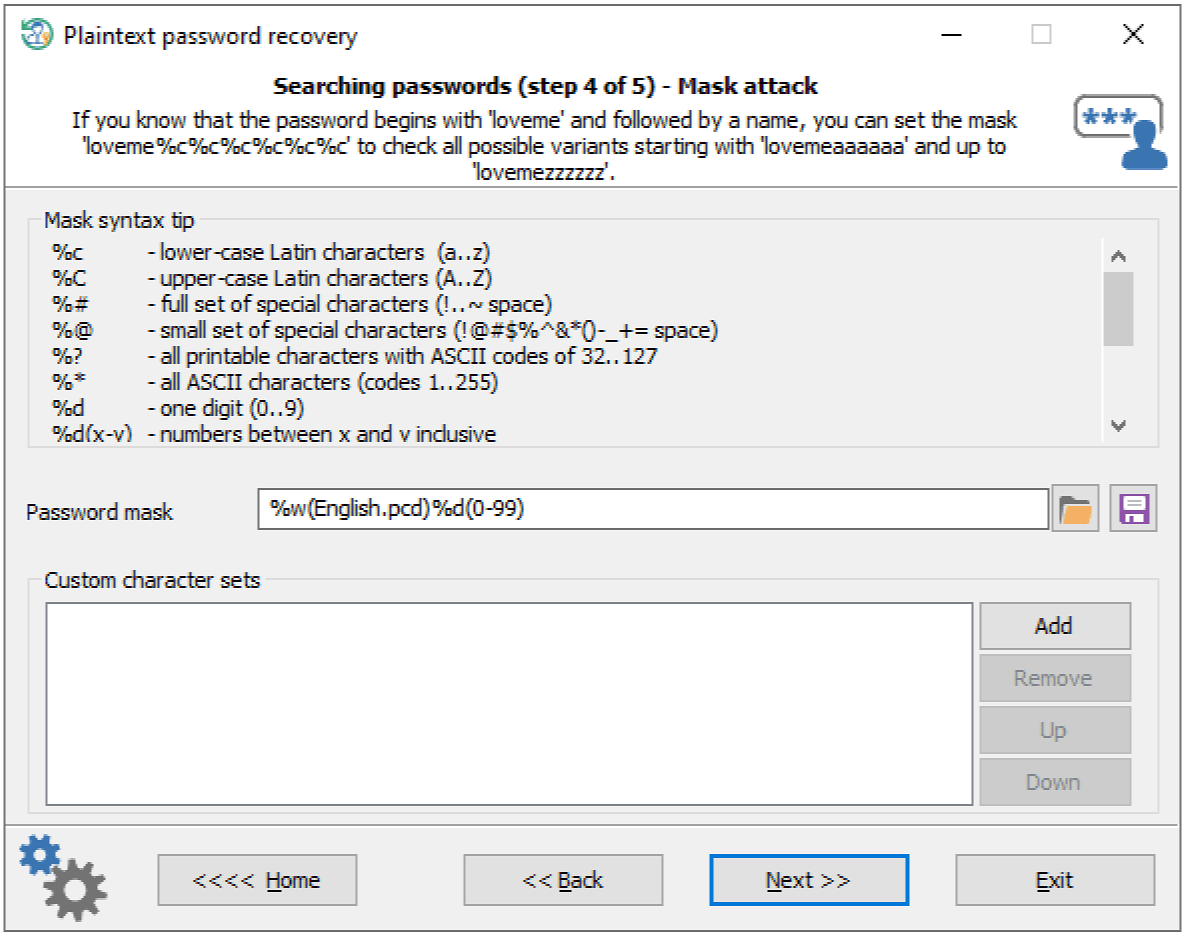
File name	File size	Full path
English.pcd	7 530 888	D:\Windows\System32\English.pcd

Mutation rules

File name	Rules	Full path
english_words.ini	30055	D:\Windows\System32\hybrid_rules\english_w...

A hybrid attack is similar to a dictionary one, except that you can set your own word mutation rules. The program comes with a huge set of rule-files. Just use one that is best for your task. The good thing in a Hybrid attack is that you can additionally create, edit and modify password mutation rules according to your needs.

Mask attack



Searching passwords (step 4 of 5) - Mask attack

If you know that the password begins with 'loveme' and followed by a name, you can set the mask 'loveme%c%c%c%c%c%c' to check all possible variants starting with 'lovemeaaaaaa' and up to 'lovemezzzzzz'.

Mask syntax tip

%c	- lower-case Latin characters (a..z)
%C	- upper-case Latin characters (A..Z)
%#	- full set of special characters (!..~ space)
%@	- small set of special characters (!@#$%^&*()-_+= space)
%?	- all printable characters with ASCII codes of 32..127
%*	- all ASCII characters (codes 1..255)
%d	- one digit (0..9)
%d(x-y)	- numbers between x and y inclusive

Password mask: %w(English.pcd)%d(0-99)

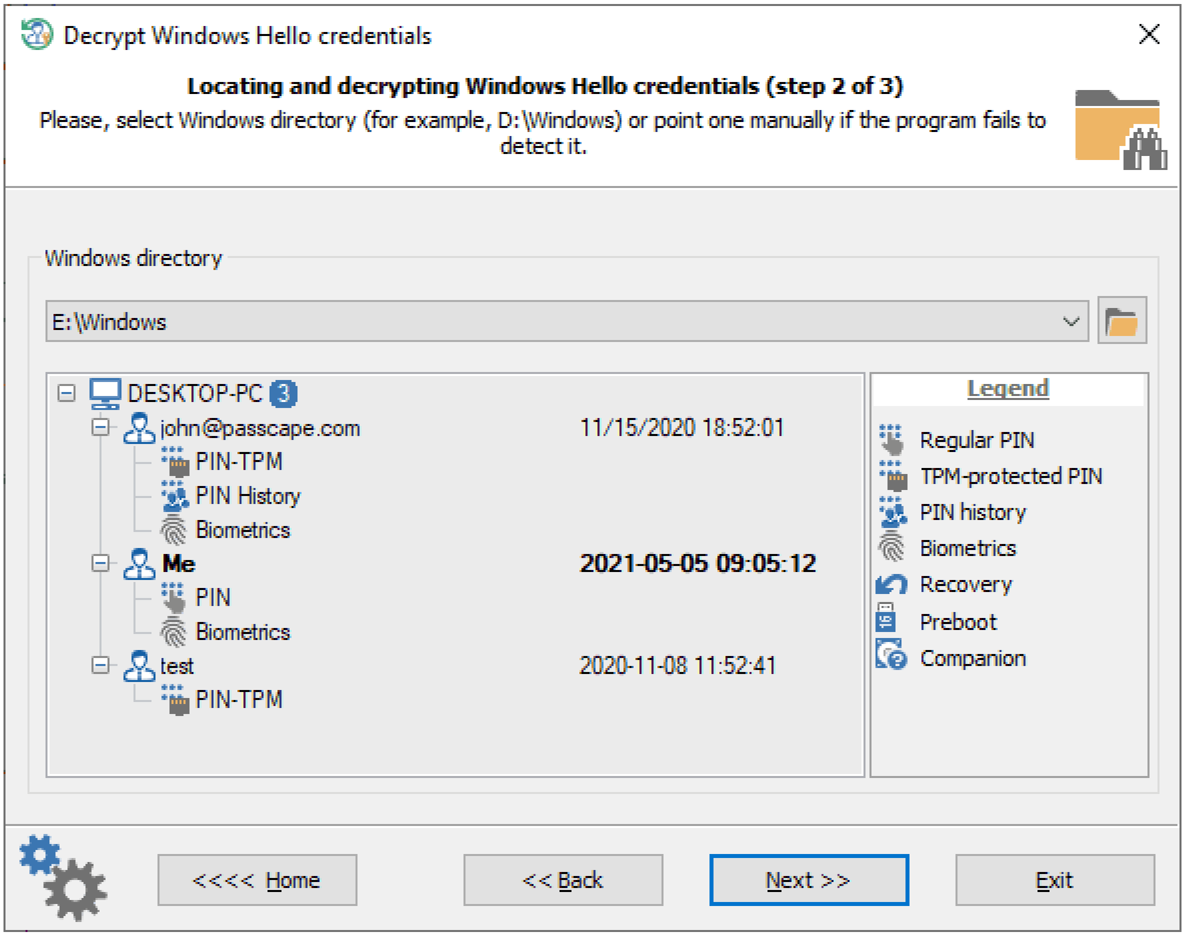
Custom character sets

A Mask attack is an irreplaceable tool when you know a part of the password or have any specific details about it. For example, if you know that the password consists of 12 characters and starts with 'loveme', obviously it's just enough to guess the last 6 characters of the password. That is what the mask attack is for. In our example, you can set the following mask: loveme%c%c%c%c%c%c
To get more information about how the mask works, please refer to our online documentation.

3.5.3 Decrypt Windows Hello credentials

Windows Hello is a biometric security system that allows Windows users to log into OS, applications and their devices without passwords but using a fingerprint, iris scan, facial or voice recognition. Windows Hello stores different types of users personal information: digital identities, PINs, plaintext logon passwords, etc.

Selecting Windows directory



Decrypt Windows Hello credentials

Locating and decrypting Windows Hello credentials (step 2 of 3)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it.

Windows directory

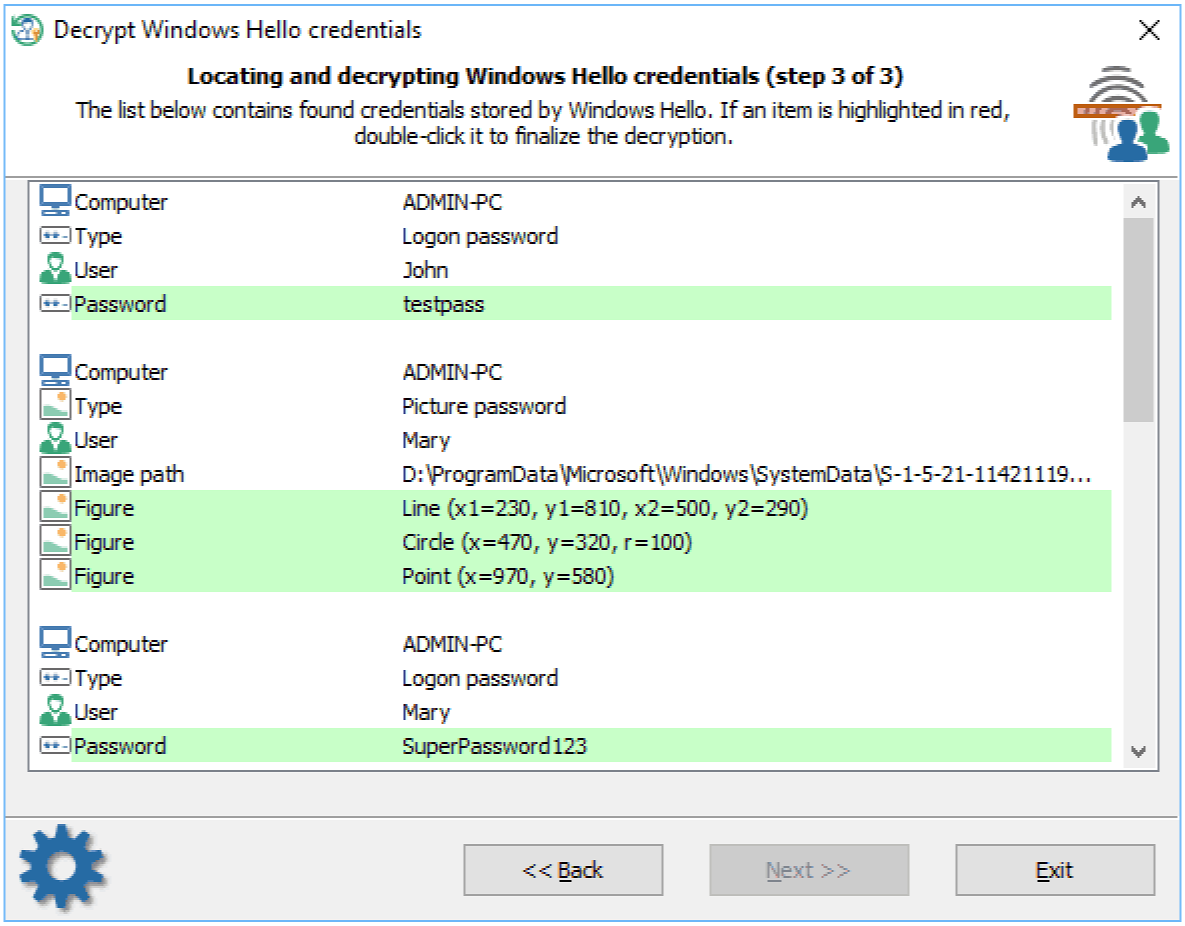
E:\Windows

DESKTOP-PC 3
john@passcape.com 11/15/2020 18:52:01
PIN-TPM
PIN History
Biometrics
Me **2021-05-05 09:05:12**
PIN
Biometrics
test 2020-11-08 11:52:41
PIN-TPM

Reset Windows Password recovers all kinds of personal data saved in Windows Hello except for some protected with TPM. First of all, you will need to specify the Windows directory of the target Windows 10 system. After the Windows directory is selected, the program analyzes the installed OS and displays a list of all available Windows Hello accounts, as well as the authentication methods they use. The last user logged in using Windows Hello is highlighted in bold. Here are the common Windows Hello authentication types:

- PIN - regular PIN authentication is available
- PIN-TPM - a TPM protection is set for PIN authentication
- PIN History - PIN history is present and can be decrypted
- Biometrics - a fingerprint authentication is used by the user

Decrypting passwords



Decrypt Windows Hello credentials

Locating and decrypting Windows Hello credentials (step 3 of 3)

The list below contains found credentials stored by Windows Hello. If an item is highlighted in red, double-click it to finalize the decryption.

Computer	ADMIN-PC
Type	Logon password
User	John
Password	testpass
Computer	ADMIN-PC
Type	Picture password
User	Mary
Image path	D:\ProgramData\Microsoft\Windows\SystemData\S-1-5-21-11421119...
Figure	Line (x1=230, y1=810, x2=500, y2=290)
Figure	Circle (x=470, y=320, r=100)
Figure	Point (x=970, y=580)
Computer	ADMIN-PC
Type	Logon password
User	Mary
Password	SuperPassword123

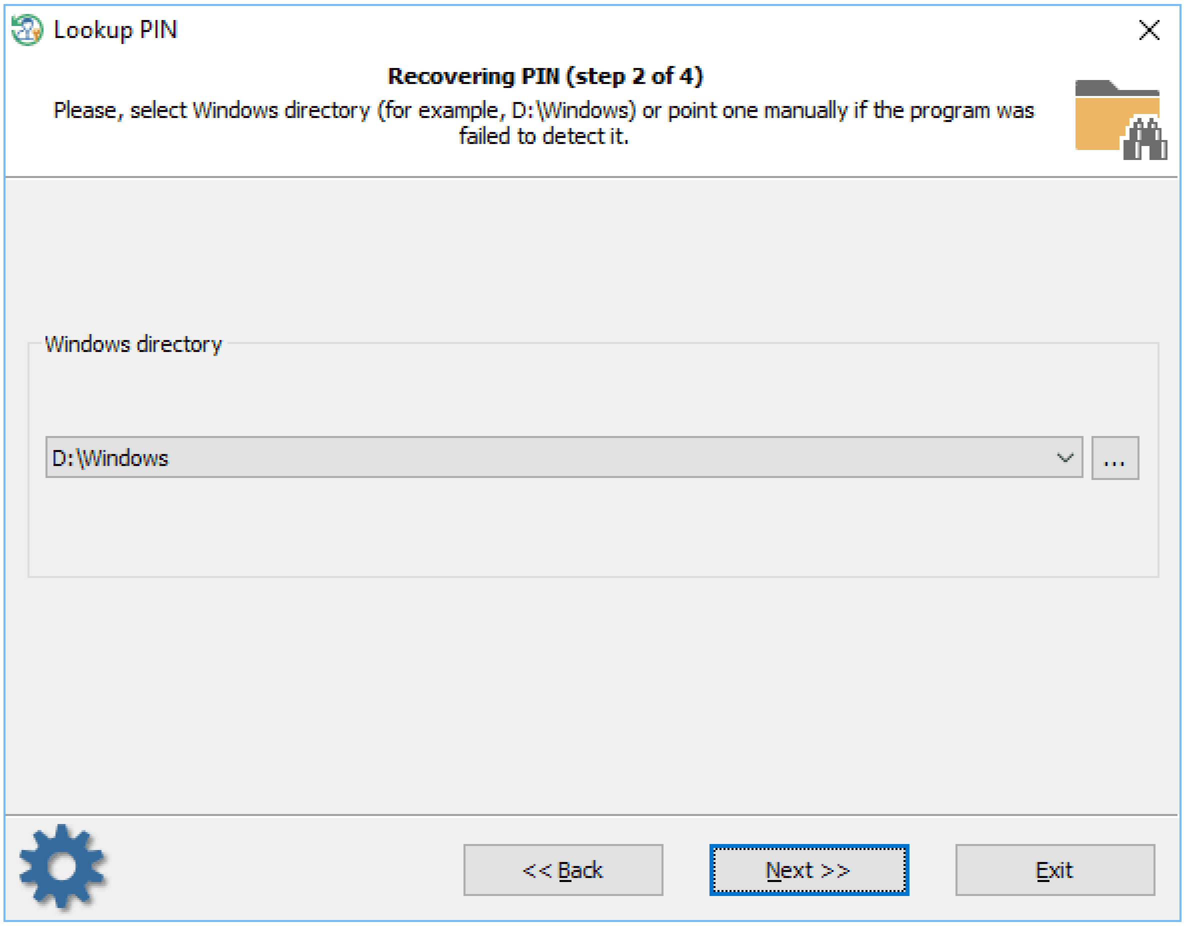
The program should then scan the target Windows directory for any personal data and output found information to the screen. Reset Windows Password automatically decrypts logon passwords if the user accounts was set up to logon using biometrics, for example, fingerprint or face recognition.

Some items in the table may be marked in red. It means that to finalize the decryption the program needs to know the PIN code of the user account. Double-click the item and type in the PIN that corresponds to the user account.

3.5.4 Lookup PIN

When you set up Windows Hello first, you're asked to create a PIN. The PIN is used as an alternative to biometric logon, when the biometric sensor is unavailable or not working properly. Unlike Windows 8, Windows 10 ensures very strong encryption (using even undocumented features and APIs) to protect PINs. Therefore, the problem of forgotten PIN's recovery is extremely vital and faces every user.

[Selecting Windows directory](#)



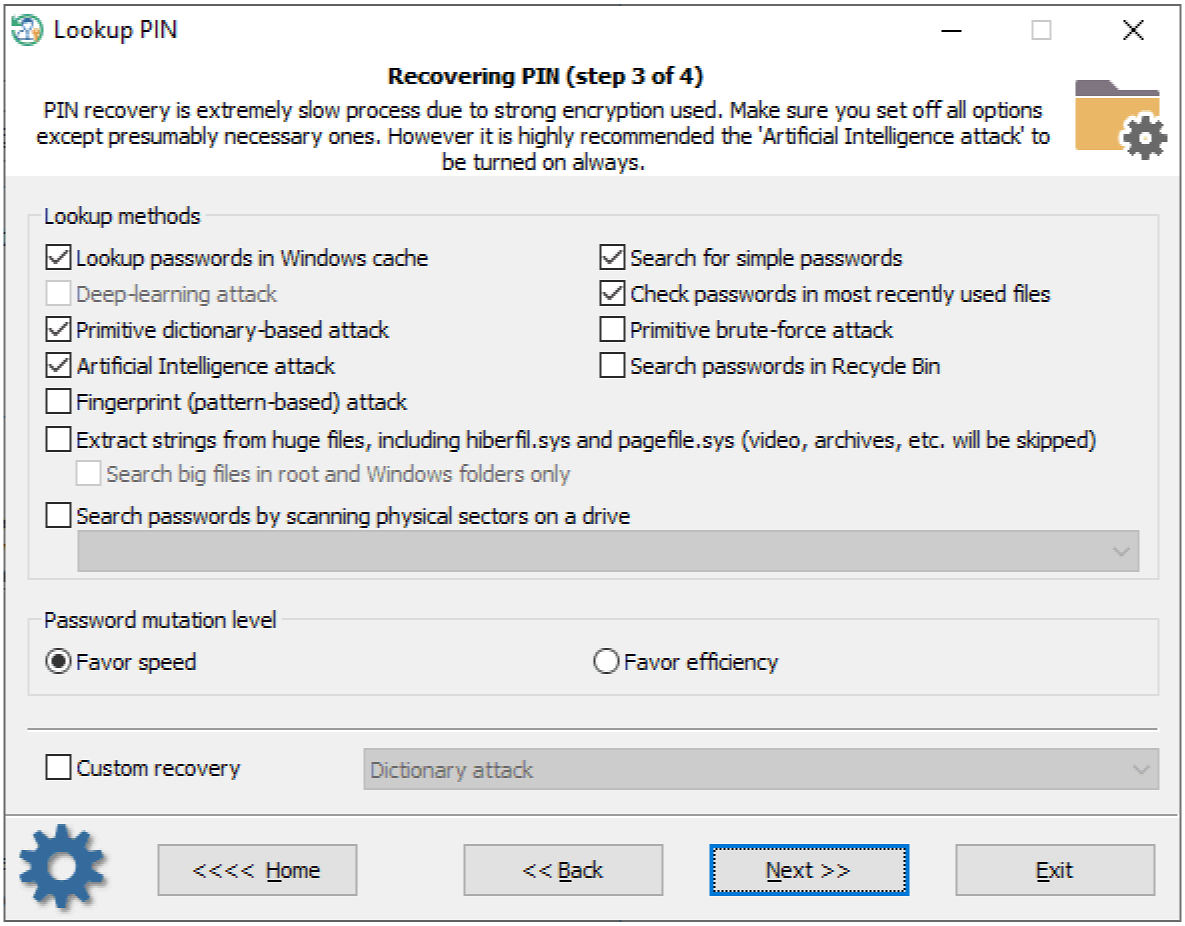
Recovering PIN (step 2 of 4)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program was failed to detect it.

Windows directory: D:\Windows

First of all, you should select the Windows directory or browse for it manually.

Setting up search and recovery options



Lookup PIN

Recovering PIN (step 3 of 4)

PIN recovery is extremely slow process due to strong encryption used. Make sure you set off all options except presumably necessary ones. However it is highly recommended the 'Artificial Intelligence attack' to be turned on always.

Lookup methods

☑ Lookup passwords in Windows cache
☐ Deep-learning attack
☑ Primitive dictionary-based attack
☑ Artificial Intelligence attack
☐ Fingerprint (pattern-based) attack
☑ Search for simple passwords
☑ Check passwords in most recently used files
☐ Primitive brute-force attack
☐ Search passwords in Recycle Bin
☐ Extract strings from huge files, including hiberfil.sys and pagefile.sys (video, archives, etc. will be skipped)
☐ Search big files in root and Windows folders only
☐ Search passwords by scanning physical sectors on a drive

Password mutation level

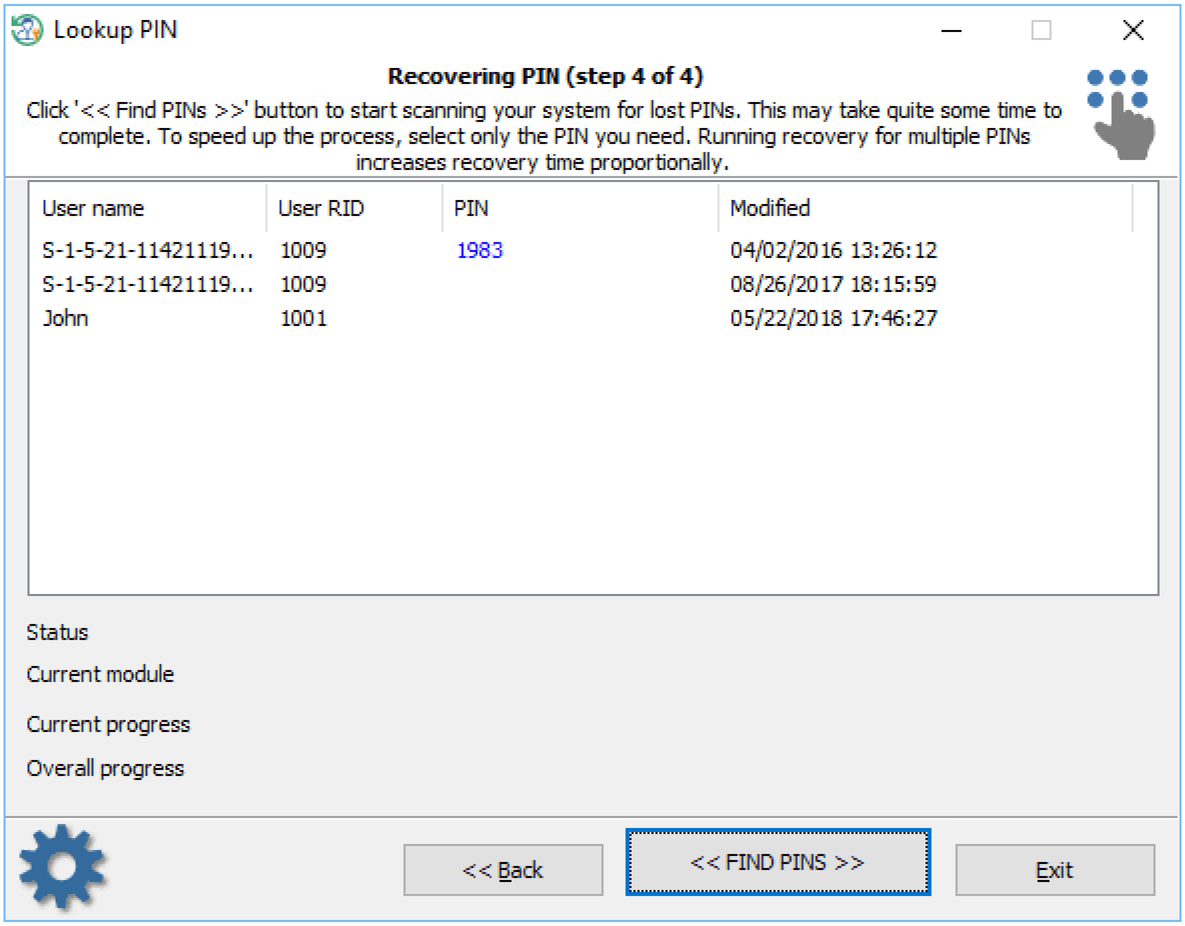
● Favor speed ○ Favor efficiency

☐ Custom recovery Dictionary attack

On the next step, the program offers available recovery methods used to search for PINs. The program's code is highly optimized for speed. But in spite of this, the process of searching for a PIN is extremely slow. For this reason, it is highly recommended to turn off most time-expensive attacks, for example, like on the picture above.

To apply a custom recovery method, turn on the 'Custom recovery' option and select one of the available attacks. On the next step you will be prompted to set up various options related to the selected attack.

Searching for PIN



Lookup PIN

Recovering PIN (step 4 of 4)

Click '<< Find PINs >>' button to start scanning your system for lost PINs. This may take quite some time to complete. To speed up the process, select only the PIN you need. Running recovery for multiple PINs increases recovery time proportionally.

User name	User RID	PIN	Modified
S-1-5-21-11421119...	1009	1983	04/02/2016 13:26:12
S-1-5-21-11421119...	1009		08/26/2017 18:15:59
John	1001		05/22/2018 17:46:27

Status

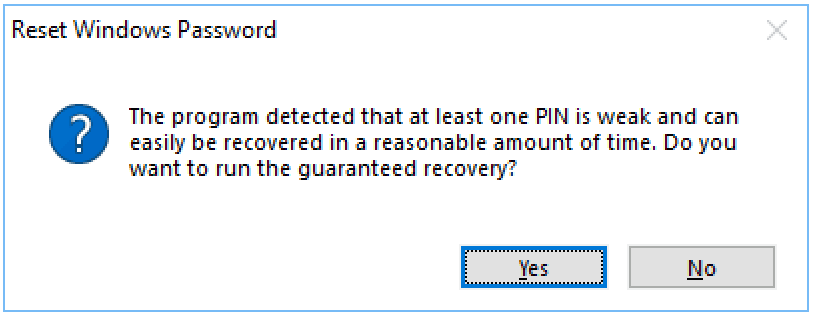
Current module

Current progress

Overall progress

The search speed is inversely proportional to the number of pins sought. That is, the more PIN codes are searched simultaneously, the lower the search speed. Therefore, it is recommended to exclude all unnecessary PINs from the search, and leave only necessary one. You can do it simply right-clicking on the PIN you need to recover and selecting *'Exclude all except selected*'. To start the process, hit the << FIND PINS >> button.

Do know that some PINs can be guaranteed to be decrypted in a reasonable amount of time. If the program can detect such a vulnerable PIN, it offers to launch the guaranteed recovery, just like on the screenshot below.



Reset Windows Password

The program detected that at least one PIN is weak and can easily be recovered in a reasonable amount of time. Do you want to run the guaranteed recovery?

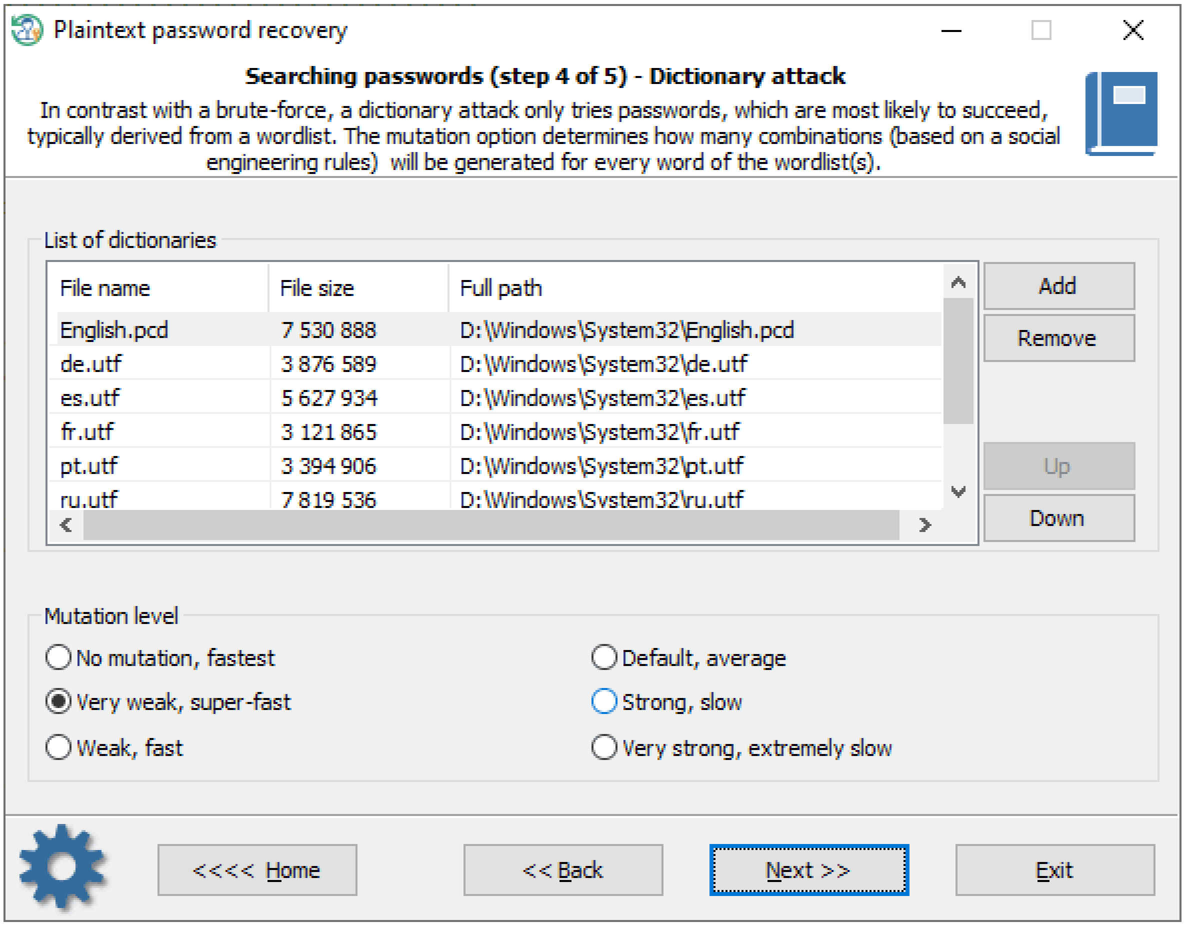
The latest version of the program implements so-called *Intelligent PIN recovery*. Every time a user tries to decrypt a Windows PIN, the program analyzes found PINs and, if some weak ones are found, offers an intelligent recovery. Initially, it launches the guaranteed recovery for the PINs that can be found in the fastest possible way, then goes time-consumptive ones, and at last, those with no guaranteed decryption but with a pattern-based search instead. A user can bypass the Intelligent recovery and launch the attack that was chosen during previous steps.

3.5.4.1 Custom recovery

Once the custom recovery option is set, the program can additionally run 3 different attacks to guess the passwords:

- Dictionary attack
- Hybrid attack
- Mask attack

Dictionary attack



Searching passwords (step 4 of 5) - Dictionary attack

In contrast with a brute-force, a dictionary attack only tries passwords, which are most likely to succeed, typically derived from a wordlist. The mutation option determines how many combinations (based on a social engineering rules) will be generated for every word of the wordlist(s).

List of dictionaries

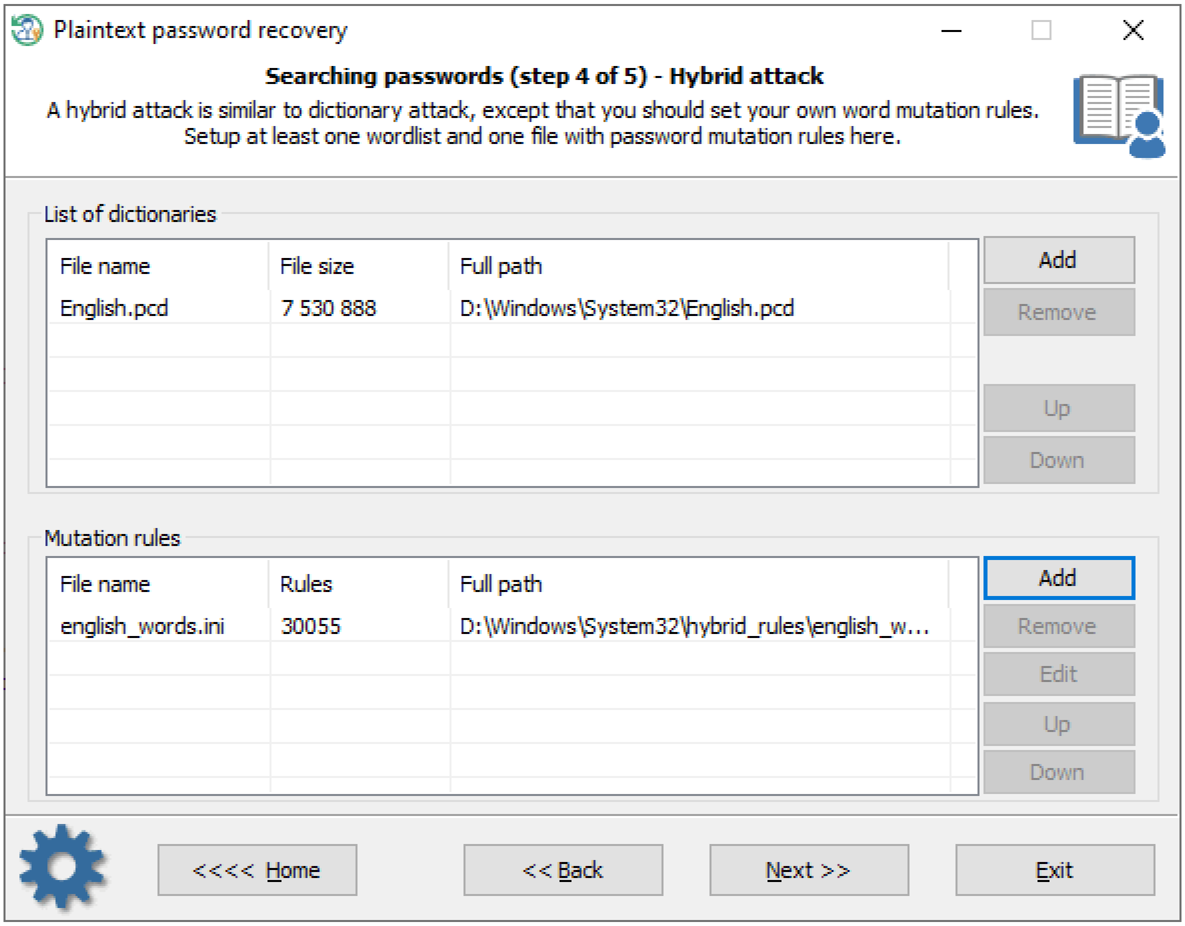
File name	File size	Full path
English.pcd	7 530 888	D:\Windows\System32\English.pcd
de.utf	3 876 589	D:\Windows\System32\de.utf
es.utf	5 627 934	D:\Windows\System32\es.utf
fr.utf	3 121 865	D:\Windows\System32\fr.utf
pt.utf	3 394 906	D:\Windows\System32\pt.utf
ru.utf	7 819 536	D:\Windows\System32\ru.utf

Mutation level

○ No mutation, fastest
● Very weak, super-fast
○ Weak, fast
○ Default, average
○ Strong, slow
○ Very strong, extremely slow

A dictionary attack tries passwords, which are most likely to succeed, typically derived from a wordlist. RWP supports for different types of dictionaries: ASCII, UNICODE, UTF8, as well as encrypted/compressed dictionaries in the native PCD format. You can use both predefined and custom dictionaries. To add your own wordlist, copy one to a USB drive and attach the drive to the target PC. The mutation level determines how many combinations (based on a social engineering rules) will be generated for every word of the wordlist(s).

Hybrid attack



Plaintext password recovery

Searching passwords (step 4 of 5) - Hybrid attack

A hybrid attack is similar to dictionary attack, except that you should set your own word mutation rules. Setup at least one wordlist and one file with password mutation rules here.

List of dictionaries

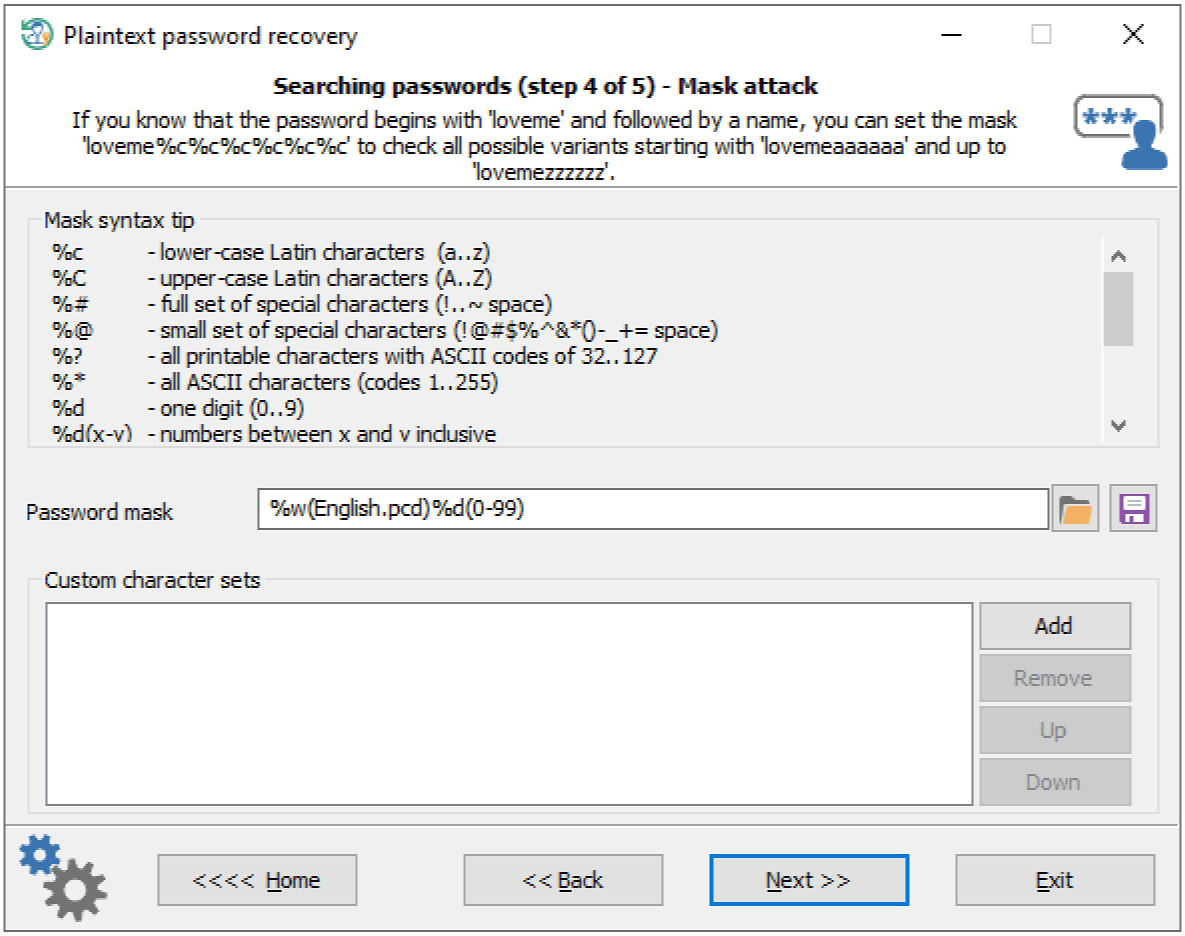
File name	File size	Full path
English.pcd	7 530 888	D:\Windows\System32\English.pcd

Mutation rules

File name	Rules	Full path
english_words.ini	30055	D:\Windows\System32\hybrid_rules\english_w...

A hybrid attack is similar to a dictionary one, except that you can set your own word mutation rules. The program comes with a huge set of rule-files. Just use one that is best for your task. The good thing in a Hybrid attack is that you can additionally create, edit and modify password mutation rules according to your needs.

Mask attack



Plaintext password recovery

Searching passwords (step 4 of 5) - Mask attack

If you know that the password begins with 'loveme' and followed by a name, you can set the mask 'loveme%c%c%c%c%c%c' to check all possible variants starting with 'lovemeaaaaaa' and up to 'lovemezzzzzz'.

Mask syntax tip

```
%c       - lower-case Latin characters  (a..z)
%C       - upper-case Latin characters (A..Z)
%#       - full set of special characters (!..~ space)
%@       - small set of special characters (!@#$%^&*()-_+= space)
%?       - all printable characters with ASCII codes of 32..127
%*       - all ASCII characters (codes 1..255)
%d       - one digit (0..9)
%d(x-y)  - numbers between x and y inclusive
```

Password mask: %w(English.pcd)%d(0-99)

Custom character sets

A Mask attack is an irreplaceable tool when you know a part of the password or have any specific details about it. For example, if you know that the password consists of 12 characters and starts with 'loveme', obviously it's just enough to guess the last 6 characters of the password. That is what the mask attack is for. In our example, you can set the following mask: loveme%c%c%c%c%c%c

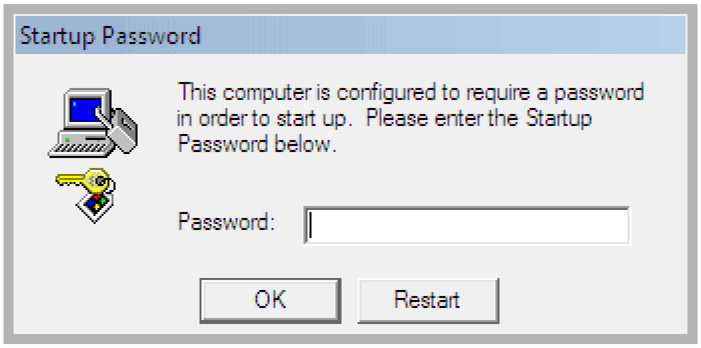
To get more information about how the mask works, please refer to our online documentation.

3.5.5 Search for SYSKEY startup password

Syskey is the additional layer of security, was introduced first in Windows 2000. It is used by default and offers 3 types of protection:

1. **Default** - when the syskey encryption key is stored in Windows registry.
2. **Startup disk** - syskey encryption key is stored on a diskette.
3. **Startup password** - syskey encryption key is generated from a user pass-phrase.

Scammers take advantage of the SYSKEY power and often set a syskey startup password on a victim's PC. Usually they contact you with a thick Indian accent identifying themselves as a member of Microsoft support and tells that your PC need to be fixed immediately because it has a critical problem. They will try convincing you to allow them to connect your system remotely and fix the issues. If you do make the mistake, they will set a SYSKEY startup password. Since you do not know the password, after reloading the system you will get the screen like that (see below) and will not be able to logon unless you pay for fix.



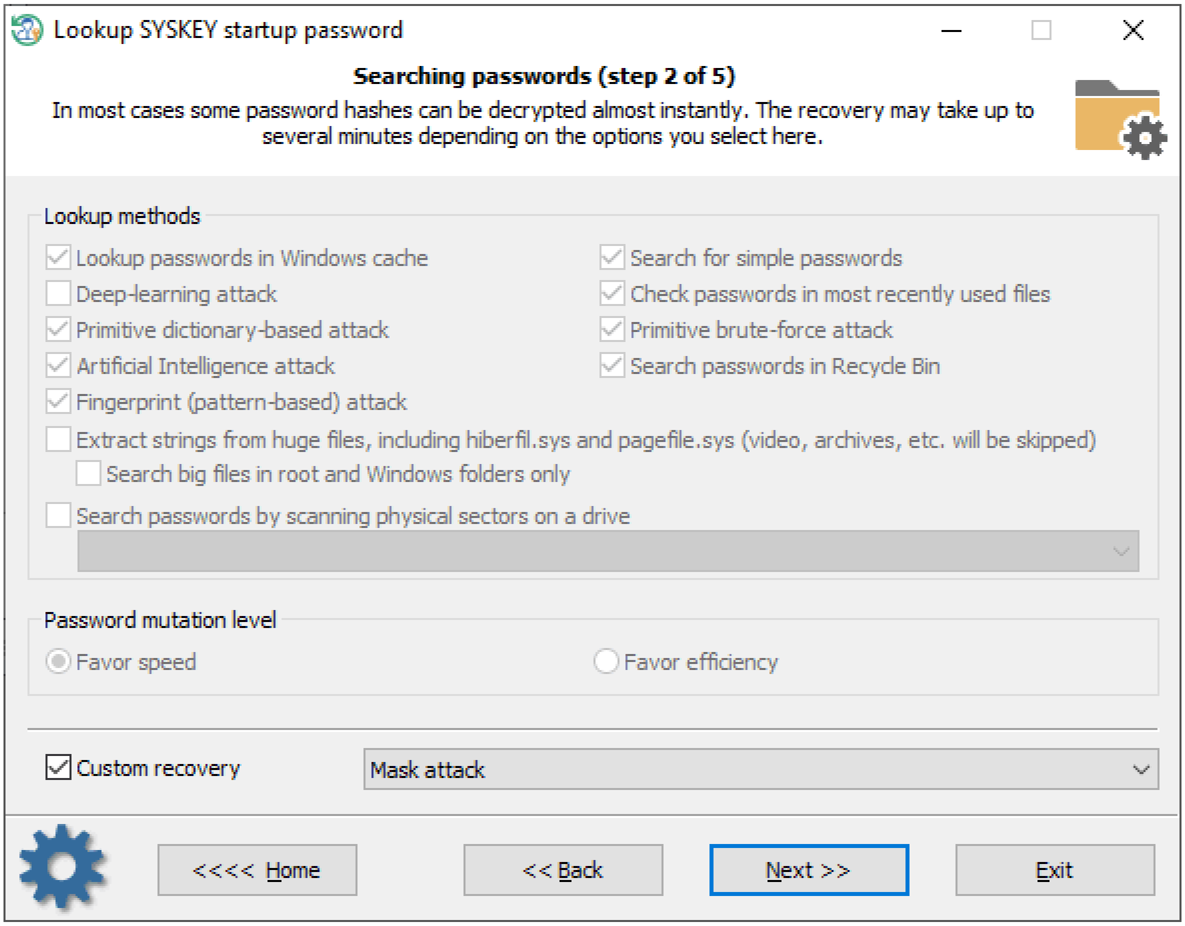
Startup Password

This computer is configured to require a password in order to start up. Please enter the Startup Password below.

Password:

Fortunately, in most cases the passwords they use are pretty trivial and can be decrypted using our SYSKEY password lookup feature. You will have to go through the 3 simple steps to start searching the password.

Setting SYSKEY recovery methods



Lookup SYSKEY startup password

Searching passwords (step 2 of 5)

In most cases some password hashes can be decrypted almost instantly. The recovery may take up to several minutes depending on the options you select here.

Lookup methods

- ☑ Lookup passwords in Windows cache
- □ Deep-learning attack
- ☑ Primitive dictionary-based attack
- ☑ Artificial Intelligence attack
- ☑ Fingerprint (pattern-based) attack
- ☑ Search for simple passwords
- ☑ Check passwords in most recently used files
- ☑ Primitive brute-force attack
- ☑ Search passwords in Recycle Bin
- □ Extract strings from huge files, including hiberfil.sys and pagefile.sys (video, archives, etc. will be skipped)
  - □ Search big files in root and Windows folders only
- □ Search passwords by scanning physical sectors on a drive

Password mutation level

● Favor speed ○ Favor efficiency

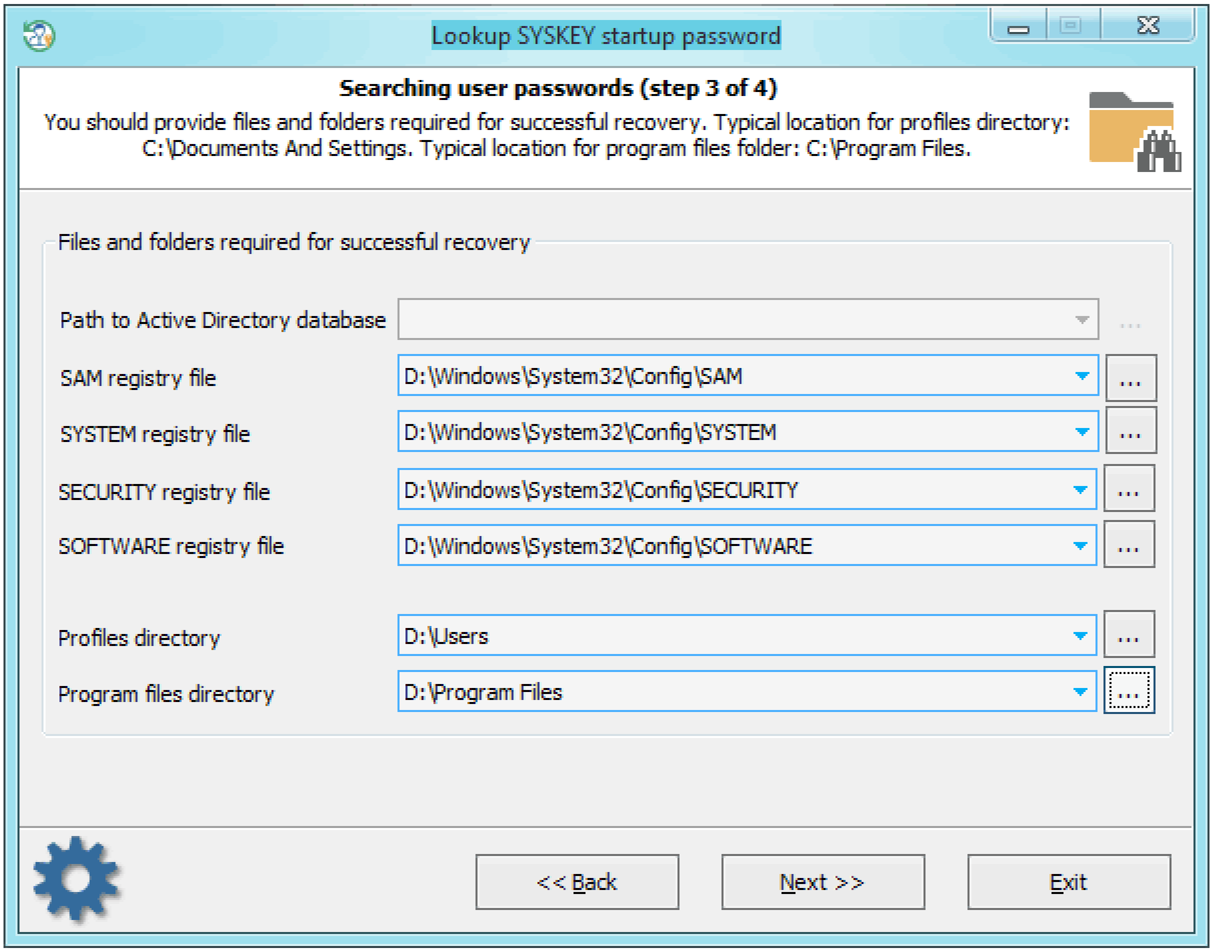
☑ Custom recovery: Mask attack

SYSKEY password lookup may take quite some time and consists of the following steps:

1. Searching information in Windows system cache. This method consists of over a dozen of mini sub-attacks, during which the program analyzes all kinds of user passwords: LSA secrets, DSL, VPN, WiFI, FTP, IM, browser passwords, etc.
2. Analyzing simple, short passwords, keyboard combinations, etc.
3. Scan, parse and analyze most recently used files of the target system.
4. Primitive dictionary attack. The application checks all passwords from the built-in dictionary for the Light and Standard editions or from several dictionaries (Arabic, Chinese, English, French, German, Portuguese, Russian, Spanish) for the Advanced Edition. If the deep search option is on, simple word mutations will also be taken into account during the search.
5. Primitive brute-force recovery will try to reveal short passwords. The brute-force options are also depend on the mutation level.
6. Artificial Intelligence attack analyzes network activity of a user on the computer. Upon the results of the analysis, the application generates user preferences and generates a semantic dictionary for the attack, which it later uses it for finding and guessing the password.
7. Look for passwords in deleted files, temporary folders and so on.
8. Searching for complicated English passwords (Fingerprint attack).
9. Extract strings and words from huge files: RAM images, hiberfil.sys, pagefile.sys ans so on. When this option is set, the program will try to skip files useless in password analysis like video, archives, audio files, etc.
10. Search passwords by reading and analyzing raw sectors of the selected drive. If the '*Password mutation level*' is set to '*Deep search*', the program additionally tries to generate different combinations and 'mutate' found passwords, thus walking through all sectors of the target drive may take quite a time. Note that the sector-based scanning algorithm is not effective against drives which have a full-disk encryption set on.

To apply a custom recovery method, turn on the 'Custom recovery' option and select one of the available attacks. On the next step you will be prompted to set up various options related to the selected attack.

Selecting data source



Lookup SYSKEY startup password

Searching user passwords (step 3 of 4)

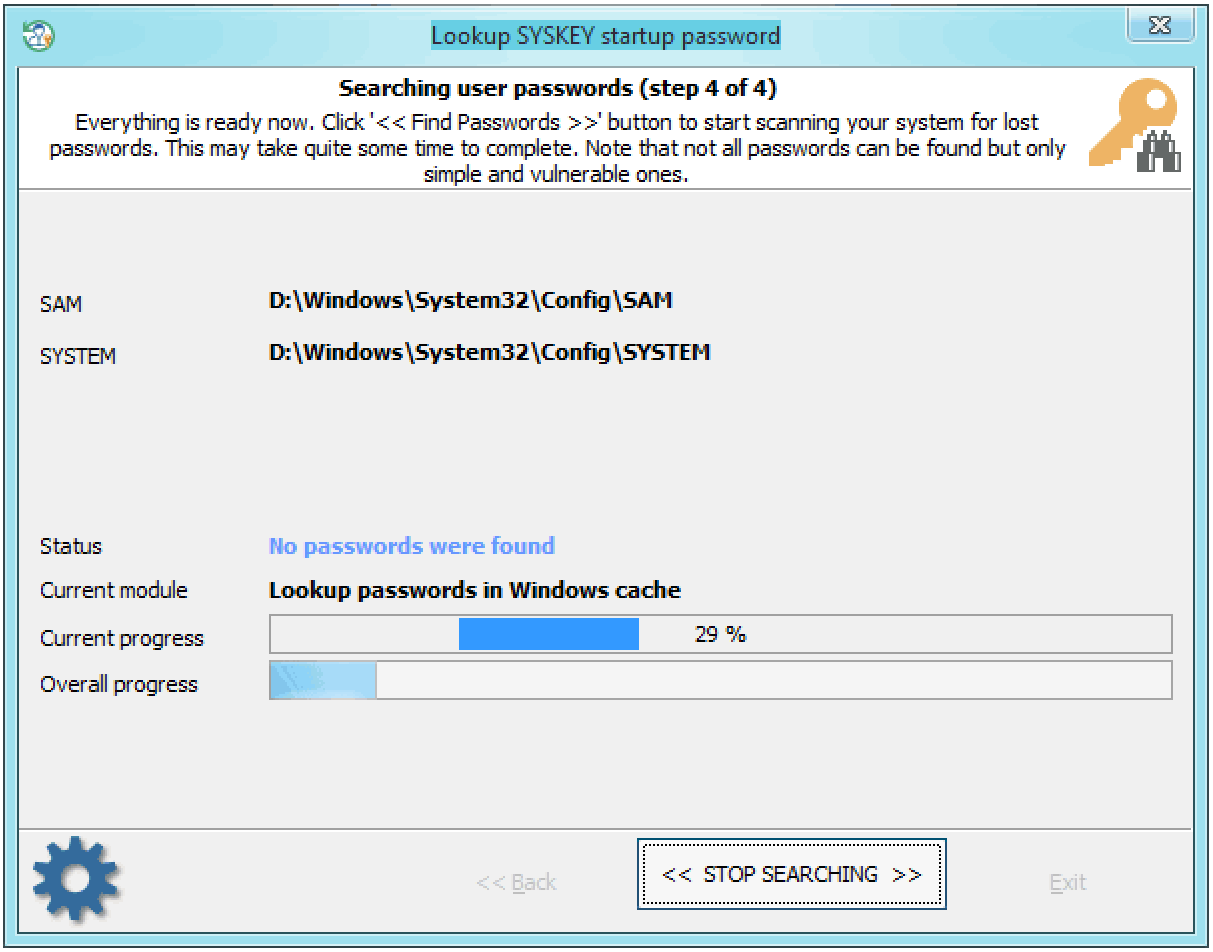
You should provide files and folders required for successful recovery. Typical location for profiles directory: C:\Documents And Settings. Typical location for program files folder: C:\Program Files.

Files and folders required for successful recovery

Path to Active Directory database	
SAM registry file	D:\Windows\System32\Config\SAM
SYSTEM registry file	D:\Windows\System32\Config\SYSTEM
SECURITY registry file	D:\Windows\System32\Config\SECURITY
SOFTWARE registry file	D:\Windows\System32\Config\SOFTWARE
Profiles directory	D:\Users
Program files directory	D:\Program Files

When searching for the SYSKEY startup password, special attention is to be paid to supplying correct files and folders required for the analysis process.Otherwise, password search will be inefficient or even not available. The application tries to locate the files automatically, but sometimes, e.g., when the computer has several operating systems installed, you may need to use the 'manual control' over it. Please also keep in mind that if the problem PC has 2 or more logical drives, the sequence of the letters for these disks may be set totally different than in the original system.

Searching for SYSKEY password



Searching user passwords (step 4 of 4)

Everything is ready now. Click '<< Find Passwords >>' button to start scanning your system for lost passwords. This may take quite some time to complete. Note that not all passwords can be found but only simple and vulnerable ones.

SAM **D:\Windows\System32\Config\SAM**

SYSTEM **D:\Windows\System32\Config\SYSTEM**

Status **No passwords were found**

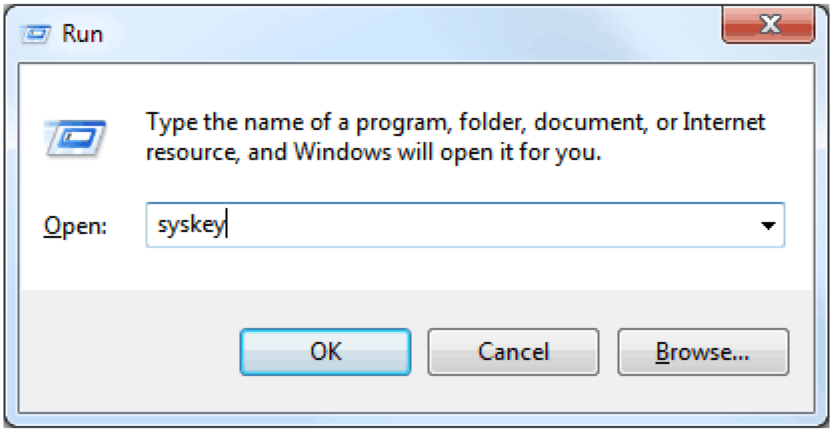
Current module **Lookup passwords in Windows cache**

Current progress 29 %

Overall progress

Finding/guessing the password may take some time, which depends on attack settings and peculiarities of your system. Note that only simple and vulnerable passwords can be recovered!

Once you retrieve the SYSKEY plaintext password, all you need is to turn off the SYSKEY startup prompt and set your system back to its original state. Turn on your problem PC and use the found password to bypass the SYSKEY startup dialog. Then logon into your Windows account, hit '**Win+R**' keys, type in '**SYSKEY**' and click '**OK**' button.

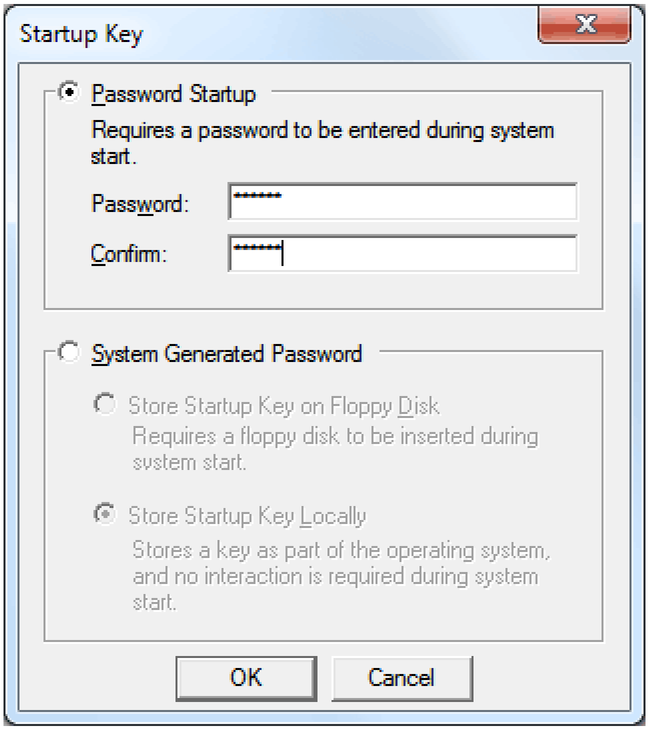


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: syskey

This should bring up the SYSKEY options dialog. All you need here is to click the '**Update**' button and switch the '**Password Startup**' option back to '**System Generated Password**' by supplying the found plaintext.



Startup Key

● Password Startup

Requires a password to be entered during system start.

Password: *******

Confirm: *******

○ System Generated Password

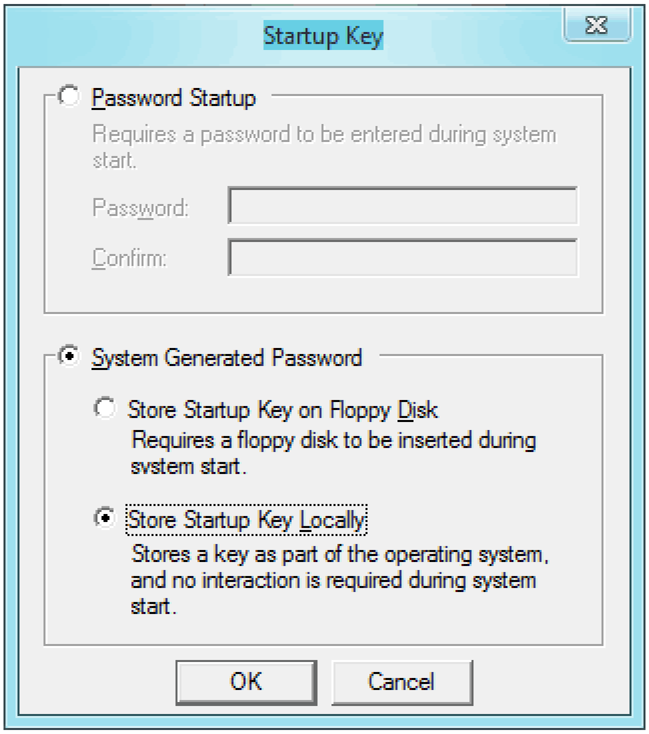
○ Store Startup Key on Floppy Disk

Requires a floppy disk to be inserted during system start.

● Store Startup Key Locally

Stores a key as part of the operating system, and no interaction is required during system start.

So, after all changes, you should have it look like this:



Startup Key

○ Password Startup

Requires a password to be entered during system start.

Password:

Confirm:

● System Generated Password

○ Store Startup Key on Floppy Disk

Requires a floppy disk to be inserted during svstem start.

● Store Startup Key Locally

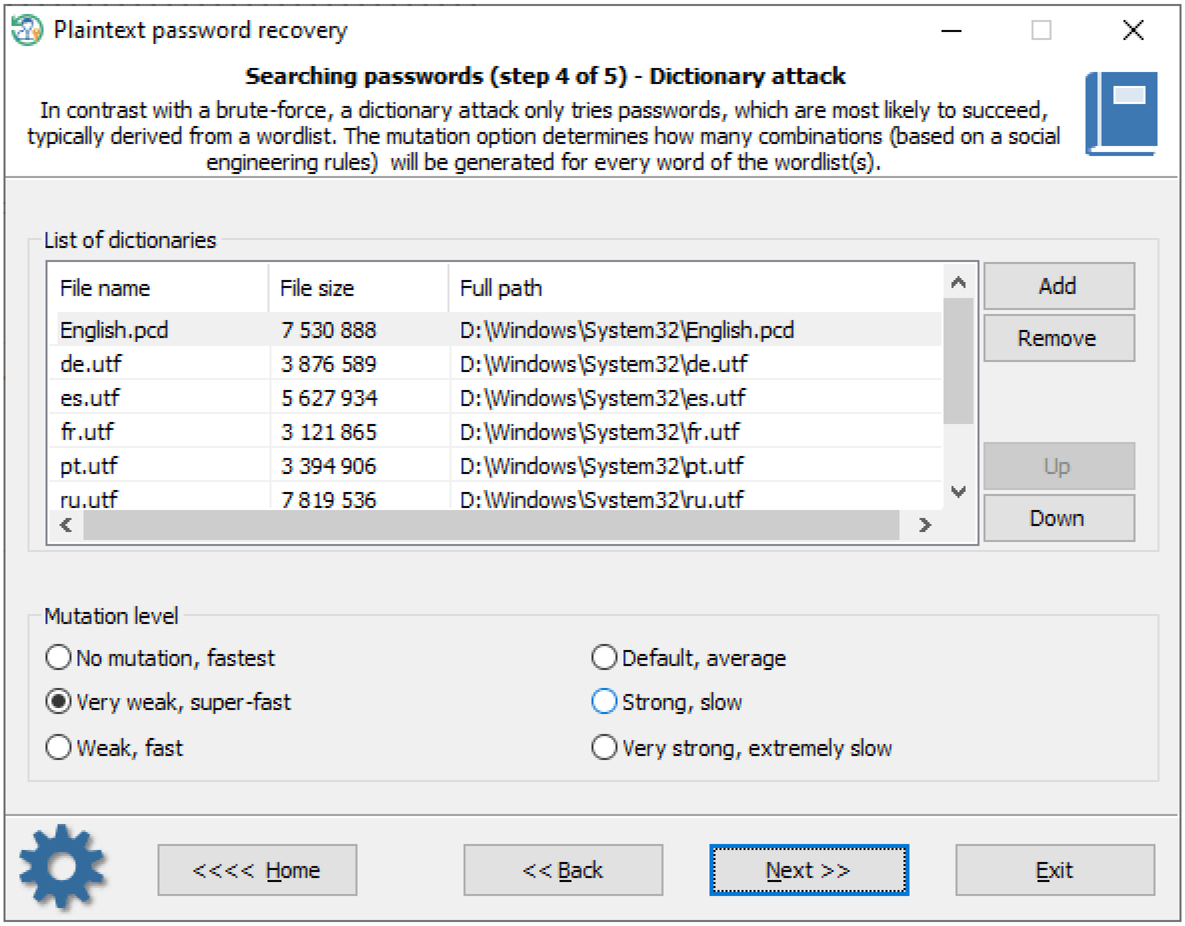
Stores a key as part of the operating system, and no interaction is required during system start.

3.5.5.1 Custom recovery

Once the custom recovery option is set, the program can additionally run 3 different attacks to guess the passwords:

- Dictionary attack
- Hybrid attack
- Mask attack

Dictionary attack



Plaintext password recovery

Searching passwords (step 4 of 5) - Dictionary attack

In contrast with a brute-force, a dictionary attack only tries passwords, which are most likely to succeed, typically derived from a wordlist. The mutation option determines how many combinations (based on a social engineering rules) will be generated for every word of the wordlist(s).

List of dictionaries

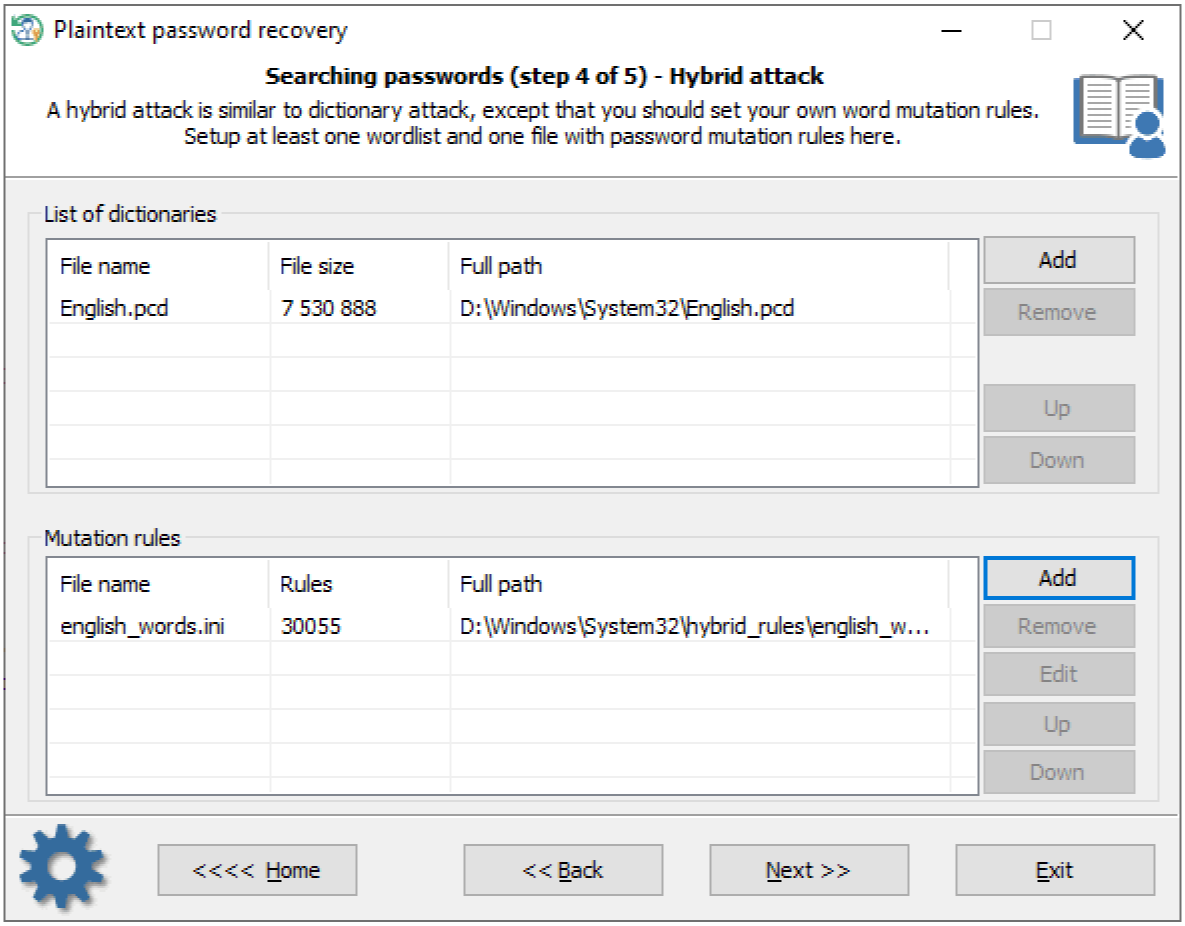
File name	File size	Full path
English.pcd	7 530 888	D:\Windows\System32\English.pcd
de.utf	3 876 589	D:\Windows\System32\de.utf
es.utf	5 627 934	D:\Windows\System32\es.utf
fr.utf	3 121 865	D:\Windows\System32\fr.utf
pt.utf	3 394 906	D:\Windows\System32\pt.utf
ru.utf	7 819 536	D:\Windows\System32\ru.utf

Mutation level

○ No mutation, fastest
● Very weak, super-fast
○ Weak, fast
○ Default, average
○ Strong, slow
○ Very strong, extremely slow

A dictionary attack tries passwords, which are most likely to succeed, typically derived from a wordlist. RWP supports for different types of dictionaries: ASCII, UNICODE, UTF8, as well as encrypted/compressed dictionaries in the native PCD format. You can use both predefined and custom dictionaries. To add your own wordlist, copy one to a USB drive and attach the drive to the target PC. The mutation level determines how many combinations (based on a social engineering rules) will be generated for every word of the wordlist(s).

Hybrid attack



Plaintext password recovery

Searching passwords (step 4 of 5) - Hybrid attack

A hybrid attack is similar to dictionary attack, except that you should set your own word mutation rules. Setup at least one wordlist and one file with password mutation rules here.

List of dictionaries

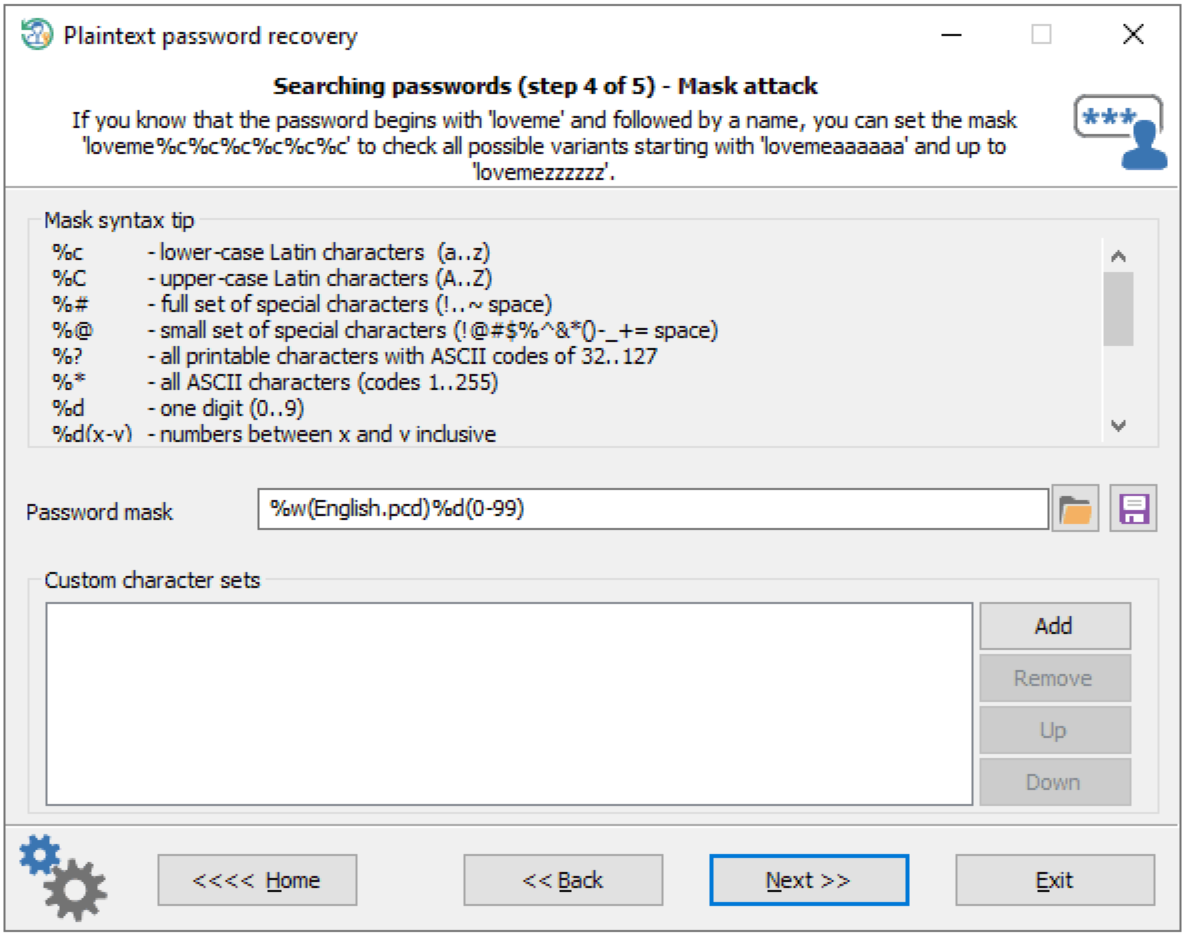
File name	File size	Full path
English.pcd	7 530 888	D:\Windows\System32\English.pcd

Mutation rules

File name	Rules	Full path
english_words.ini	30055	D:\Windows\System32\hybrid_rules\english_w...

A hybrid attack is similar to a dictionary one, except that you can set your own word mutation rules. The program comes with a huge set of rule-files. Just use one that is best for your task. The good thing in a Hybrid attack is that you can additionally create, edit and modify password mutation rules according to your needs.

Mask attack



Plaintext password recovery

Searching passwords (step 4 of 5) - Mask attack

If you know that the password begins with 'loveme' and followed by a name, you can set the mask 'loveme%c%c%c%c%c%c' to check all possible variants starting with 'lovemeaaaaaa' and up to 'lovemezzzzzz'.

Mask syntax tip

%c	- lower-case Latin characters (a..z)
%C	- upper-case Latin characters (A..Z)
%#	- full set of special characters (!..~ space)
%@	- small set of special characters (!@#$%^&*()-_+= space)
%?	- all printable characters with ASCII codes of 32..127
%*	- all ASCII characters (codes 1..255)
%d	- one digit (0..9)
%d(x-y)	- numbers between x and y inclusive

Password mask: %w(English.pcd)%d(0-99)

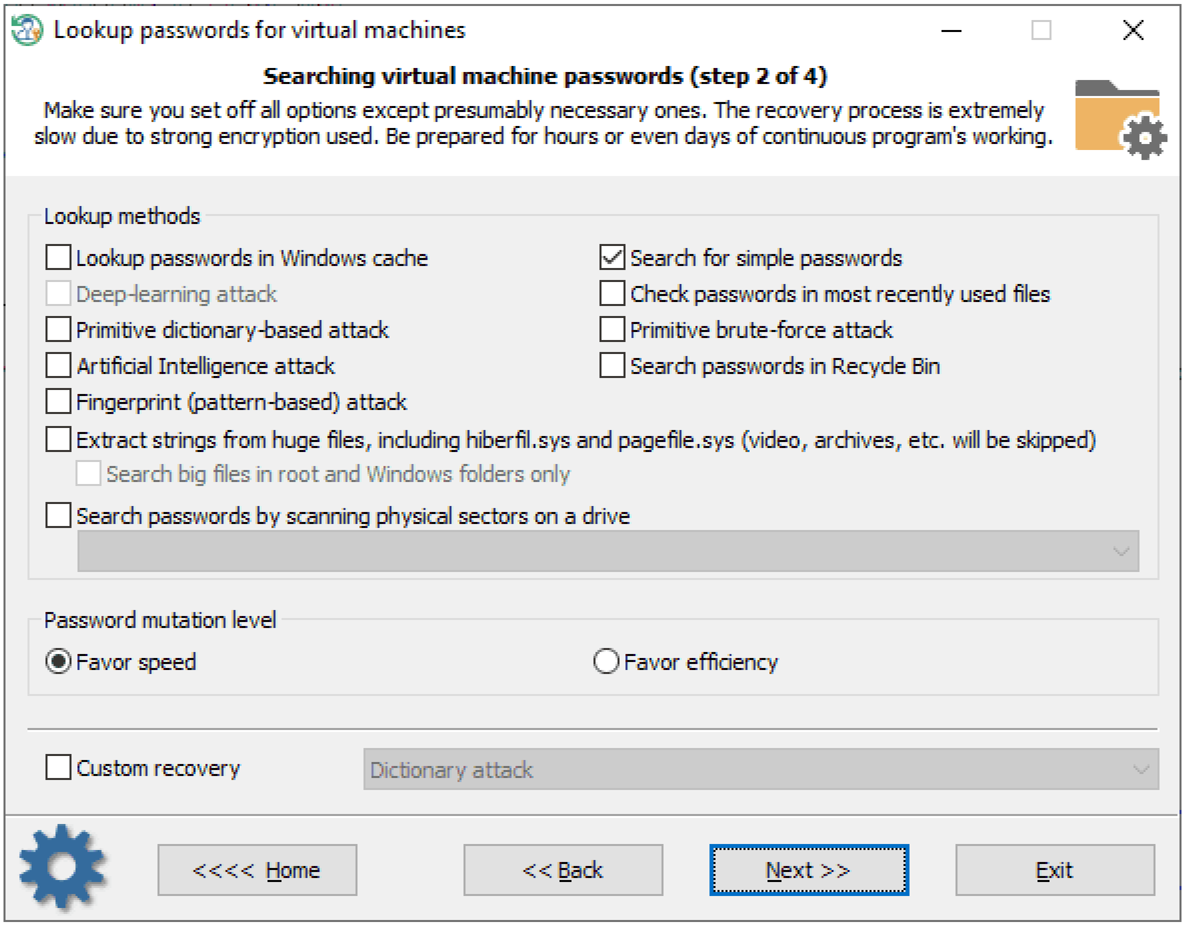
Custom character sets

A Mask attack is an irreplaceable tool when you know a part of the password or have any specific details about it. For example, if you know that the password consists of 12 characters and starts with 'loveme', obviously it's just enough to guess the last 6 characters of the password. That is what the mask attack is for. In our example, you can set the following mask: loveme%c%c%c%c%c%c
To get more information about how the mask works, please refer to our online documentation.

3.5.6 Search for virtual machine passwords

Once a password for Virtual Machine is forgotten, you can use this RWP feature to get back access to your locked VM. The current version of the program supports VmWare and Oracle VirtualBox virtual machines. Both virtualization programs have very strong protection, thus password recovery for these VMs has some peculiarities described below.

Setting up password recovery methods



Lookup passwords for virtual machines

Searching virtual machine passwords (step 2 of 4)

Make sure you set off all options except presumably necessary ones. The recovery process is extremely slow due to strong encryption used. Be prepared for hours or even days of continuous program's working.

Lookup methods

- □ Lookup passwords in Windows cache
- □ Deep-learning attack
- □ Primitive dictionary-based attack
- □ Artificial Intelligence attack
- □ Fingerprint (pattern-based) attack
- ☑ Search for simple passwords
- □ Check passwords in most recently used files
- □ Primitive brute-force attack
- □ Search passwords in Recycle Bin
- □ Extract strings from huge files, including hiberfil.sys and pagefile.sys (video, archives, etc. will be skipped)
  - □ Search big files in root and Windows folders only
- □ Search passwords by scanning physical sectors on a drive

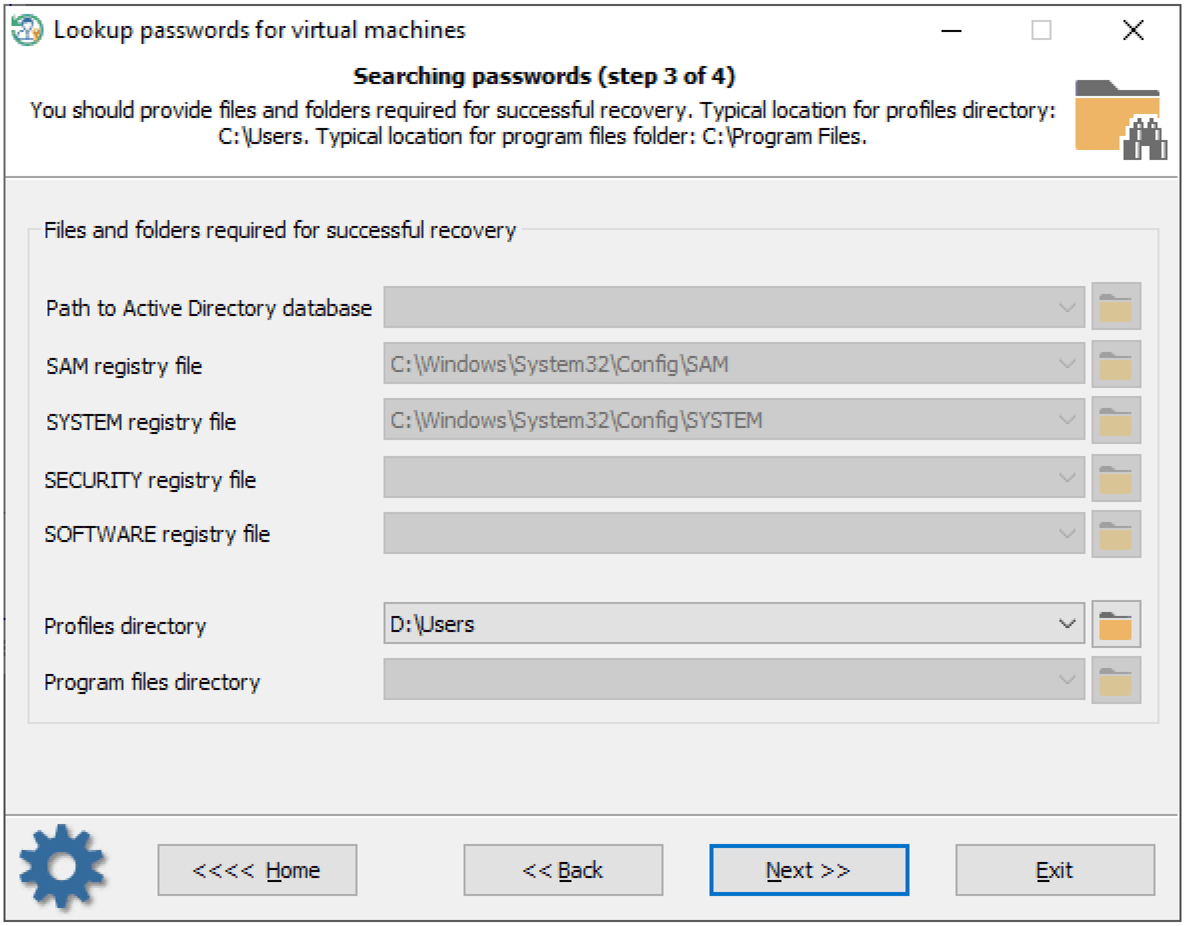
Password mutation level

● Favor speed ○ Favor efficiency

□ Custom recovery Dictionary attack

At the very beginning, determine what search methods fit best for your task. Password recovery for Virtual Machines is an extremely slow process, so it is highly recommended to disable the most time-expensive items. The 'Custom recovery' checkbox switches between custom and predefined attack templates. If the first is selected, you will be asked to configure some options for the selected attack during the next Wizard steps. If certain information about the password is known, a custom attack would be your choice.

Selecting data source



Searching passwords (step 3 of 4)

You should provide files and folders required for successful recovery. Typical location for profiles directory: C:\Users. Typical location for program files folder: C:\Program Files.

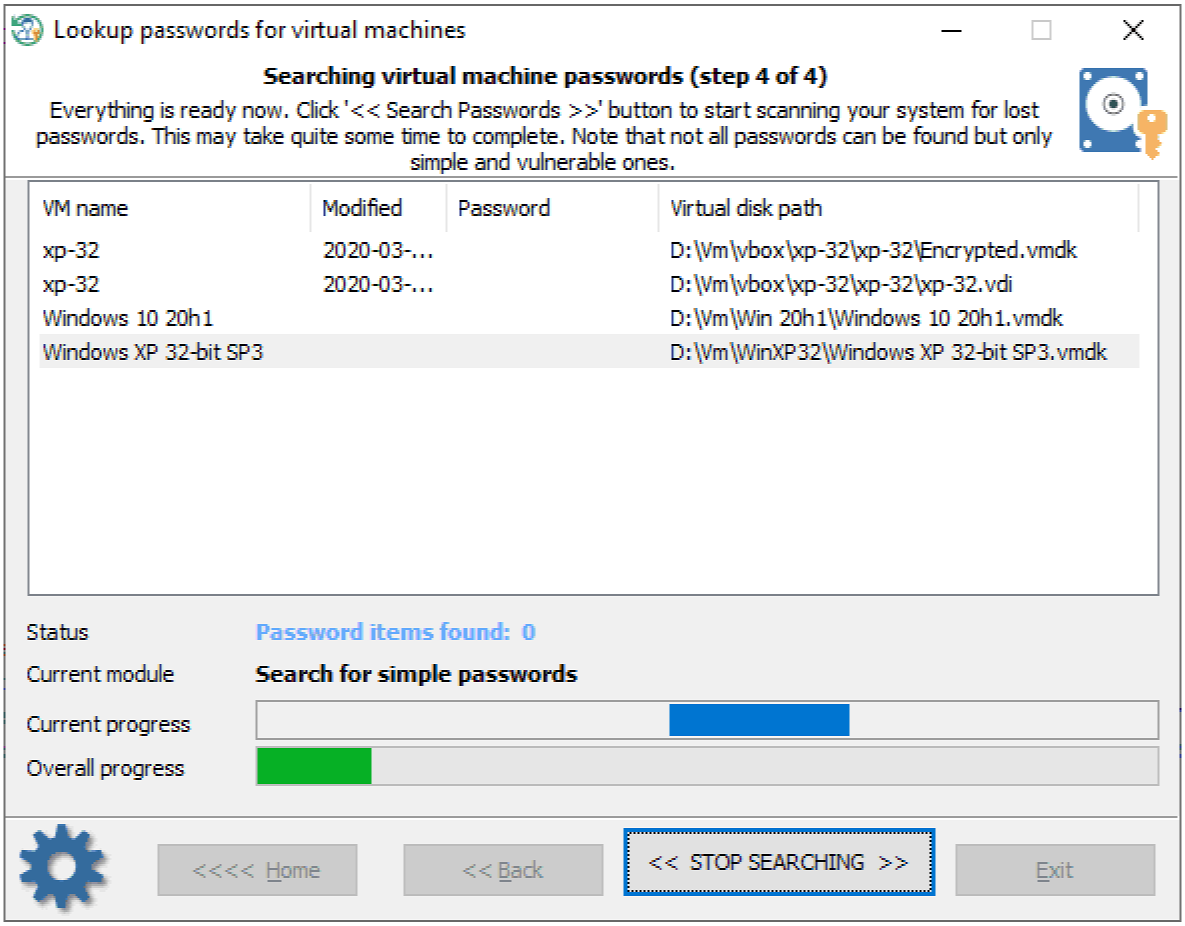
Files and folders required for successful recovery

Path to Active Directory database	
SAM registry file	C:\Windows\System32\Config\SAM
SYSTEM registry file	C:\Windows\System32\Config\SYSTEM
SECURITY registry file	
SOFTWARE registry file	
Profiles directory	D:\Users
Program files directory	

Please, pay special attention to setting up all folders required for further system analysis. Otherwise, the program will be able neither to detect Virtual Machines not to search for passwords properly. In most cases, RWP automatically fills up all fields with required files and folders.

Keep in mind that the disk letters may differ from ones on the original system!

Searching for virtual machine passwords



Lookup passwords for virtual machines

Searching virtual machine passwords (step 4 of 4)

Everything is ready now. Click '<< Search Passwords >>' button to start scanning your system for lost passwords. This may take quite some time to complete. Note that not all passwords can be found but only simple and vulnerable ones.

VM name	Modified	Password	Virtual disk path
xp-32	2020-03-...		D:\Vm\vbox\xp-32\xp-32\Encrypted.vmdk
xp-32	2020-03-...		D:\Vm\vbox\xp-32\xp-32\xp-32.vdi
Windows 10 20h1			D:\Vm\Win 20h1\Windows 10 20h1.vmdk
Windows XP 32-bit SP3			D:\Vm\WinXP32\Windows XP 32-bit SP3.vmdk

Status: Password items found: 0

Current module: **Search for simple passwords**

Current progress

Overall progress

Searching for VM passwords usually takes a really long time. All virtual machines have very strong protection and in some cases, the password search speed is as low as only a few passwords per second. Therefore, to optimize and increase the process, just exclude unnecessary virtual machines from the search list and leave active the only one you need. Use the context menu for that.

3.5.7 Search passwords for encrypted documents

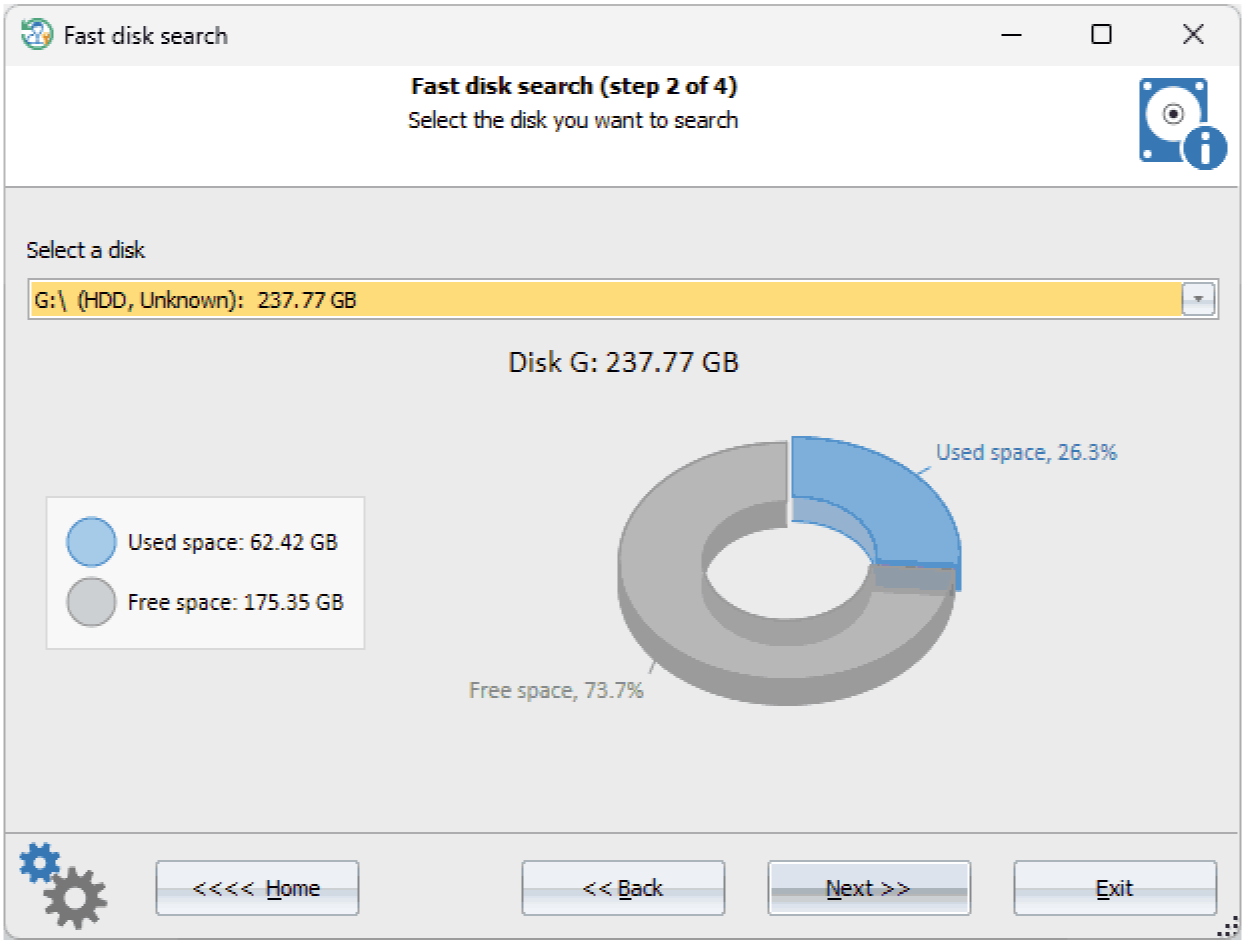
Modern documents have extremely strong password protection that makes common recovery methods like a brute-force or a dictionary attack useless in most cases. Therefore, once the encryption password for such a document was not recovered using any other program applying the common recovery methods, then the Reset Windows Password is your last chance to find the password.

A well-known secret that uncovers password weakness is that many users often reuse their passwords or use slightly modified variations when creating Internet accounts, encrypting documents, creating wireless networks, etc. RWP utilizes the weakness in its powerful built-in engine to increase the recovery percentage for algorithms that cannot be broken using common methods. If you do not go into details, then everything is quite trivial at first glance: the program scans the system, enumerates every found password, as well as some password candidates, for every found item it makes all possible mutations and modifications, and at the final stage, tries to guess the original password using the huge variety of the generated items. Despite its apparent simplicity, the internal algorithms are quite complex. For example, the general password lookup module consists of several dozen sub-modules. This also applies to other modules and groups of modules such as mutation, artificial intelligence, etc.

The current version of the program supports the following file formats:

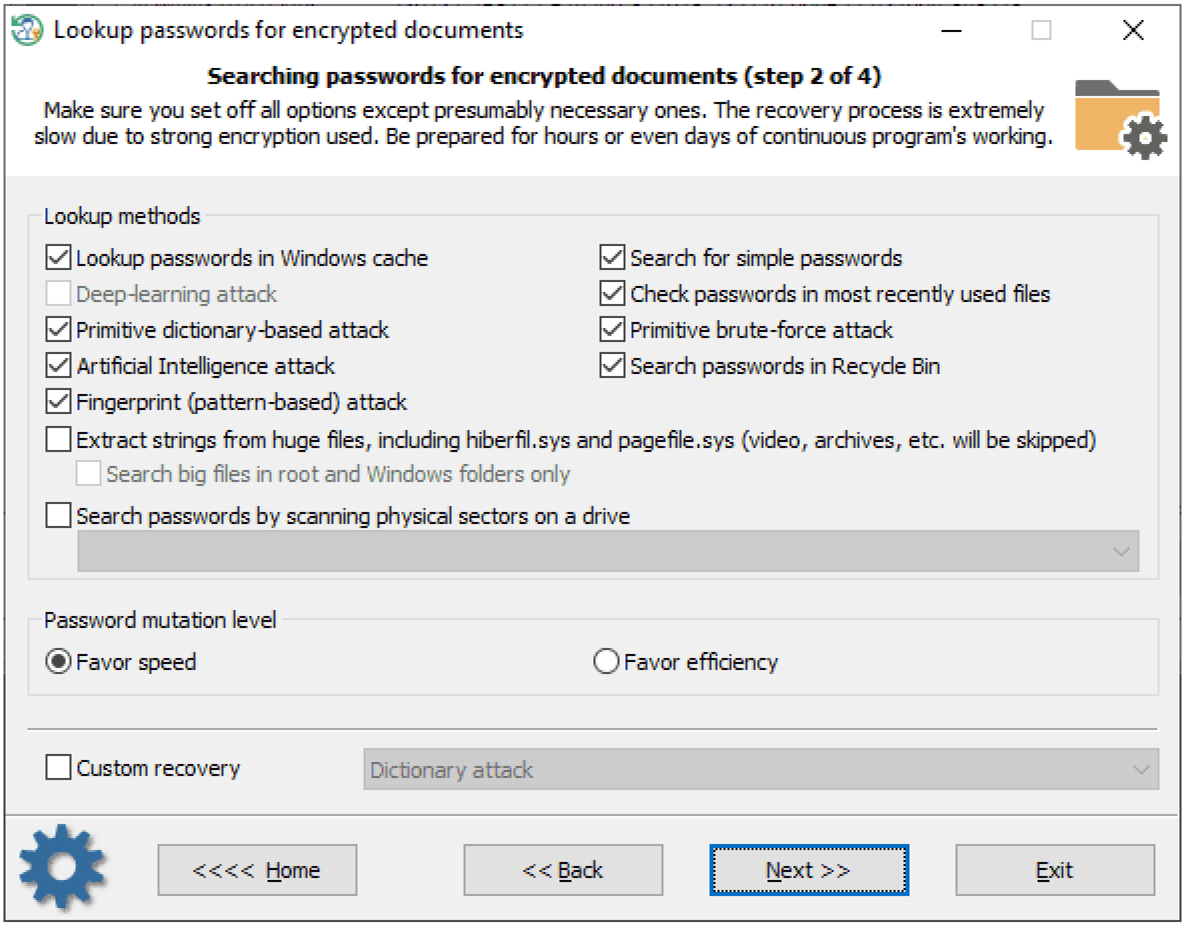
- Microsoft Office 97 and newer documents
- Files in OpenDocument format: OpenOffice, LibreOffice, MyOffice.
- PDF documents (both user and owner passwords).

Selecting source disk



Select the disk on which you want to search for documents.
Keep in mind that as soon as you select the disk and click the *Next* button, the program will immediately start the background scanning of the disk. Thus, by the final dialogue, you should typically get a list of all the encrypted documents found on the selected disk.

Setting up password recovery methods



Lookup passwords for encrypted documents

Searching passwords for encrypted documents (step 2 of 4)

Make sure you set off all options except presumably necessary ones. The recovery process is extremely slow due to strong encryption used. Be prepared for hours or even days of continuous program's working.

Lookup methods

☑ Lookup passwords in Windows cache

□ Deep-learning attack

☑ Primitive dictionary-based attack

☑ Artificial Intelligence attack

☑ Fingerprint (pattern-based) attack

☑ Search for simple passwords

☑ Check passwords in most recently used files

☑ Primitive brute-force attack

☑ Search passwords in Recycle Bin

□ Extract strings from huge files, including hiberfil.sys and pagefile.sys (video, archives, etc. will be skipped)

□ Search big files in root and Windows folders only

□ Search passwords by scanning physical sectors on a drive

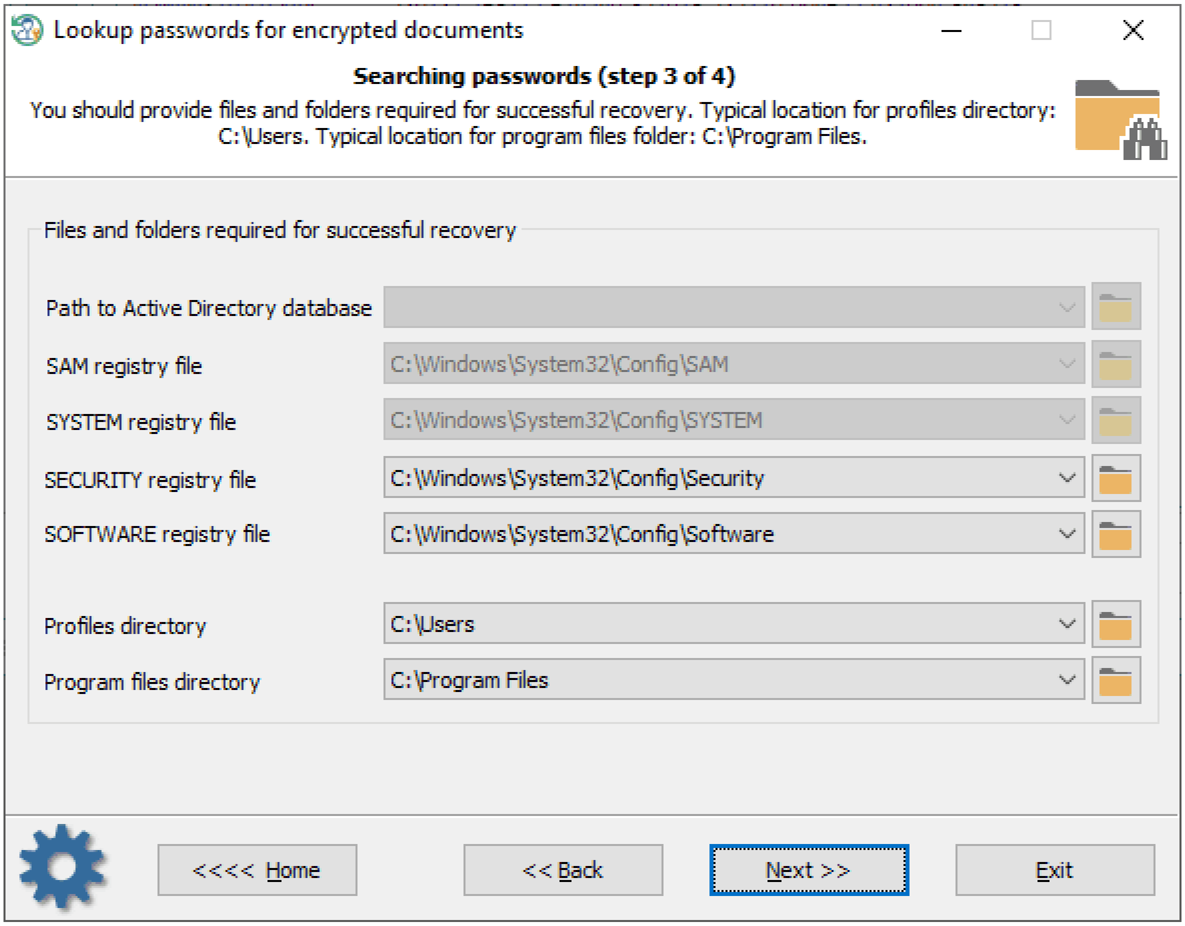
Password mutation level

● Favor speed ○ Favor efficiency

□ Custom recovery Dictionary attack

At the very beginning, determine what search methods would fit best for your task. Password recovery for encrypted documents is an extremely slow process, especially if you have more than one file to decrypt. Thus it is highly recommended to turn off the most time-consumptive methods. If certain information about the password is known then it would not be unreasonable to switch to a custom attack. Just click the 'Custom recovery' checkbox and choose one of the available methods. For example, a Mask attack. Otherwise, the default parameters is your best choice.

Setting up folders



Searching passwords (step 3 of 4)

You should provide files and folders required for successful recovery. Typical location for profiles directory: C:\Users. Typical location for program files folder: C:\Program Files.

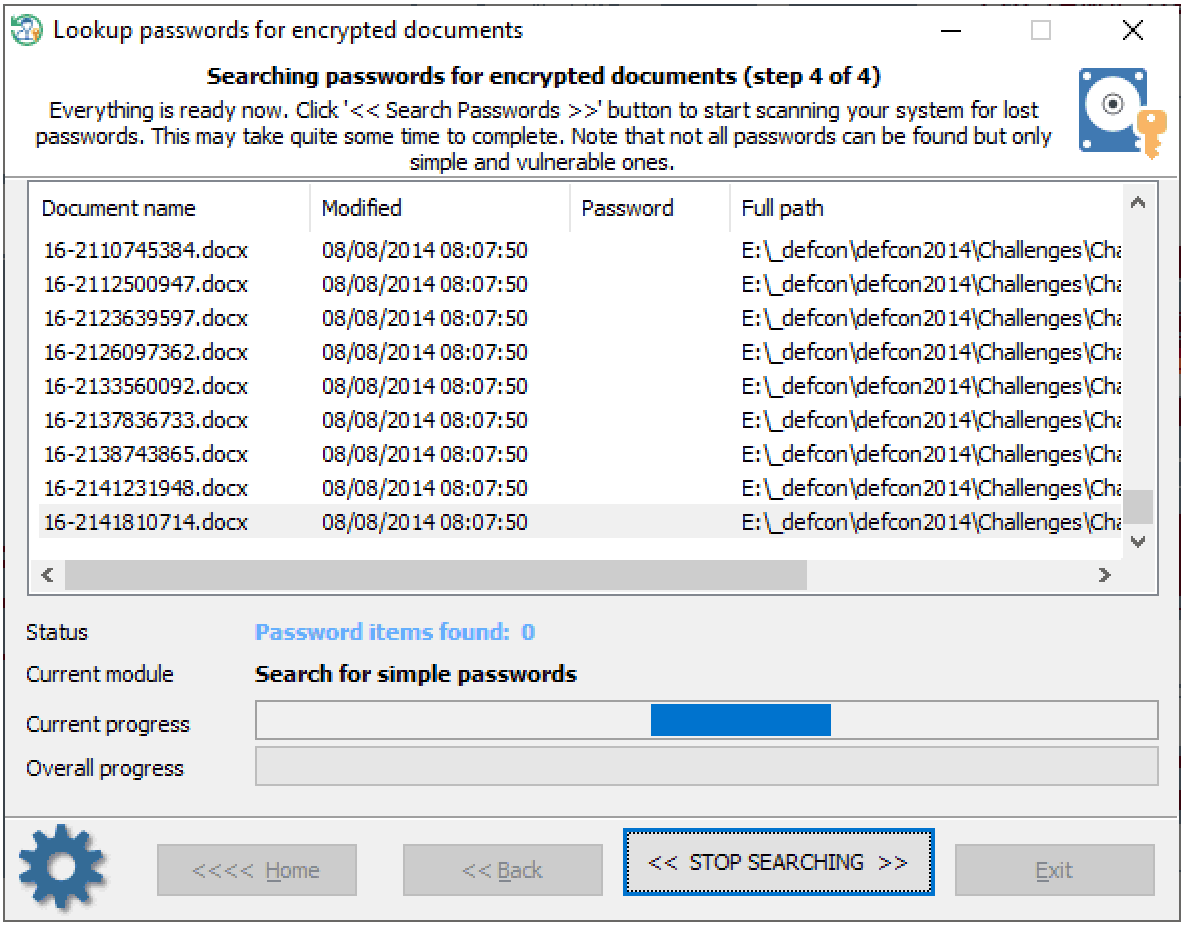
Files and folders required for successful recovery

Path to Active Directory database	
SAM registry file	C:\Windows\System32\Config\SAM
SYSTEM registry file	C:\Windows\System32\Config\SYSTEM
SECURITY registry file	C:\Windows\System32\Config\Security
SOFTWARE registry file	C:\Windows\System32\Config\Software
Profiles directory	C:\Users
Program files directory	C:\Program Files

All you need here is to set up all the required folders properly. Some of them are vital when analyzing files and password candidates. In most cases, the program sets them up automatically.

Keep in mind, the the drive letters may differ from the original system!

[Searching password for encrypted documents]



Lookup passwords for encrypted documents

Searching passwords for encrypted documents (step 4 of 4)

Everything is ready now. Click '<< Search Passwords >>' button to start scanning your system for lost passwords. This may take quite some time to complete. Note that not all passwords can be found but only simple and vulnerable ones.

Document name	Modified	Password	Full path
16-2110745384.docx	08/08/2014 08:07:50		E:_defcon\defcon2014\Challenges\Cha
16-2112500947.docx	08/08/2014 08:07:50		E:_defcon\defcon2014\Challenges\Cha
16-2123639597.docx	08/08/2014 08:07:50		E:_defcon\defcon2014\Challenges\Cha
16-2126097362.docx	08/08/2014 08:07:50		E:_defcon\defcon2014\Challenges\Cha
16-2133560092.docx	08/08/2014 08:07:50		E:_defcon\defcon2014\Challenges\Cha
16-2137836733.docx	08/08/2014 08:07:50		E:_defcon\defcon2014\Challenges\Cha
16-2138743865.docx	08/08/2014 08:07:50		E:_defcon\defcon2014\Challenges\Cha
16-2141231948.docx	08/08/2014 08:07:50		E:_defcon\defcon2014\Challenges\Cha
16-2141810714.docx	08/08/2014 08:07:50		E:_defcon\defcon2014\Challenges\Cha

Status: Password items found: 0

Current module: Search for simple passwords

Current progress

Overall progress

The program guesses passwords for all found documents simultaneously (unless you mark some of them to be skipped). The password lookup process usually takes quite some time. For example, guessing passwords for Microsoft Office 2013 and newer documents runs at less than 10 passwords per second for a single document! Therefore, to optimize and increase the search speed, do exclude unnecessary documents from the search list, ideally leaving only the necessary one. You can use the context menu for that.

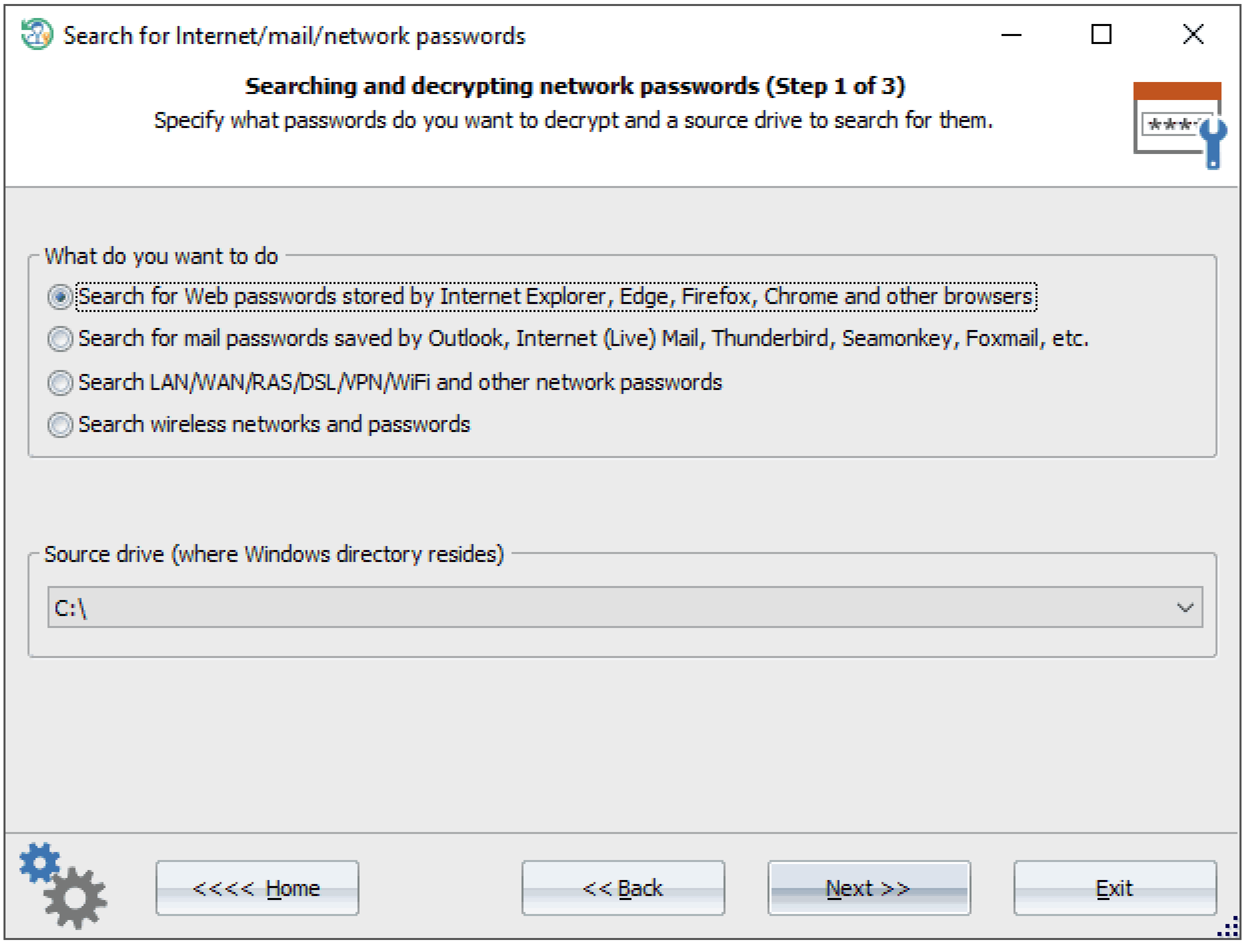
To add a new file, right-click them mouse button and select '*Add new document*'.

Starting with version 11 the program has a built-in technic to recover Indian Aadhaar and e-pan cards out-of-the-box. An Aadhaar card is a pdf file that contains a unique Identification Authority of Indian citizens. An e-pan card is a digital identifier issued by the Indian Income Tax Department..

To recover an Aadhaar/e-pan card, right-click the list of found items and deactivate any other documents except those you need to decrypt. Setting active Aadhaar/e-pan pdfs only should increase the recovery speed drastically. Then click the << Start searching >> button to launch the password lookup. The program automatically involves 7 built-in attacks. That allows keeping the success rate close to 100%.

3.5.8 Search for Internet/mail/network passwords

One of the application's most notable features is searching and decrypting PC users' network passwords. Reset Windows Password supports all major popular browsers and email clients. The interface is split into three steps to make the process as easy as possible, and the specific details are left to the program.



Search for Internet/mail/network passwords

Searching and decrypting network passwords (Step 1 of 3)

Specify what passwords do you want to decrypt and a source drive to search for them.

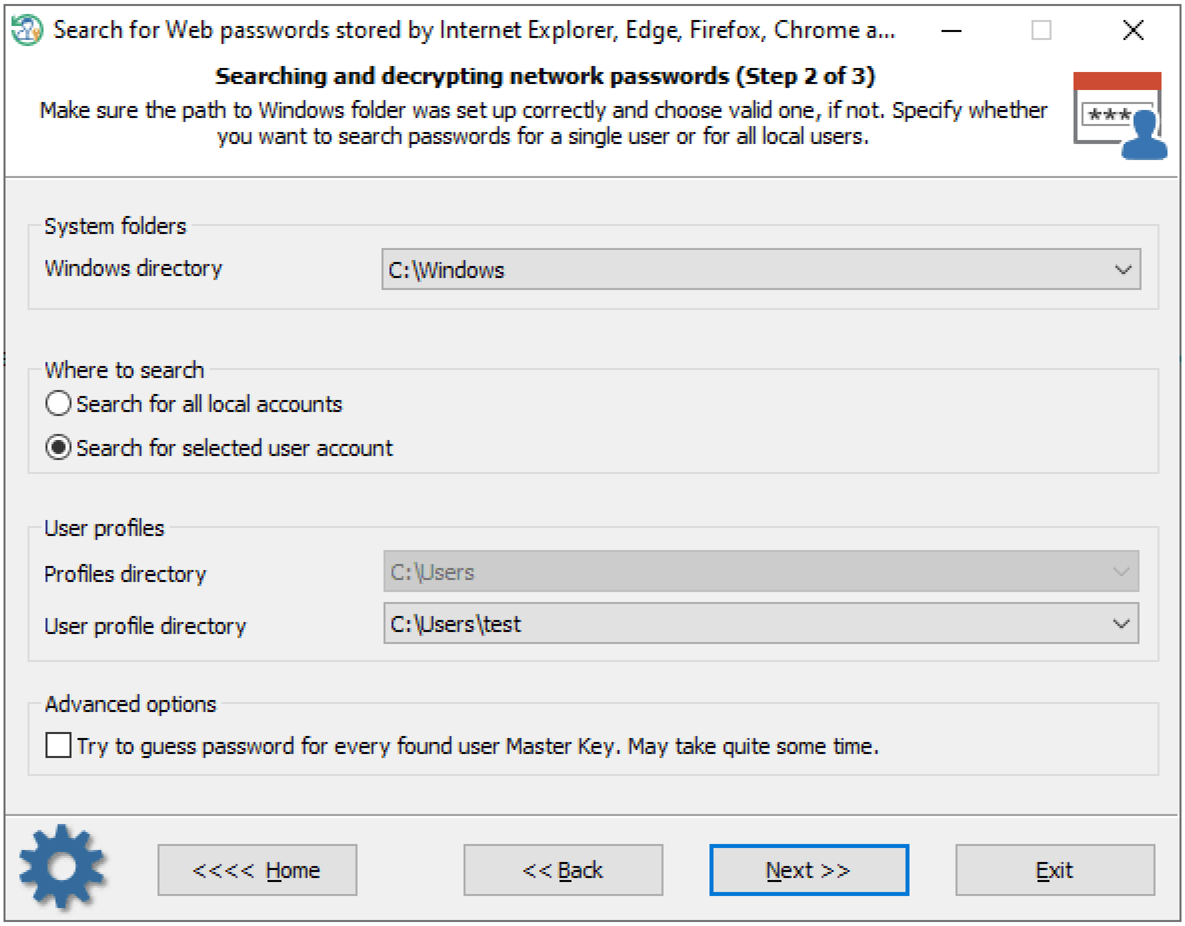
What do you want to do

- ● Search for Web passwords stored by Internet Explorer, Edge, Firefox, Chrome and other browsers
- ○ Search for mail passwords saved by Outlook, Internet (Live) Mail, Thunderbird, Seamonkey, Foxmail, etc.
- ○ Search LAN/WAN/RAS/DSL/VPN/WiFi and other network passwords
- ○ Search wireless networks and passwords

Source drive (where Windows directory resides)

C:\

On the first step of the Wizard, the program prompts you to select the type of passwords to be searched for and the source drive with the Windows folder. By default, the program selects the first hard drive, where the operating system is installed.



Search for Web passwords stored by Internet Explorer, Edge, Firefox, Chrome a...

Searching and decrypting network passwords (Step 2 of 3)

Make sure the path to Windows folder was set up correctly and choose valid one, if not. Specify whether you want to search passwords for a single user or for all local users.

System folders

Windows directory: C:\Windows

Where to search

○ Search for all local accounts

● Search for selected user account

User profiles

Profiles directory: C:\Users

User profile directory: C:\Users\test

Advanced options

□ Try to guess password for every found user Master Key. May take quite some time.

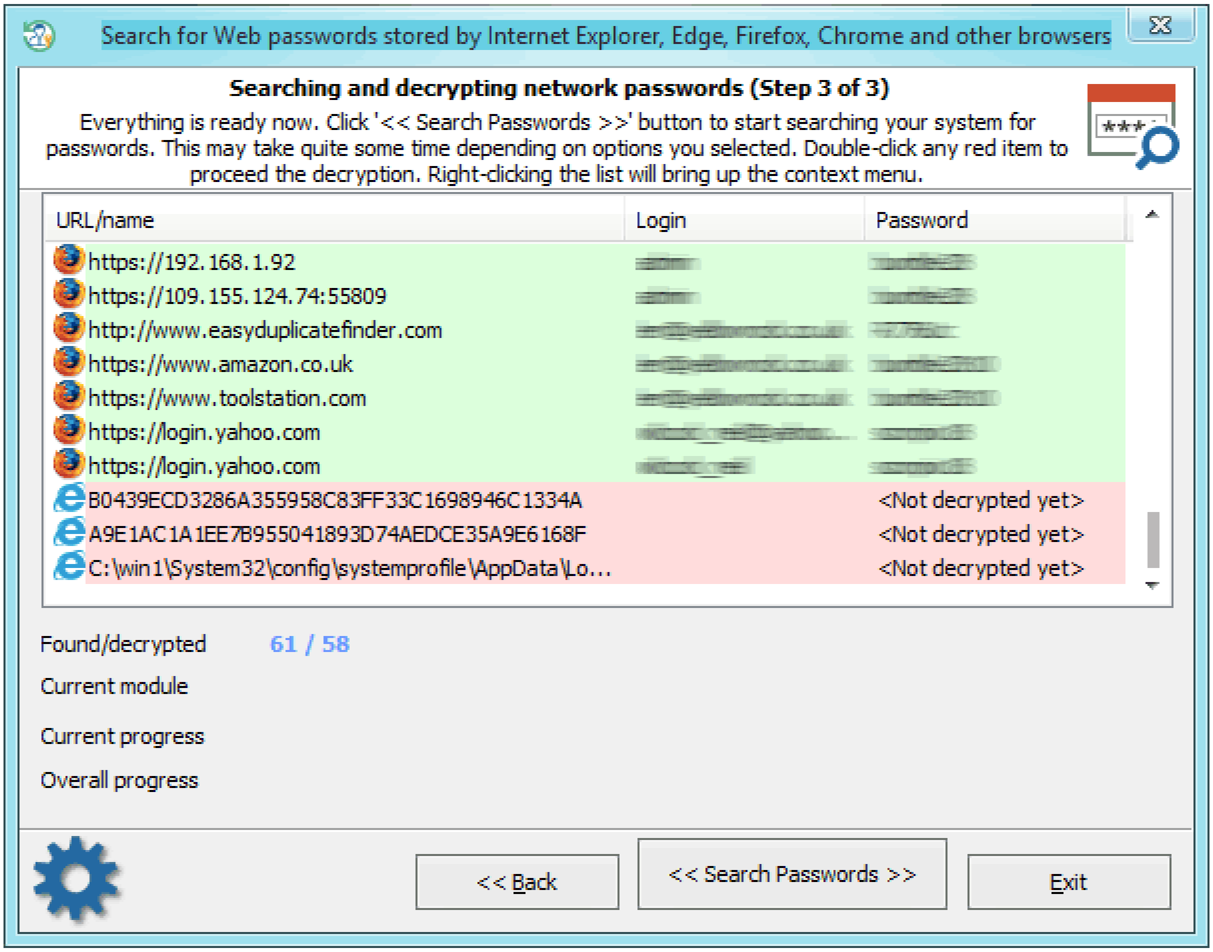
On the next step, specify the location of the Windows folder and the folders where the program will try to find the passwords: all user profiles or only the selected one. In the latter case, select the respective folder.

By default, the program automatically scans the system for any information (for example, TBAL or domain secrets) that can be used to decrypt DPAPI data without providing user logon passwords. However, setting the advanced option on, you can force the program to guess DPAPI Master Key passwords using some found items. For example, using cached credentials, LSA secrets, extracted browsers' passwords, wireless/dialup/dls/ras/lan and other network passwords, etc. Once a DPAPI Master Key password is guessed, there's no need to provide user logon credentials. The program uses the decrypted Master Key to decode any data protected with this Key.
However, the process may take quite some time depending on the number of found Master Keys and password items to guess.

In the final dialog, clicking the **<< Search Passwords >>** button launches the process of gathering, analyzing, and decrypting data. Please be patient; depending on the selected options and the number of users in the system, the process may take quite some time.

3.5.8.1 Search for Web passwords stored by Internet browsers

Selecting the internet password search opens a screen like this:



Search for Web passwords stored by Internet Explorer, Edge, Firefox, Chrome and other browsers

Searching and decrypting network passwords (Step 3 of 3)

Everything is ready now. Click '<< Search Passwords >>' button to start searching your system for passwords. This may take quite some time depending on options you selected. Double-click any red item to proceed the decryption. Right-clicking the list will bring up the context menu.

URL/name	Login	Password
https://192.168.1.92	[redacted]	[redacted]
https://109.155.124.74:55809	[redacted]	[redacted]
http://www.easyduplicatefinder.com	[redacted]	[redacted]
https://www.amazon.co.uk	[redacted]	[redacted]
https://www.toolstation.com	[redacted]	[redacted]
https://login.yahoo.com	[redacted]	[redacted]
https://login.yahoo.com	[redacted]	[redacted]
B0439ECD3286A355958C83FF33C1698946C1334A		<Not decrypted yet>
A9E1AC1A1EE7B955041893D74AEDCE35A9E6168F		<Not decrypted yet>
C:\win1\System32\config\systemprofile\AppData\Lo...		<Not decrypted yet>

Found/decrypted 61 / 58

Current module

Current progress

Overall progress

The application decrypts passwords from all major Web browsers:

- Internet Explorer
- Edge
- Firefox
- Opera
- Chrome
- Safari
- Majority of Mozilla-based browsers: Flock, Seamonkey, Pale Moon, Waterfox, etc.
- Major browsers based on Chromium sources: 360 Safe Browser, 7Star, Amigo, Brave, Centbrowser, Chedot, Canary, Coccoc, Comodo Dragon, Elements, Kometa, Orbitum, QQ Browser, Sputnik, Torch, UC Browser, Uran, Vivaldi.

Web browsers use different algorithms for protecting users' personal data. Passwords from the following browsers can be decrypted almost instantly:

- Internet Explorer 4-6
- Firefox and other Mozilla-based browsers (unless Master Password is set)
- Old versions of Opera (unless Master Password is set)

Decrypting other data requires additional information. That is usually the Master Password or the user logon password:

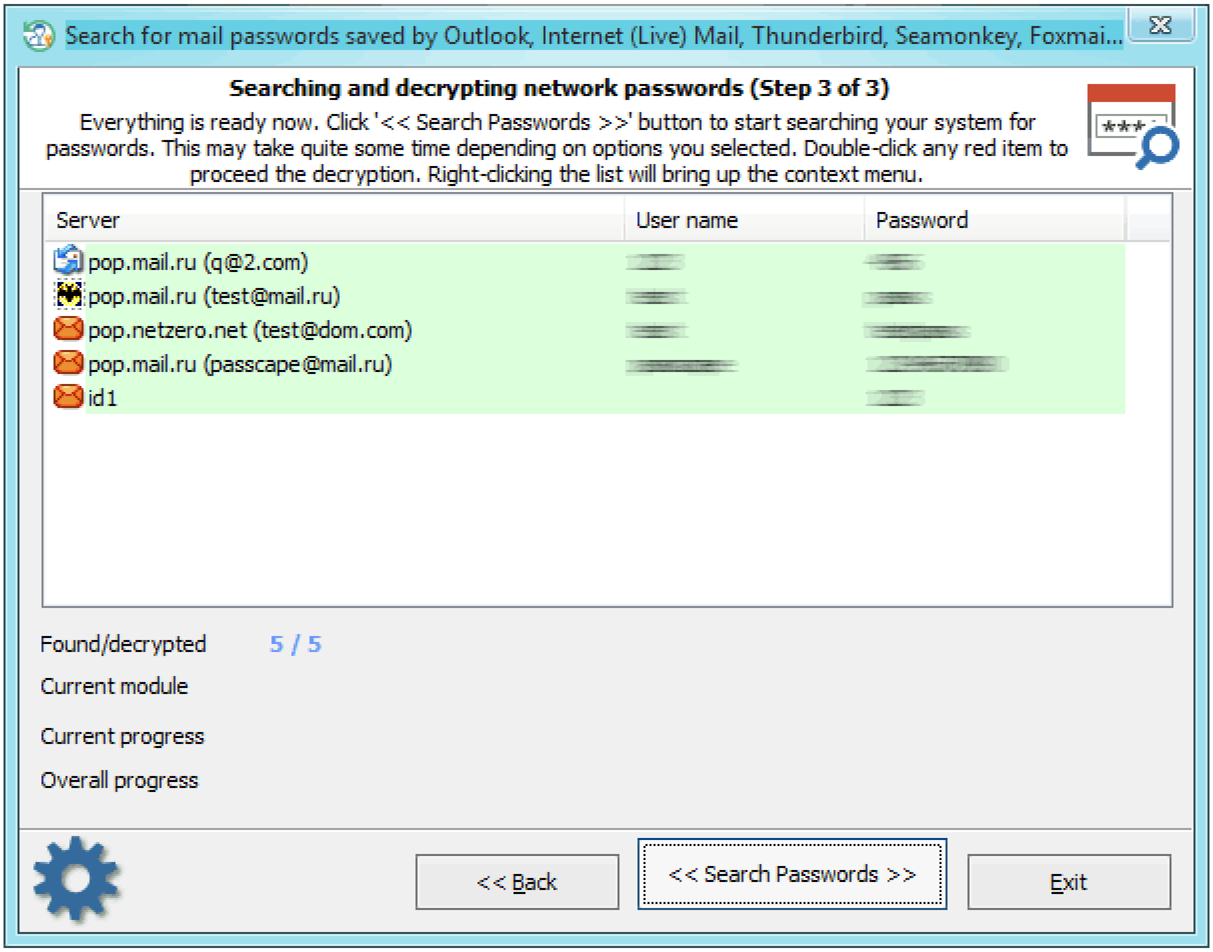
- Internet Explorer 10
- Edge
- Firefox (if Master Password is set)

- Opera (if Master Password is set)
- Chrome
- Safari

To activate the next step of the decryption, simply double-click on the record highlighted in red.

Internet Explorer 7-9 require three-step decryption. First, one should enter the URL where the password was saved, then enter the account password. More information on this tricky kind of protection used in Internet Explorer 7-9 can be found in our article.

3.5.8.2 Search for mail passwords saved by email clients



Search for mail passwords saved by Outlook, Internet (Live) Mail, Thunderbird, Seamonkey, Foxmai...

Searching and decrypting network passwords (Step 3 of 3)

Everything is ready now. Click '<< Search Passwords >>' button to start searching your system for passwords. This may take quite some time depending on options you selected. Double-click any red item to proceed the decryption. Right-clicking the list will bring up the context menu.

Server	User name	Password
pop.mail.ru (q@2.com)	[redacted]	[redacted]
pop.mail.ru (test@mail.ru)	[redacted]	[redacted]
pop.netzero.net (test@dom.com)	[redacted]	[redacted]
pop.mail.ru (passcape@mail.ru)	[redacted]	[redacted]
id1		[redacted]

Found/decrypted 5 / 5

Current module

Current progress

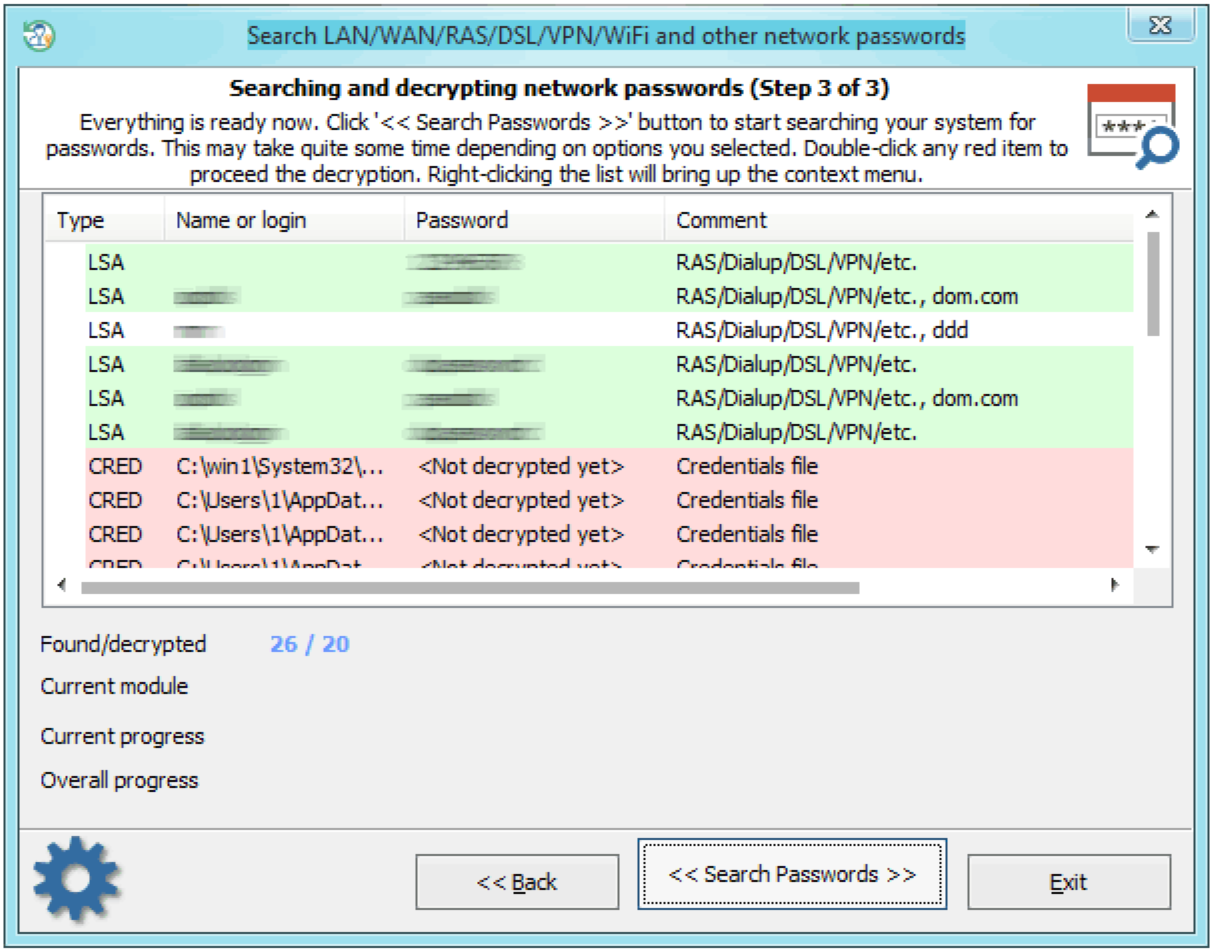
Overall progress

The following email clients are supported:

- Outlook Express
- Microsoft Office Outlook
- Internet Mail
- Internet Live Mail
- Windows Mail
- TheBat!
- Incredimail
- Eudora

Please keep in mind that some email passwords could be stored in browsers. This depends on whether the user used the email client or read their email using a Web browser. Passwords from Outlook Express, TheBat!, Incredimail, Eudora, and some versions of MS Office Outlook can be decrypted almost instantly. Decrypting other data requires the account password. Simply double-click on the record highlighted in red. That activates the second step of analyzing found data. If the entered user password matches the other records, they will be decoded automatically.

3.5.8.3 Search LAN/WAN/RAS/DSL/VPN/WiFi and other network passwords



Search LAN/WAN/RAS/DSL/VPN/WiFi and other network passwords

Searching and decrypting network passwords (Step 3 of 3)

Everything is ready now. Click '<< Search Passwords >>' button to start searching your system for passwords. This may take quite some time depending on options you selected. Double-click any red item to proceed the decryption. Right-clicking the list will bring up the context menu.

Type	Name or login	Password	Comment
LSA		[redacted]	RAS/Dialup/DSL/VPN/etc.
LSA	[redacted]	[redacted]	RAS/Dialup/DSL/VPN/etc., dom.com
LSA	[redacted]		RAS/Dialup/DSL/VPN/etc., ddd
LSA	[redacted]	[redacted]	RAS/Dialup/DSL/VPN/etc.
LSA	[redacted]	[redacted]	RAS/Dialup/DSL/VPN/etc., dom.com
LSA	[redacted]	[redacted]	RAS/Dialup/DSL/VPN/etc.
CRED	C:\win1\System32\...	<Not decrypted yet>	Credentials file
CRED	C:\Users\1\AppDat...	<Not decrypted yet>	Credentials file
CRED	C:\Users\1\AppDat...	<Not decrypted yet>	Credentials file
CRED	C:\Users\1\AppDat...	<Not decrypted yet>	Credentials file

Found/decrypted 26 / 20

Current module

Current progress

Overall progress

For gathering network passwords, the program has several modules for reading and decrypting secrets of LSA, protected storage, password manager, Windows Vault, etc.

The decryption of data stored in LSA secrets and in the protected storage is carried out automatically and does not require entering additional parameters. This applies to the following data:

- Cached user passwords
- Passwords of some system accounts, SQL server, remote assistant, etc.
- Passwords of services launched with specific credentials
- Some network passwords stored in server OSes
- Wired connection passwords: RAS, DSL, VPN, etc
- Passwords from old versions of Internet Explorer/Outlook/Outlook Express/FTP, etc.

- Passwords for wireless (WPA/WPA2) connections
- Passwords from domain group policies
- VNC passwords
- Passwords for Tortoise SVN accounts
- Open VPN passwords
- other

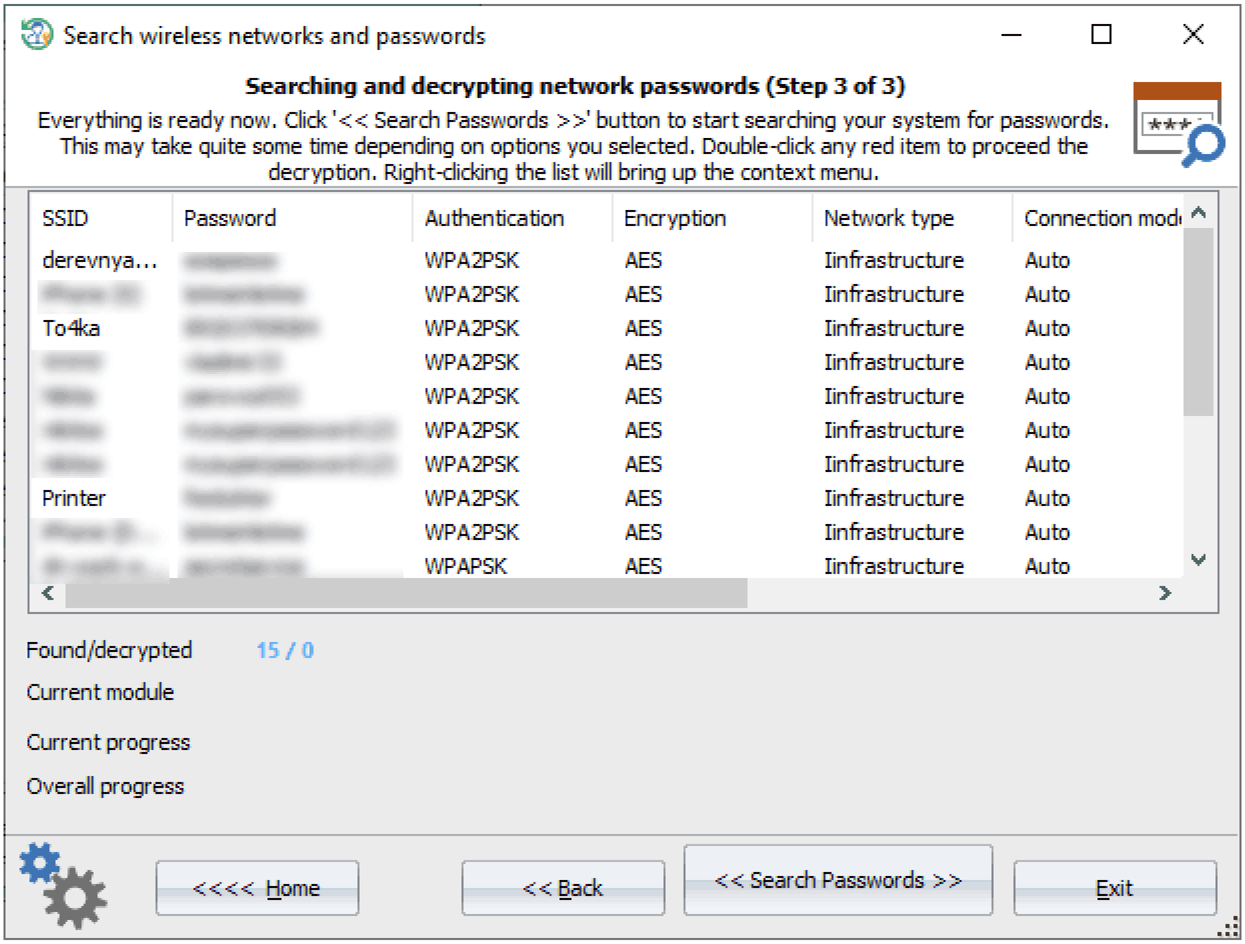
For other passwords protected with DPAPI, user account password is required for the successful decryption:

- Passwords stored in Credential manager: passwords for remote computers in your LAN, passwords for some mail accounts (stored by Microsoft Outlook), MSN Messenger passwords, Internet Explorer 7-9 passwords for Web sites that use Basic Authentication or Digest Access Authentication, Remote Desktop, RSS feed credentials, etc.
- Windows Vault records: passwords for some versions of Internet Explorer/Outlook/Windows Mail, account passwords when using PIN/Picture password or biometric authentication (only for Windows 8).

More on DPAPI encryption can be found in our detailed review that covers this protection method.

In some server operating systems, the program can successfully exploit the vulnerability we have found, which allows decrypting DPAPI blobs without entering the data owner’s account password! More information on this is available in our article that covers vulnerabilities in server OSes.

3.5.8.4 Search for wireless credentials



Searching and decrypting network passwords (Step 3 of 3)

Everything is ready now. Click '<< Search Passwords >>' button to start searching your system for passwords. This may take quite some time depending on options you selected. Double-click any red item to proceed the decryption. Right-clicking the list will bring up the context menu.

SSID	Password	Authentication	Encryption	Network type	Connection mod
derevnya...	[redacted]	WPA2PSK	AES	Infrastructure	Auto
[redacted]	[redacted]	WPA2PSK	AES	Infrastructure	Auto
To4ka	[redacted]	WPA2PSK	AES	Infrastructure	Auto
[redacted]	[redacted]	WPA2PSK	AES	Infrastructure	Auto
[redacted]	[redacted]	WPA2PSK	AES	Infrastructure	Auto
[redacted]	[redacted]	WPA2PSK	AES	Infrastructure	Auto
[redacted]	[redacted]	WPA2PSK	AES	Infrastructure	Auto
Printer	[redacted]	WPA2PSK	AES	Infrastructure	Auto
[redacted]	[redacted]	WPA2PSK	AES	Infrastructure	Auto
[redacted]	[redacted]	WPAPSK	AES	Infrastructure	Auto

Found/decrypted 15 / 0

Current module

Current progress

Overall progress

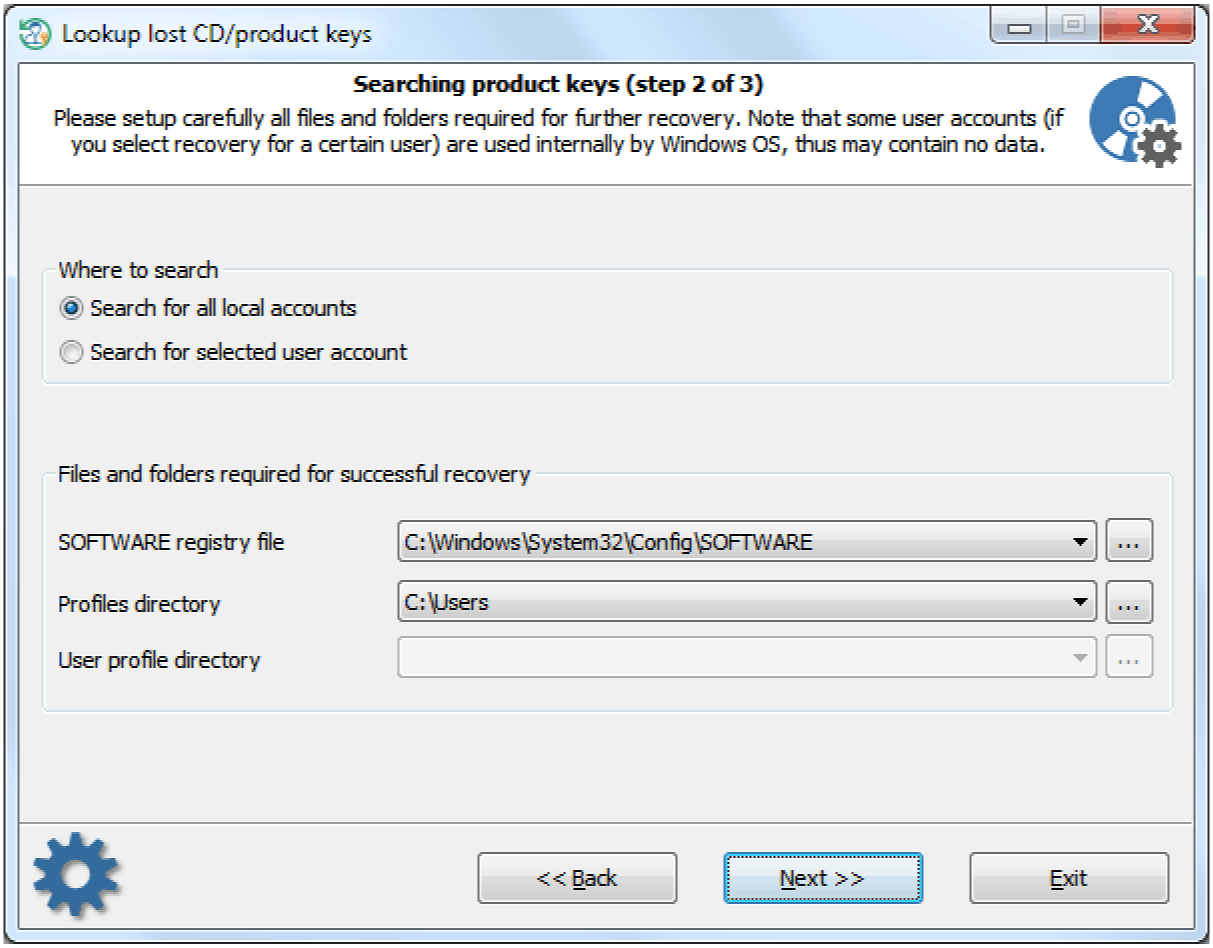
The program decrypts connection passwords of wireless networks for all user accounts instantly.

3.5.9 Search for lost product/CD keys

Using this feature, you can easily recover lost product keys and serial numbers, even if the target system is not bootable any longer.

Almost all commercial programs for Windows come with a serial key that binds the program to your PC and makes the software legal or fully featured. By losing this key, you will no longer have access to your own software unless you get the key back. Just imagine that one day you need to reinstall your operating system. There might be a lot of reasons why you want to do so, from updating to getting rid of viruses, fixing a problem, etc. And after reinstalling, you will find out that you need to reinstall most of your software and supply it with serial codes that you no longer have access to. Without the keys, you cannot reinstall the software.

Luckily, a large proportion of computer programs store their product keys in the Windows registry and thus can easily be extracted. That's what this feature is for. Using a built-in script language, the 'Reset Windows Password' can recover serial keys for more than 1,000 software products. And yet it is very simple to use.


Lookup lost CD/product keys

Searching product keys (step 2 of 3)

Please setup carefully all files and folders required for further recovery. Note that some user accounts (if you select recovery for a certain user) are used internally by Windows OS, thus may contain no data.

Where to search

● Search for all local accounts

○ Search for selected user account

Files and folders required for successful recovery

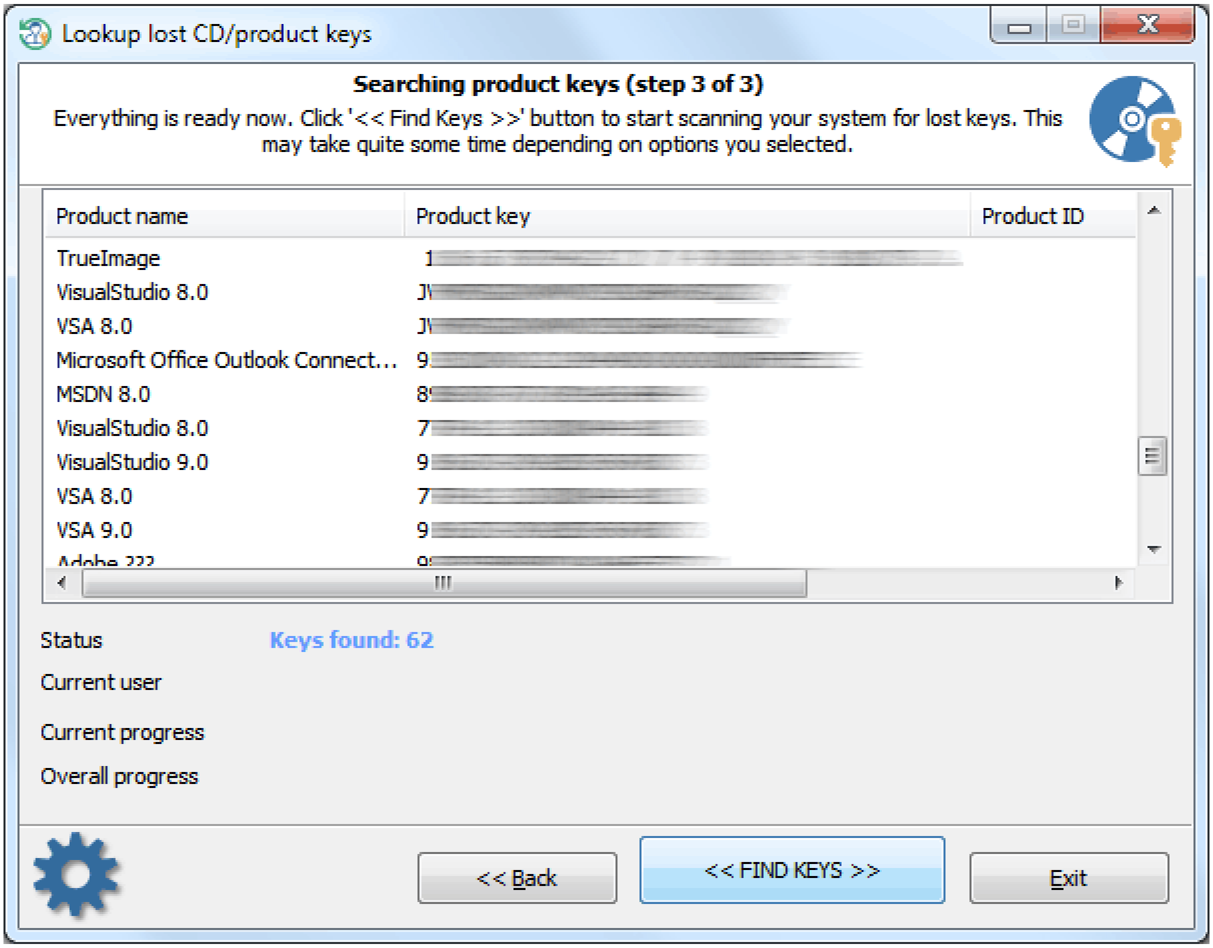
SOFTWARE registry file: C:\Windows\System32\Config\SOFTWARE

Profiles directory: C:\Users

User profile directory:

First, indicate to the program whether you need to recover serial keys for all local users or for a selected account only. Recovering keys for all user accounts needs at least two parameters to be set properly:
1. SOFTWARE registry file that is located at the following directory: *'C:\Windows\System32\Config'*. Note, the drive letter as well as the Windows folder may be different. For example, *'D:\Windows'*, *'E:\Win'*, etc.
2. Profiles folder. That is the directory where all local user accounts are physically stored. For Windows Vista and higher OSs, it is usually *'C:\Users'* while Windows XP uses the *'C:\Documents and Settings'* folder. Usually, the profiles folder is on the same drive where the Windows directory is located, not always though.
The program will attempt to detect these folders automatically. All you need to do is select one from the drop-down list or specify an alternative path otherwise.

If you need to recover serials for a certain user, just set the appropriate option and additionally select the user from the 'User profile directory' list.



Searching product keys (step 3 of 3)

Everything is ready now. Click '<< Find Keys >>' button to start scanning your system for lost keys. This may take quite some time depending on options you selected.

Product name	Product key	Product ID
TrueImage	[redacted]	
VisualStudio 8.0	[redacted]	
VSA 8.0	[redacted]	
Microsoft Office Outlook Connect...	[redacted]	
MSDN 8.0	[redacted]	
VisualStudio 8.0	[redacted]	
VisualStudio 9.0	[redacted]	
VSA 8.0	[redacted]	
VSA 9.0	[redacted]	
Adobe ???	[redacted]	

Status Keys found: 62

Current user

Current progress

Overall progress

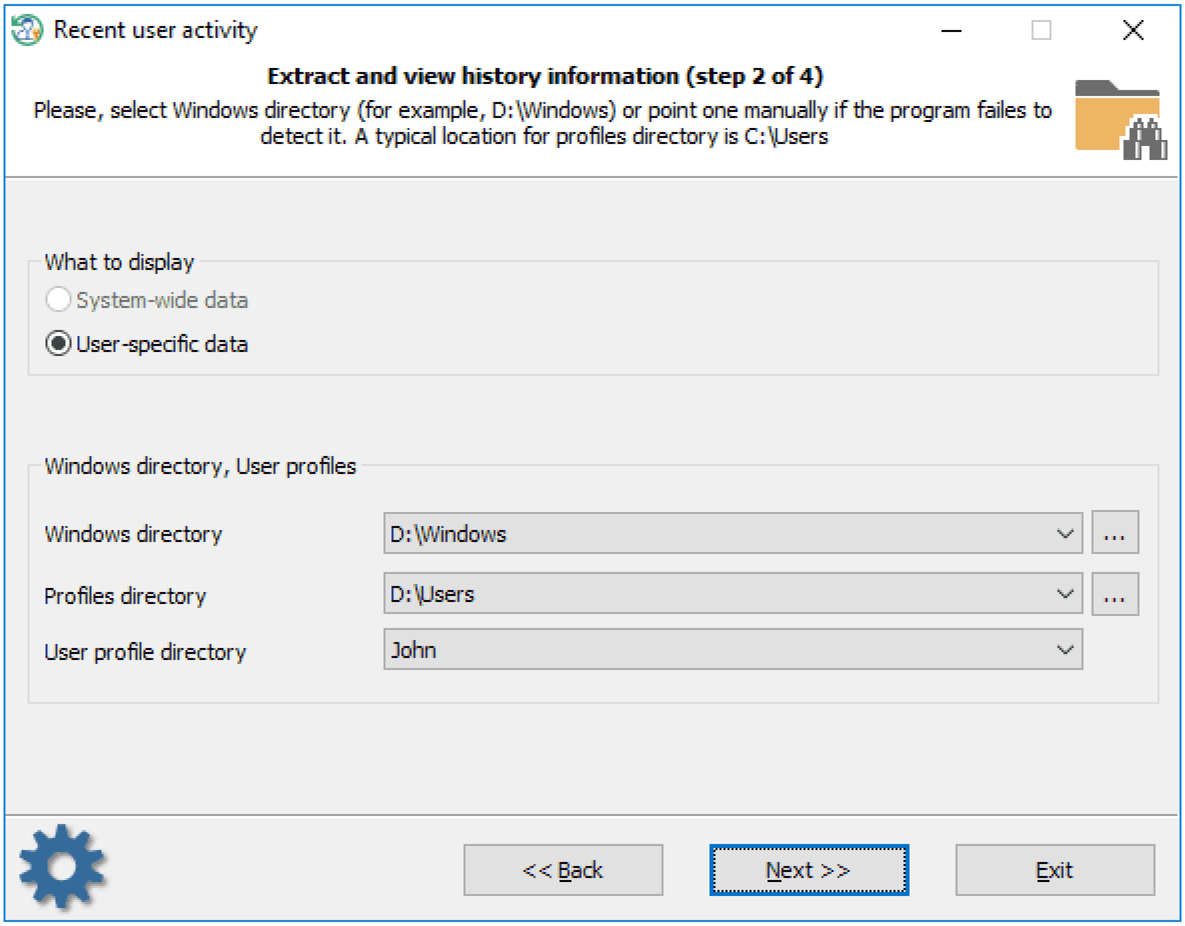
After the required options are set, proceed to the final step and clicking the *'<< FIND KEYS >>'* button to start the program searching for lost serial keys.

3.6 User activity

3.6.1 View recent user activity

This tool collects all available information about recent user activity occurred on this computer.

Selecting a type of activity



Recent user activity

Extract and view history information (step 2 of 4)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program failes to detect it. A typical location for profiles directory is C:\Users

What to display

○ System-wide data

● User-specific data

Windows directory, User profiles

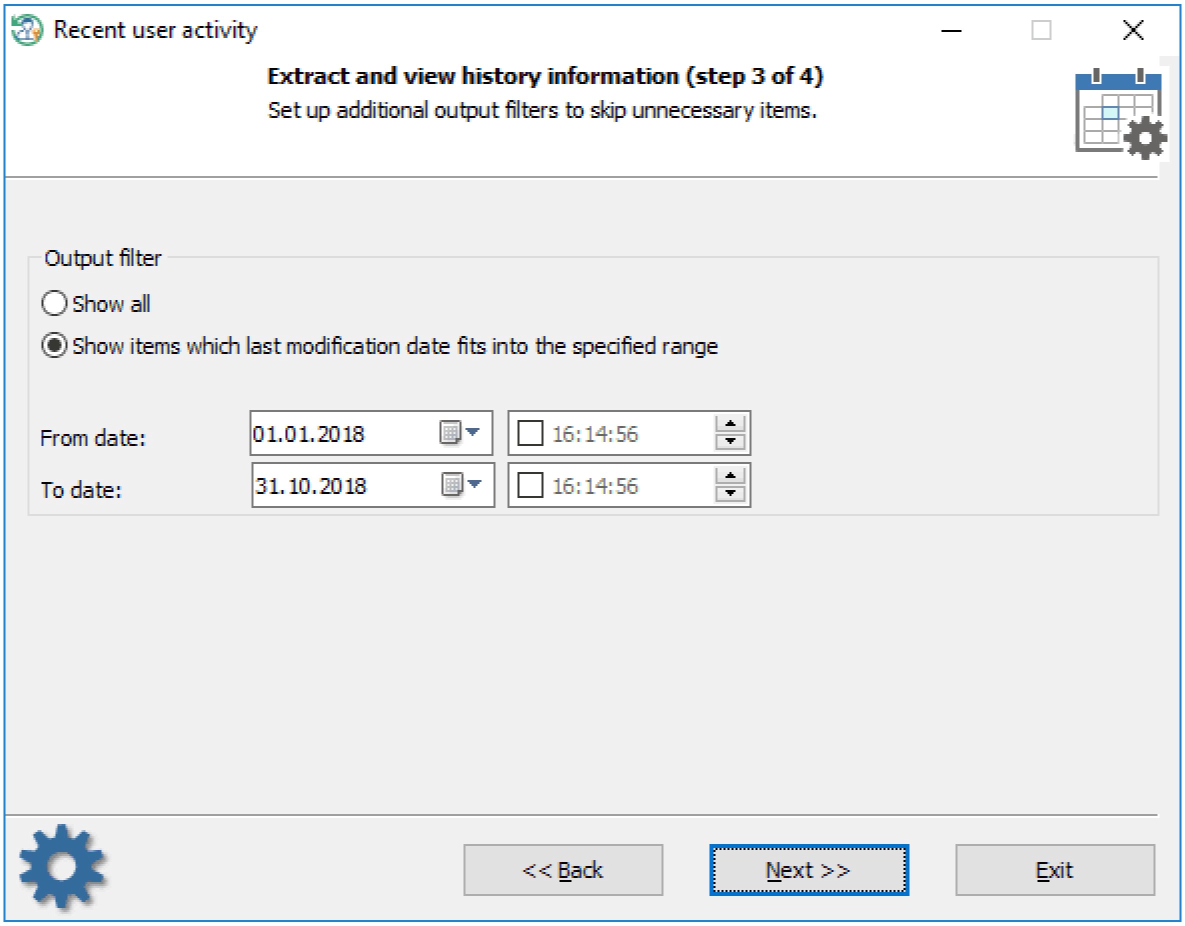
Windows directory: D:\Windows

Profiles directory: D:\Users

User profile directory: John

First of all, select if you want to view system-wide or user-specific data.

Setting output filters



Extract and view history information (step 3 of 4)

Set up additional output filters to skip unnecessary items.

Output filter

○ Show all

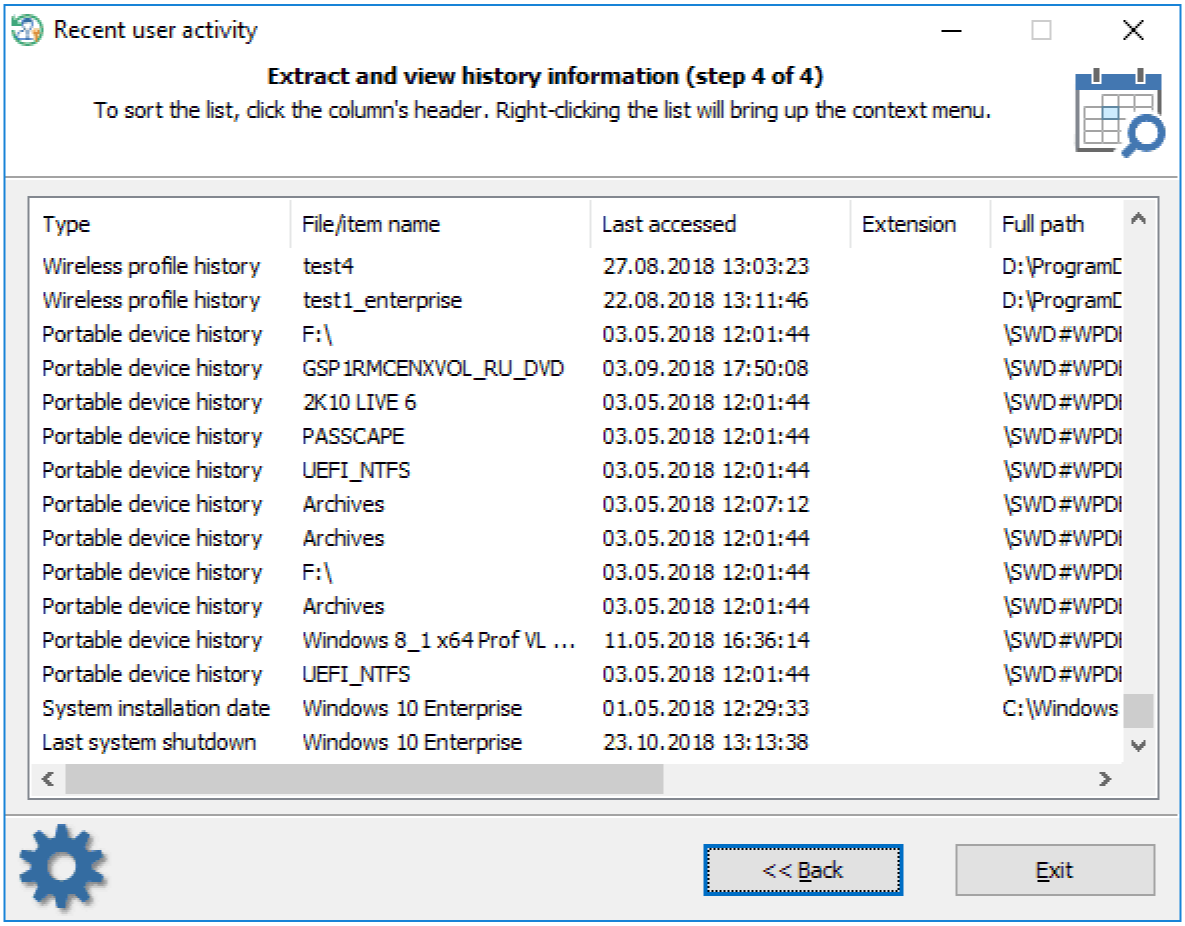
● Show items which last modification date fits into the specified range

From date: 01.01.2018 □ 16:14:56

To date: 31.10.2018 □ 16:14:56

Then specify if all entries are to be displayed or only ones that fit into specific time frames.

Displaying recent user activity



Extract and view history information (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu.

Type	File/item name	Last accessed	Extension	Full path
Wireless profile history	test4	27.08.2018 13:03:23		D:\ProgramD
Wireless profile history	test1_enterprise	22.08.2018 13:11:46		D:\ProgramD
Portable device history	F:\	03.05.2018 12:01:44		\SWD#WPDI
Portable device history	GSP1RMCENXVOL_RU_DVD	03.09.2018 17:50:08		\SWD#WPDI
Portable device history	2K10 LIVE 6	03.05.2018 12:01:44		\SWD#WPDI
Portable device history	PASSCAPE	03.05.2018 12:01:44		\SWD#WPDI
Portable device history	UEFI_NTFS	03.05.2018 12:01:44		\SWD#WPDI
Portable device history	Archives	03.05.2018 12:07:12		\SWD#WPDI
Portable device history	Archives	03.05.2018 12:01:44		\SWD#WPDI
Portable device history	F:\	03.05.2018 12:01:44		\SWD#WPDI
Portable device history	Archives	03.05.2018 12:01:44		\SWD#WPDI
Portable device history	Windows 8_1 x64 Prof VL ...	11.05.2018 16:36:14		\SWD#WPDI
Portable device history	UEFI_NTFS	03.05.2018 12:01:44		\SWD#WPDI
System installation date	Windows 10 Enterprise	01.05.2018 12:29:33		C:\Windows
Last system shutdown	Windows 10 Enterprise	23.10.2018 13:13:38		

Be patient, gathering the statistics may take quite some time.
To hide unnecessary record(s), right-click your mouse on the list and select the appropriate menu item.

The current version of the program supports for the following information (some items are not available in old OSes):

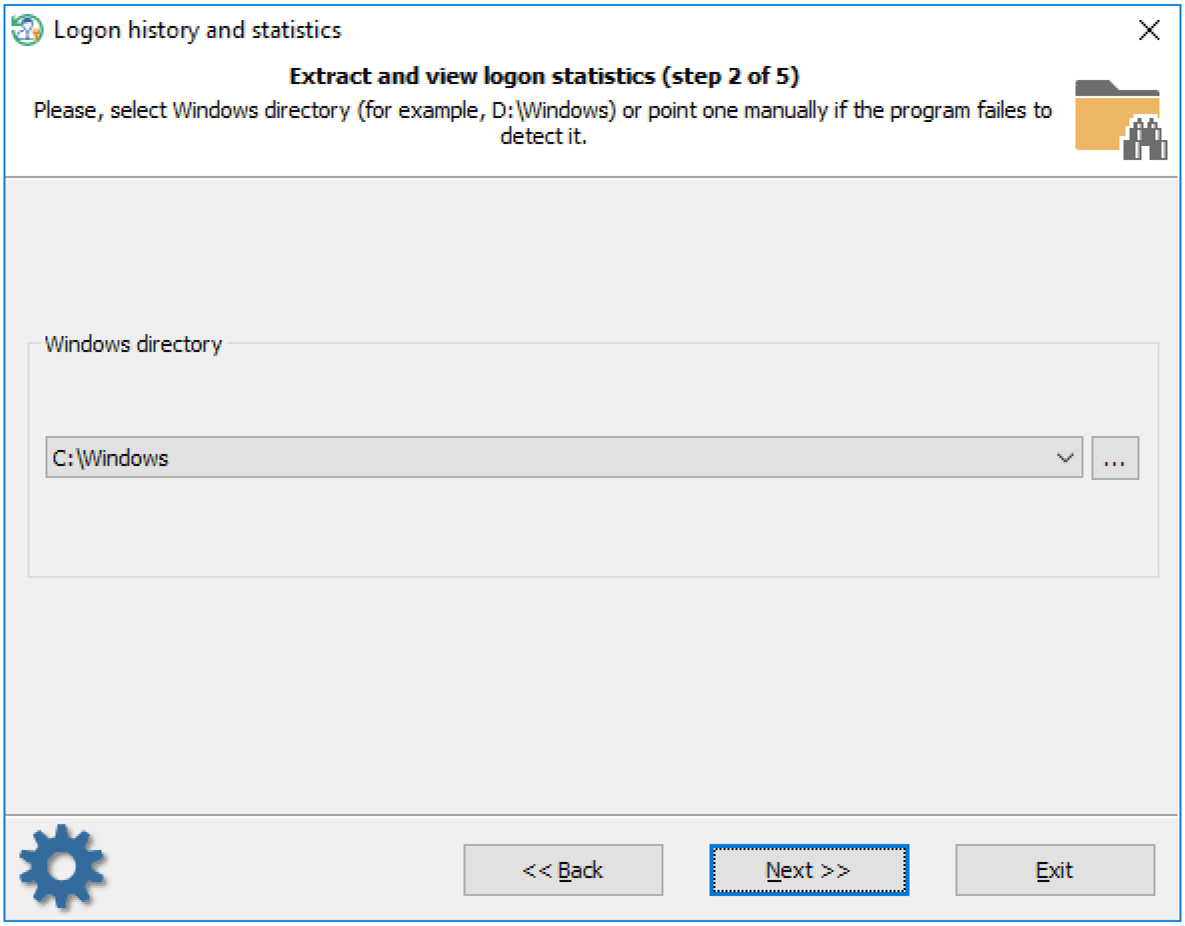
- Last items in file open/save dialogs
- Task Run items
- Mapped network drives
- Recent network find items
- Recent file/folder find items
- Recent files of Windows applets
- Last opened Regedit key
- Recently opened documents
- Recently opened MS Office documents
- Recent Outlook accounts and connections
- Recently run applications
- Recent application items
- Recent RDP connections
- Internet Explorer typed URLs
- Explorer typed paths
- Explorer search history
- Explorer User Assist items
- Recent background activity items
- Recent desktop activity items

- Wireless connections
- Bluetooth activity
- Recent portable devices
- Windows installation date
- Last system shutdown date

3.6.2 View logon history and statistics

This is a tool to view miscellaneous logon statistics of both regular and domain users.

Selecting Windows directory



Logon history and statistics

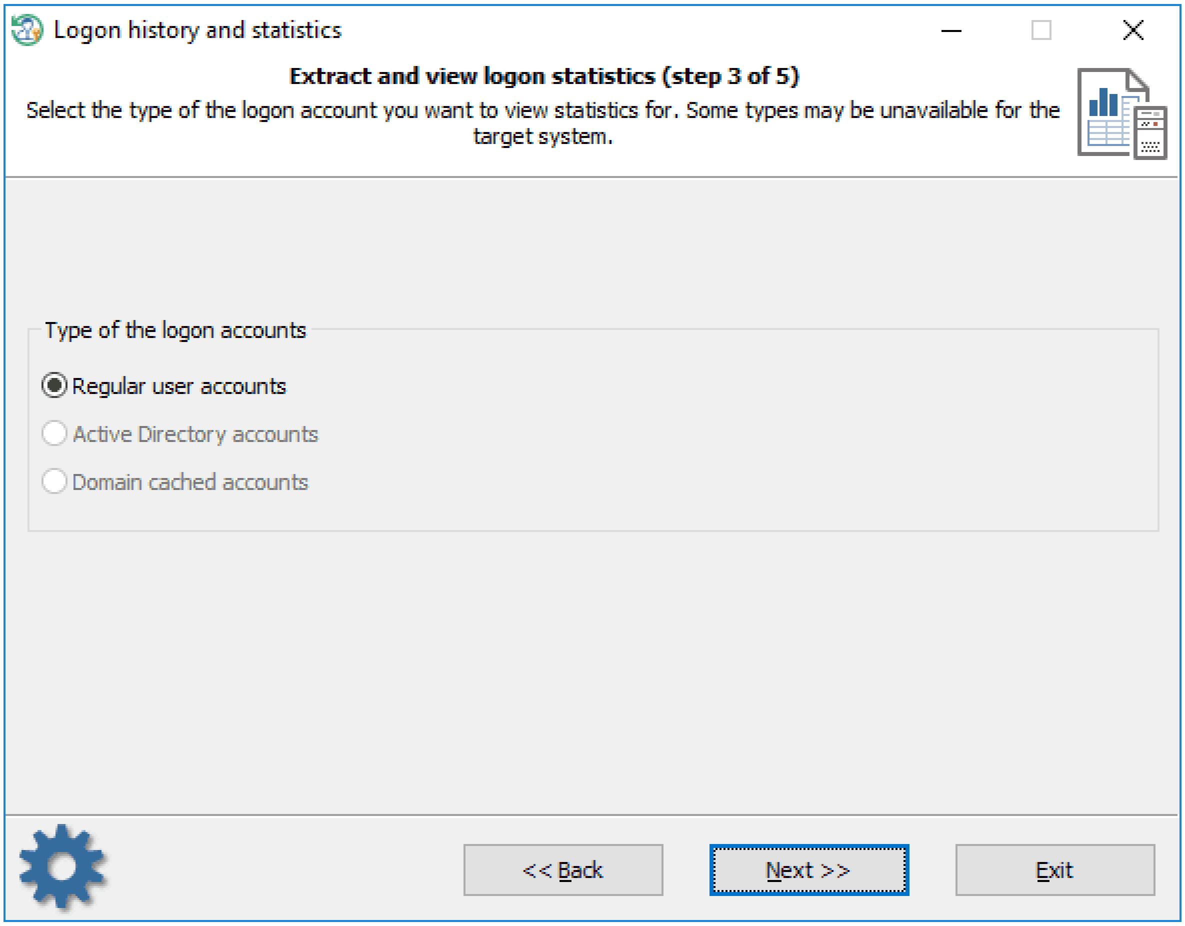
Extract and view logon statistics (step 2 of 5)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program failes to detect it.

Windows directory: C:\Windows

First of all, you should select a target Windows directory or browse for it if the program fails to detect one automatically.

Type of the logon accounts



Logon history and statistics

Extract and view logon statistics (step 3 of 5)

Select the type of the logon account you want to view statistics for. Some types may be unavailable for the target system.

Type of the logon accounts

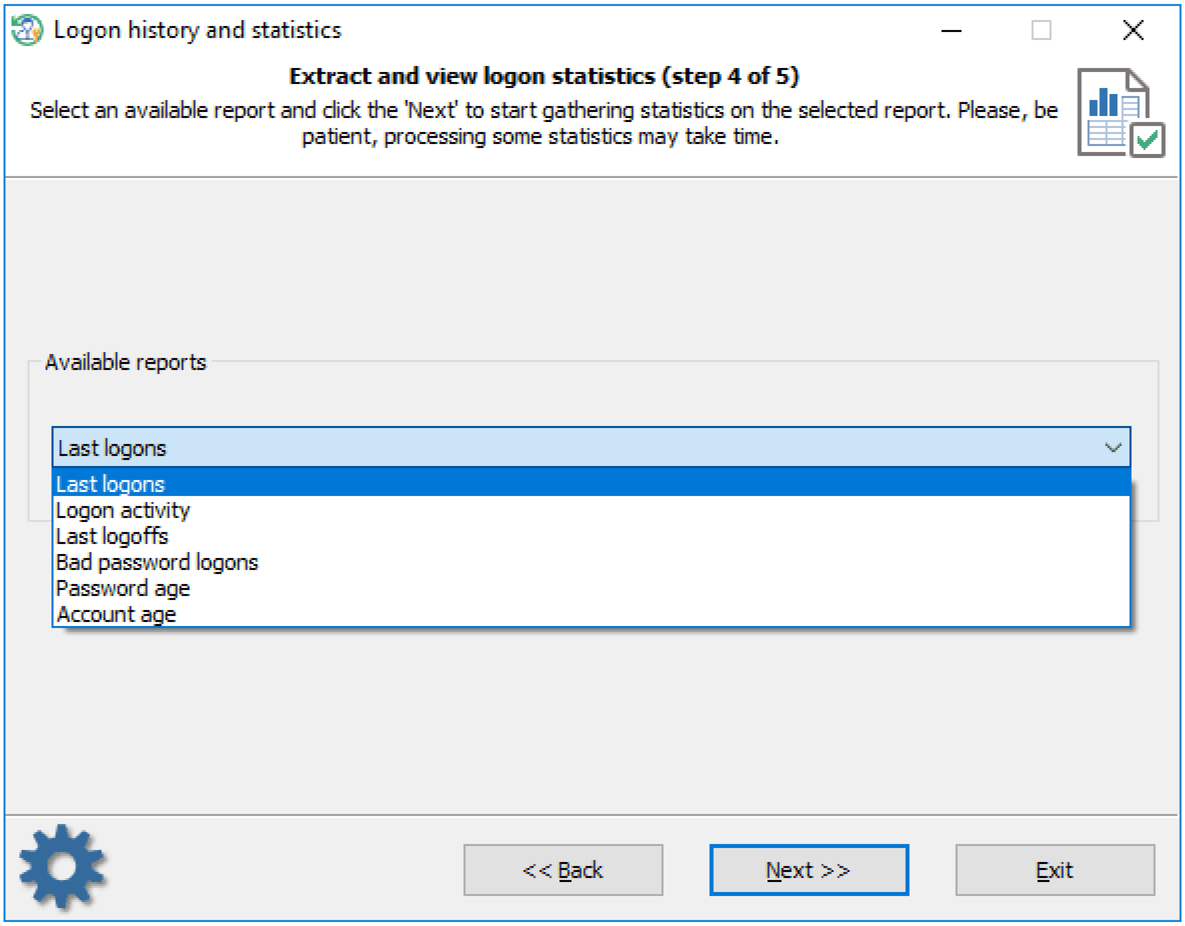
● Regular user accounts

○ Active Directory accounts

○ Domain cached accounts

Once the Windows directory is selected, the program will try to detect if the system contains any domain accounts (in addition to regular ones). Select the type of the logon accounts you want to view the statistics for and proceed to the next step.

Available reports



Extract and view logon statistics (step 4 of 5)

Select an available report and click the 'Next' to start gathering statistics on the selected report. Please, be patient, processing some statistics may take time.

Available reports

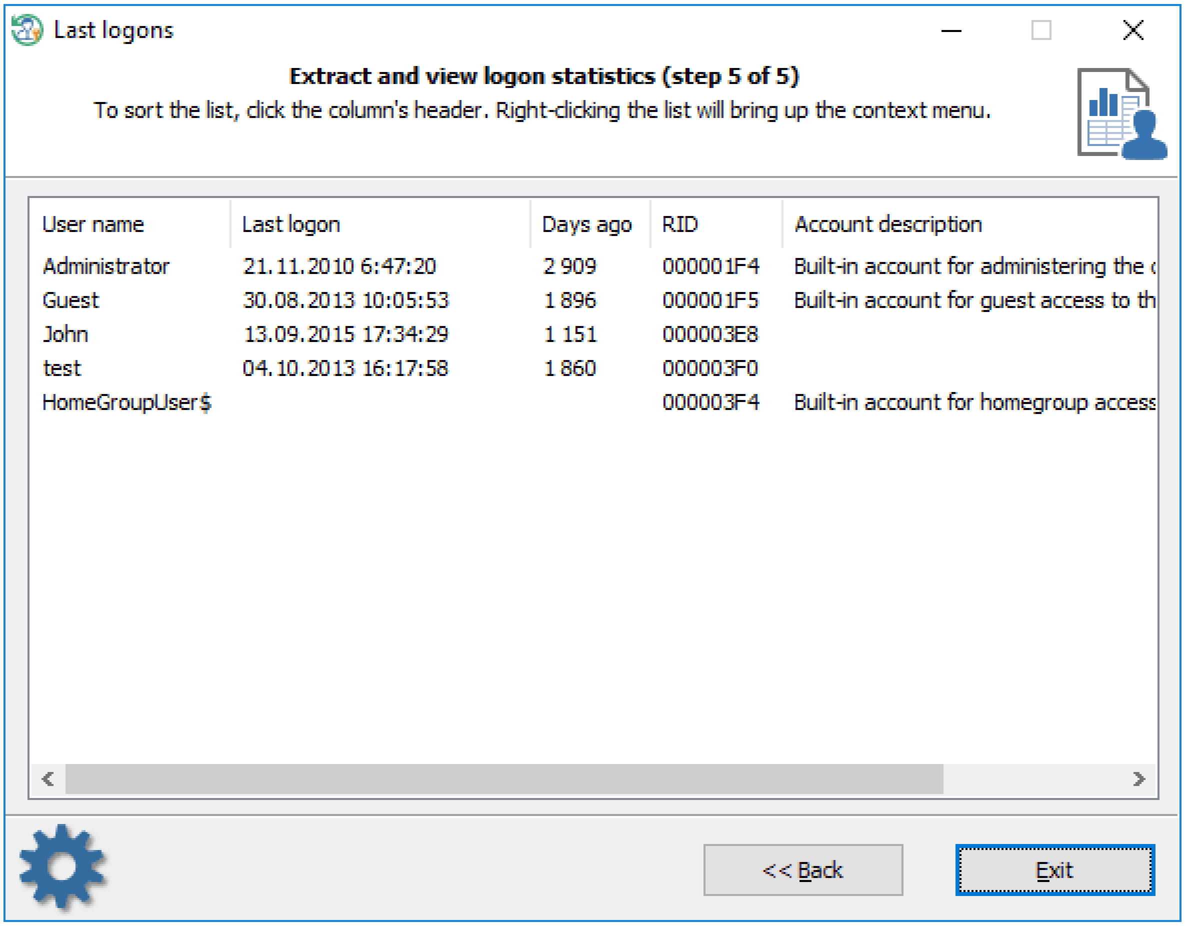
Last logons

Here you can choose one of the following reports:

- Last logons - displays last logon date of the users
- Logon activity - outputs most active users
- Last logoffs - unfortunately, most versions of Windows stopped saving the logoff date. However, some related information is available in 'User activity'.
- Bad password logons - the last time when a user attempted to log on into his/her account with an invalid password.
- Password age - the last time when a user changed his/her password.
- Account age - when the account was created first.

Some of the reports are unavailable for domain cached accounts.

Logon statistics



Extract and view logon statistics (step 5 of 5)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu.

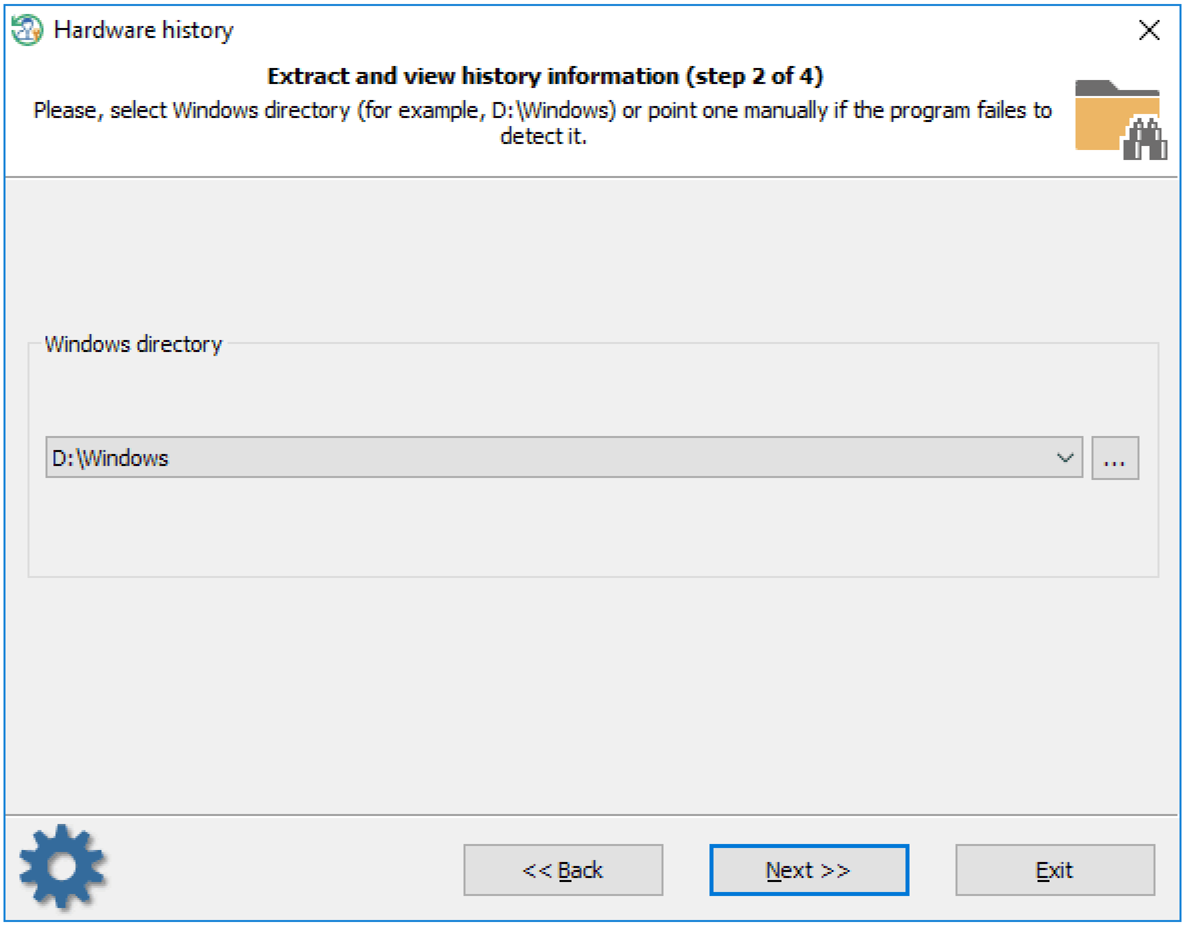
User name	Last logon	Days ago	RID	Account description
Administrator	21.11.2010 6:47:20	2 909	000001F4	Built-in account for administering the c
Guest	30.08.2013 10:05:53	1 896	000001F5	Built-in account for guest access to th
John	13.09.2015 17:34:29	1 151	000003E8	
test	04.10.2013 16:17:58	1 860	000003F0	
HomeGroupUser$			000003F4	Built-in account for homegroup access

You can copy statistics to the clipboard or save it to file.

3.6.3 Vew hardware history

The hardware history enumerates all hardware of the target OS and sorts it by installation or last arrival/removal date.

Selecting Windows directory



Hardware history

Extract and view history information (step 2 of 4)

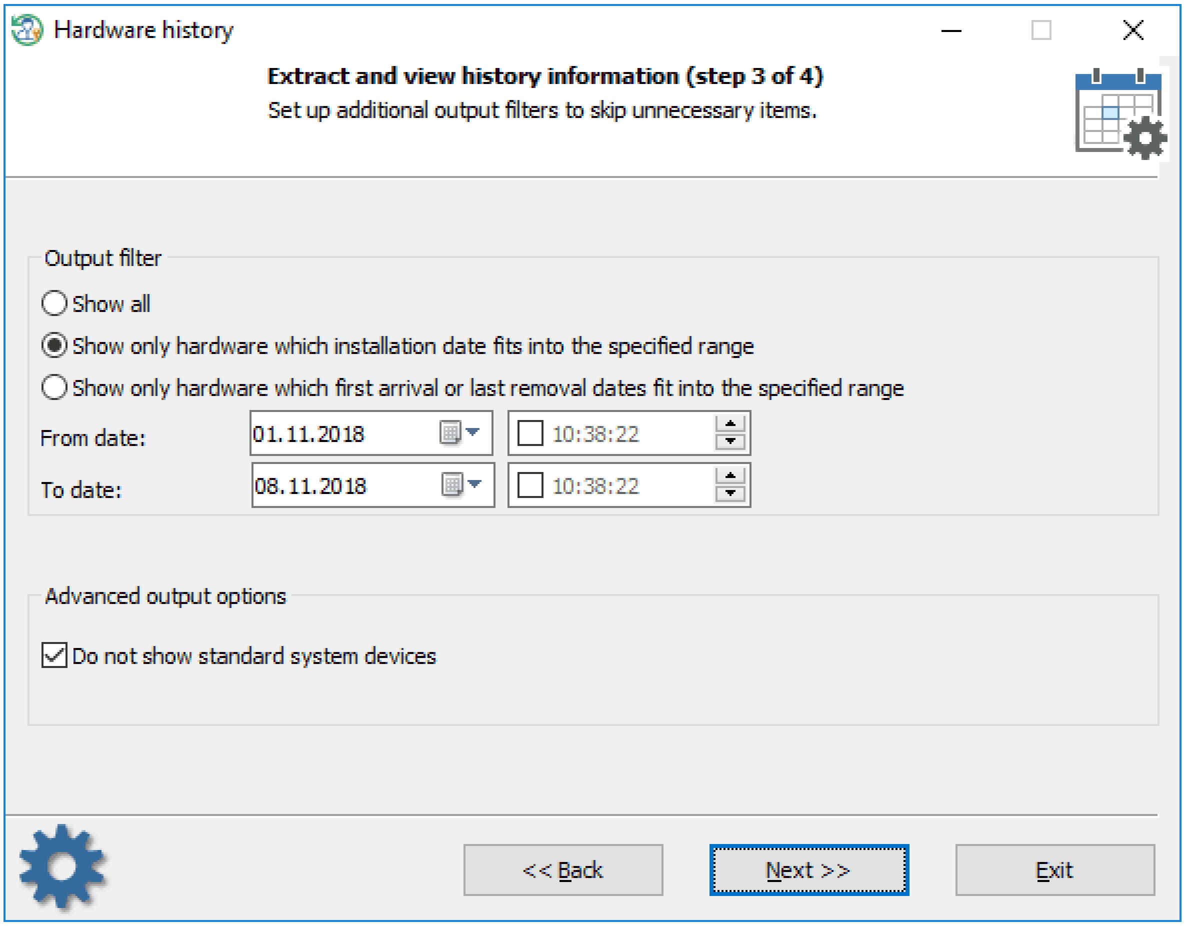
Please, select Windows directory (for example, D:\Windows) or point one manually if the program failes to detect it.

Windows directory

D:\Windows

Select the target Windows folder first. The program usually does it automatically.

Select output filters



Hardware history

Extract and view history information (step 3 of 4)

Set up additional output filters to skip unnecessary items.

Output filter

○ Show all

● Show only hardware which installation date fits into the specified range

○ Show only hardware which first arrival or last removal dates fit into the specified range

From date: 01.11.2018 □ 10:38:22

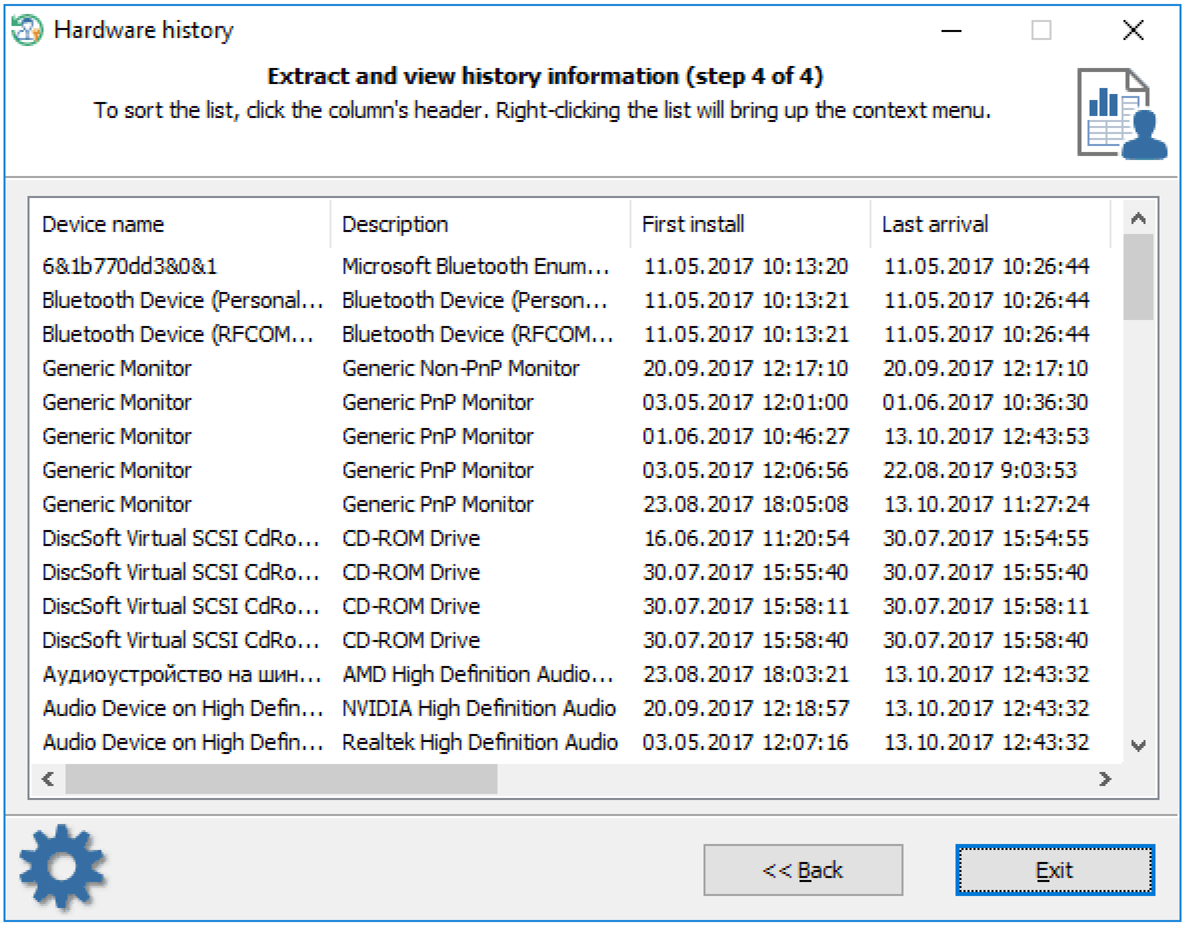
To date: 08.11.2018 □ 10:38:22

Advanced output options

☑ Do not show standard system devices

Set up additional output filters to skip unnecessary items. You can set the program up so that to display only hardware that was installed or arrived/removed last time on the date you specified.

Hardware history information



Extract and view history information (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu.

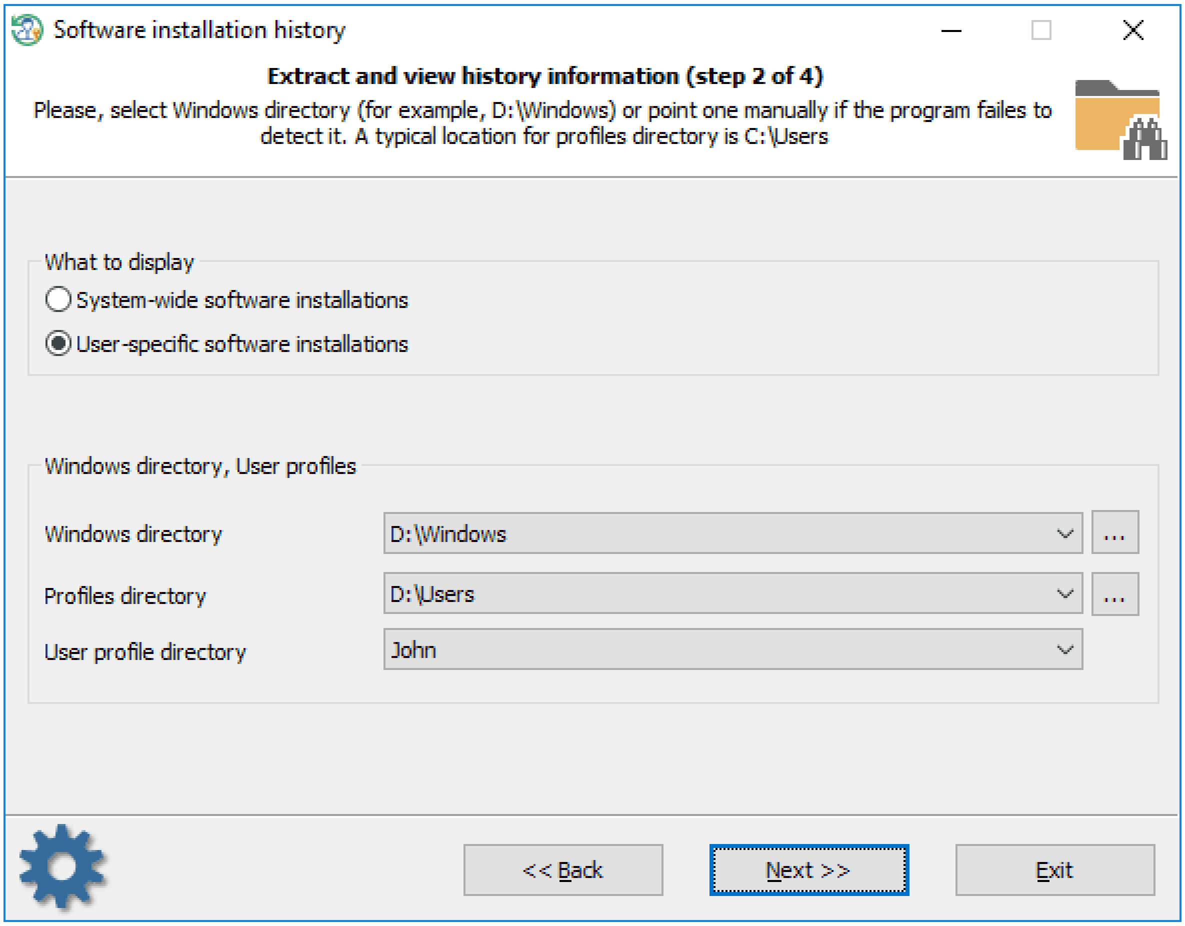
Device name	Description	First install	Last arrival
6&1b770dd3&0&1	Microsoft Bluetooth Enum...	11.05.2017 10:13:20	11.05.2017 10:26:44
Bluetooth Device (Personal...	Bluetooth Device (Person...	11.05.2017 10:13:21	11.05.2017 10:26:44
Bluetooth Device (RFCOM...	Bluetooth Device (RFCOM...	11.05.2017 10:13:21	11.05.2017 10:26:44
Generic Monitor	Generic Non-PnP Monitor	20.09.2017 12:17:10	20.09.2017 12:17:10
Generic Monitor	Generic PnP Monitor	03.05.2017 12:01:00	01.06.2017 10:36:30
Generic Monitor	Generic PnP Monitor	01.06.2017 10:46:27	13.10.2017 12:43:53
Generic Monitor	Generic PnP Monitor	03.05.2017 12:06:56	22.08.2017 9:03:53
Generic Monitor	Generic PnP Monitor	23.08.2017 18:05:08	13.10.2017 11:27:24
DiscSoft Virtual SCSI CdRo...	CD-ROM Drive	16.06.2017 11:20:54	30.07.2017 15:54:55
DiscSoft Virtual SCSI CdRo...	CD-ROM Drive	30.07.2017 15:55:40	30.07.2017 15:55:40
DiscSoft Virtual SCSI CdRo...	CD-ROM Drive	30.07.2017 15:58:11	30.07.2017 15:58:11
DiscSoft Virtual SCSI CdRo...	CD-ROM Drive	30.07.2017 15:58:40	30.07.2017 15:58:40
Аудиоустройство на шин...	AMD High Definition Audio...	23.08.2017 18:03:21	13.10.2017 12:43:32
Audio Device on High Defin...	NVIDIA High Definition Audio	20.09.2017 12:18:57	13.10.2017 12:43:32
Audio Device on High Defin...	Realtek High Definition Audio	03.05.2017 12:07:16	13.10.2017 12:43:32

To sort the list, click one of the columns.

3.6.4 Vew software history

The software history displays all the programs that were installed in the target OS.

Selecting a type of software installations



Software installation history

Extract and view history information (step 2 of 4)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program failes to detect it. A typical location for profiles directory is C:\Users

What to display

○ System-wide software installations

● User-specific software installations

Windows directory, User profiles

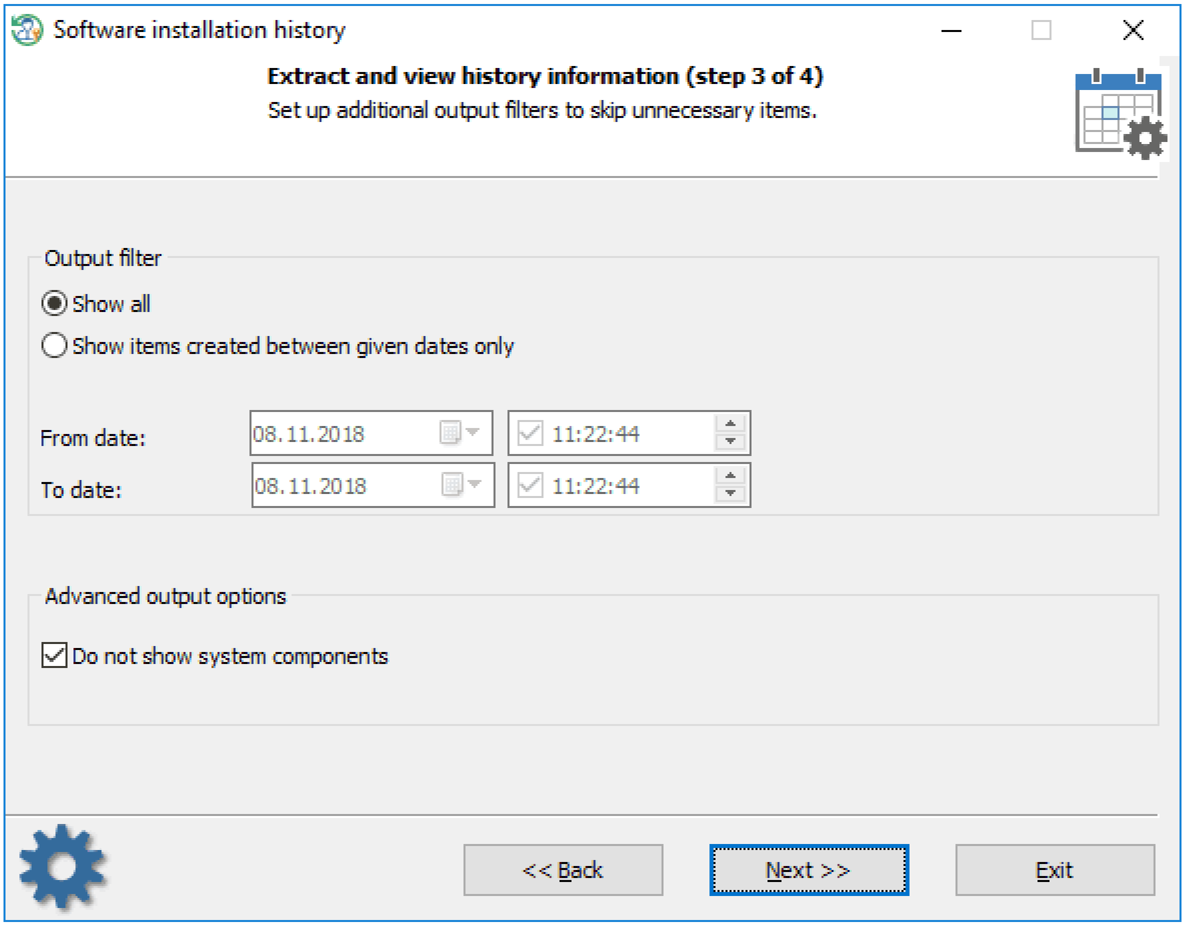
Windows directory: D:\Windows

Profiles directory: D:\Users

User profile directory: John

Select what type of the software installations you want to view. This is either user specific installations (programs installed for a certain user account) or system-wide installations (programs that are available for all users).

Output filters



Software installation history

Extract and view history information (step 3 of 4)

Set up additional output filters to skip unnecessary items.

Output filter

● Show all

○ Show items created between given dates only

From date: 08.11.2018 ☑ 11:22:44

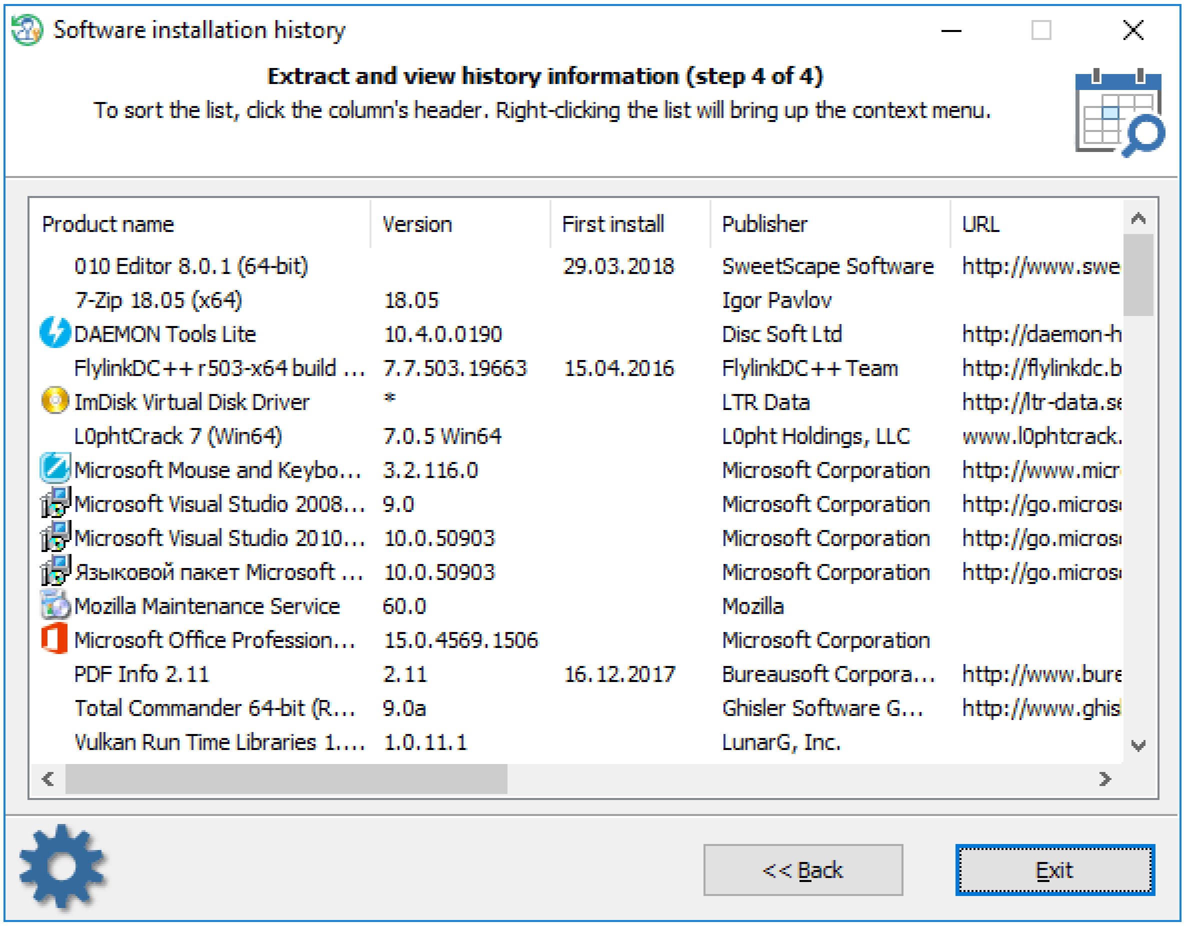
To date: 08.11.2018 ☑ 11:22:44

Advanced output options

☑ Do not show system components

You can point the program to display all items or items that were created between given dates only. The additional option is aimed to hide some system components, like system updates, etc.

Software installations



Extract and view history information (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu.

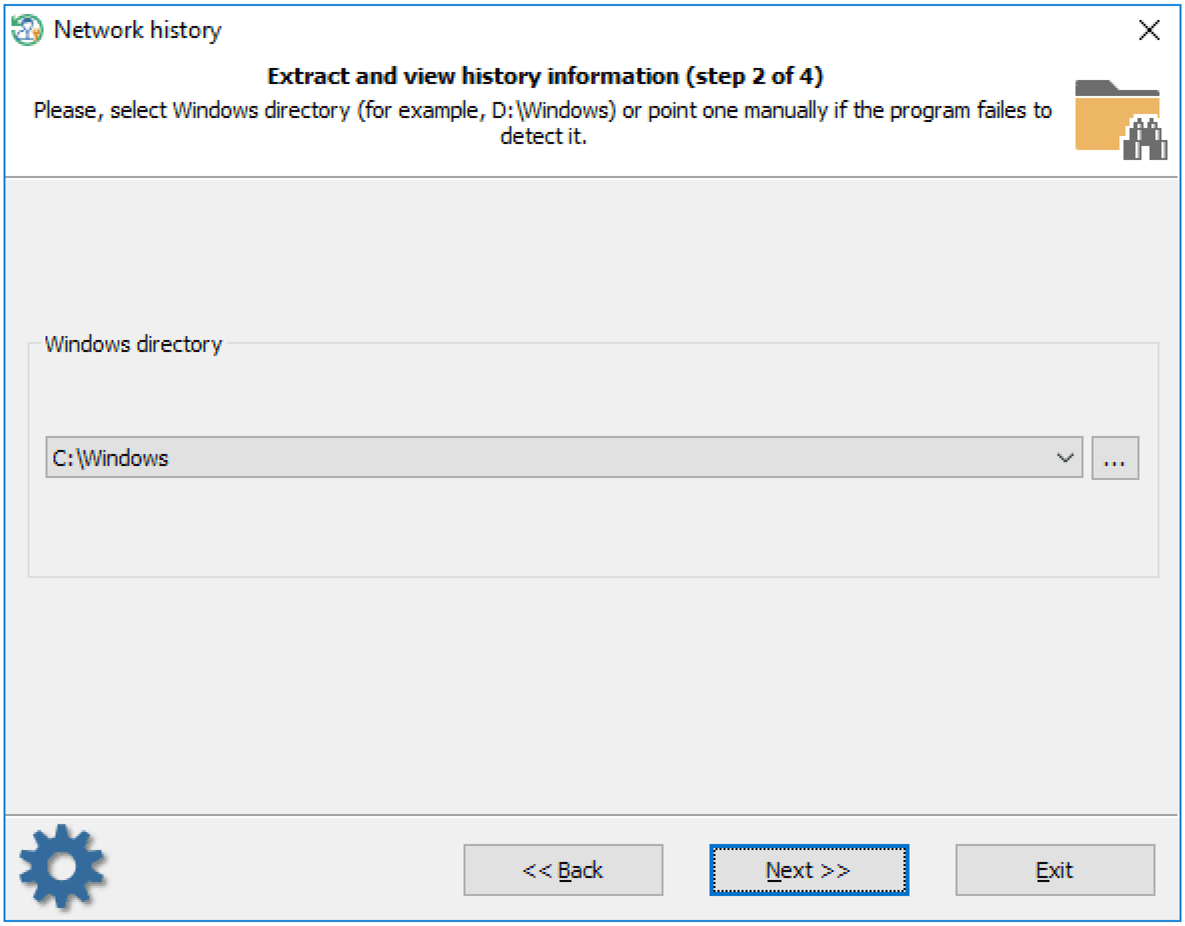
Product name	Version	First install	Publisher	URL
010 Editor 8.0.1 (64-bit)		29.03.2018	SweetScape Software	http://www.swe
7-Zip 18.05 (x64)	18.05		Igor Pavlov	
DAEMON Tools Lite	10.4.0.0190		Disc Soft Ltd	http://daemon-h
FlylinkDC++ r503-x64 build ...	7.7.503.19663	15.04.2016	FlylinkDC++ Team	http://flylinkdc.b
ImDisk Virtual Disk Driver	*		LTR Data	http://ltr-data.se
L0phtCrack 7 (Win64)	7.0.5 Win64		L0pht Holdings, LLC	www.l0phtcrack.
Microsoft Mouse and Keybo...	3.2.116.0		Microsoft Corporation	http://www.micr
Microsoft Visual Studio 2008...	9.0		Microsoft Corporation	http://go.micros
Microsoft Visual Studio 2010...	10.0.50903		Microsoft Corporation	http://go.micros
Языковой пакет Microsoft ...	10.0.50903		Microsoft Corporation	http://go.micros
Mozilla Maintenance Service	60.0		Mozilla	
Microsoft Office Profession...	15.0.4569.1506		Microsoft Corporation	
PDF Info 2.11	2.11	16.12.2017	Bureausoft Corpora...	http://www.bure
Total Commander 64-bit (R...	9.0a		Ghisler Software G...	http://www.ghis
Vulkan Run Time Libraries 1....	1.0.11.1		LunarG, Inc.	

To sort the list click one of the columns.

3.6.5 Vew network history

The network connection history displays all available networks along with their installation and last connection dates.

Selecting Windows directory



Network history

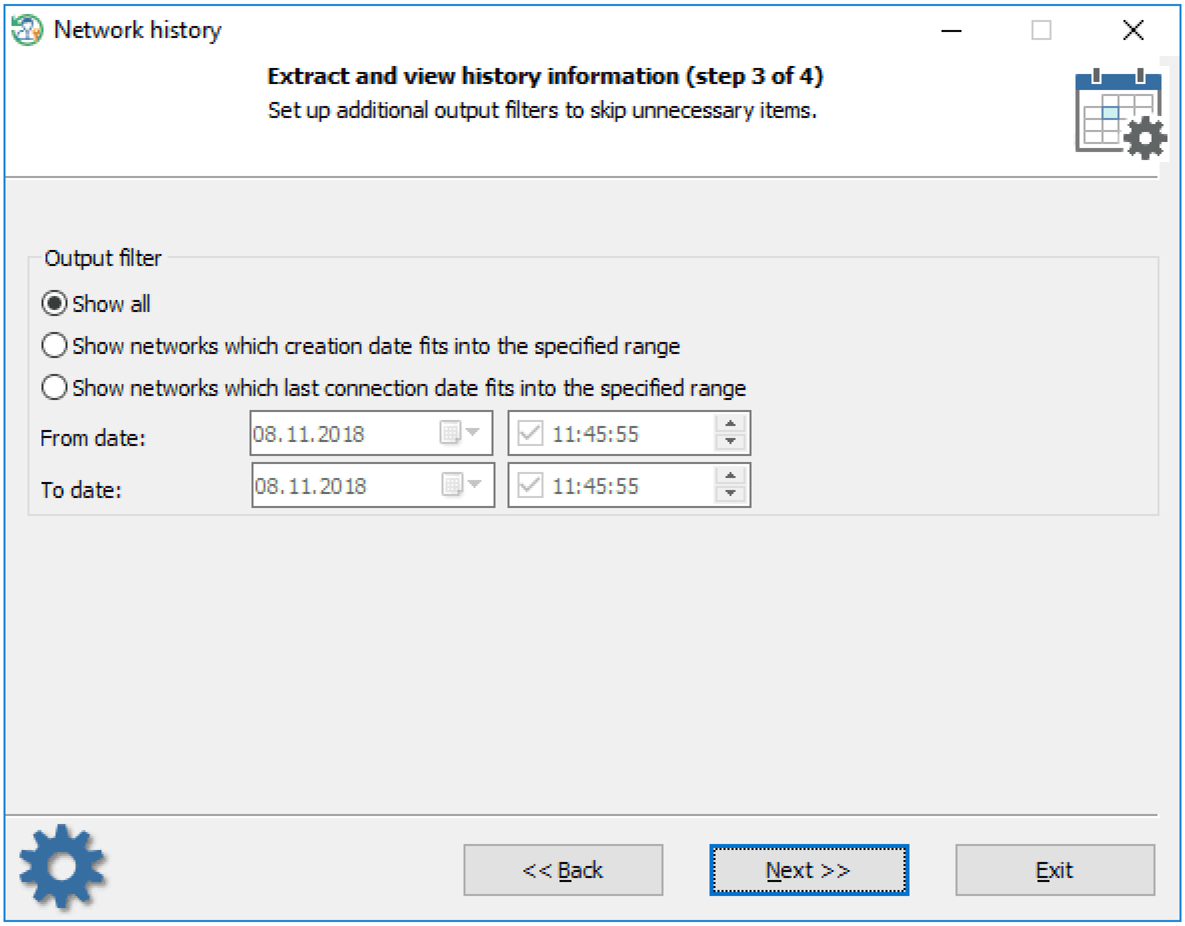
Extract and view history information (step 2 of 4)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program failes to detect it.

Windows directory: C:\Windows

Select the target Windows folder first. The program should do it for you.

Setting output filters



Extract and view history information (step 3 of 4)

Set up additional output filters to skip unnecessary items.

Output filter

● Show all

○ Show networks which creation date fits into the specified range

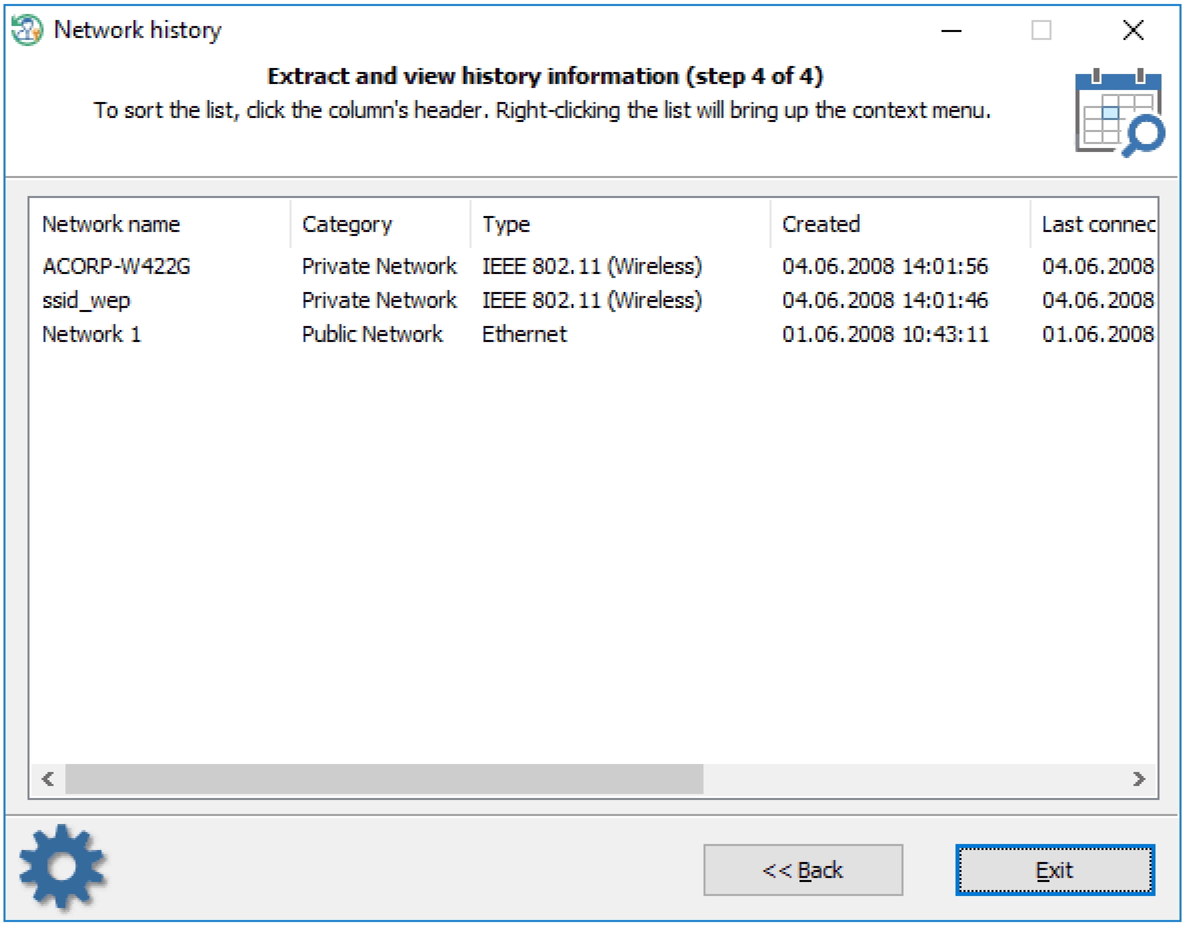
○ Show networks which last connection date fits into the specified range

From date: 08.11.2018 ☑ 11:45:55

To date: 08.11.2018 ☑ 11:45:55

Set up additional output filters to display only networks of your interest.

Network connection history



Extract and view history information (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu.

Network name	Category	Type	Created	Last connec
ACORP-W422G	Private Network	IEEE 802.11 (Wireless)	04.06.2008 14:01:56	04.06.2008
ssid_wep	Private Network	IEEE 802.11 (Wireless)	04.06.2008 14:01:46	04.06.2008
Network 1	Public Network	Ethernet	01.06.2008 10:43:11	01.06.2008

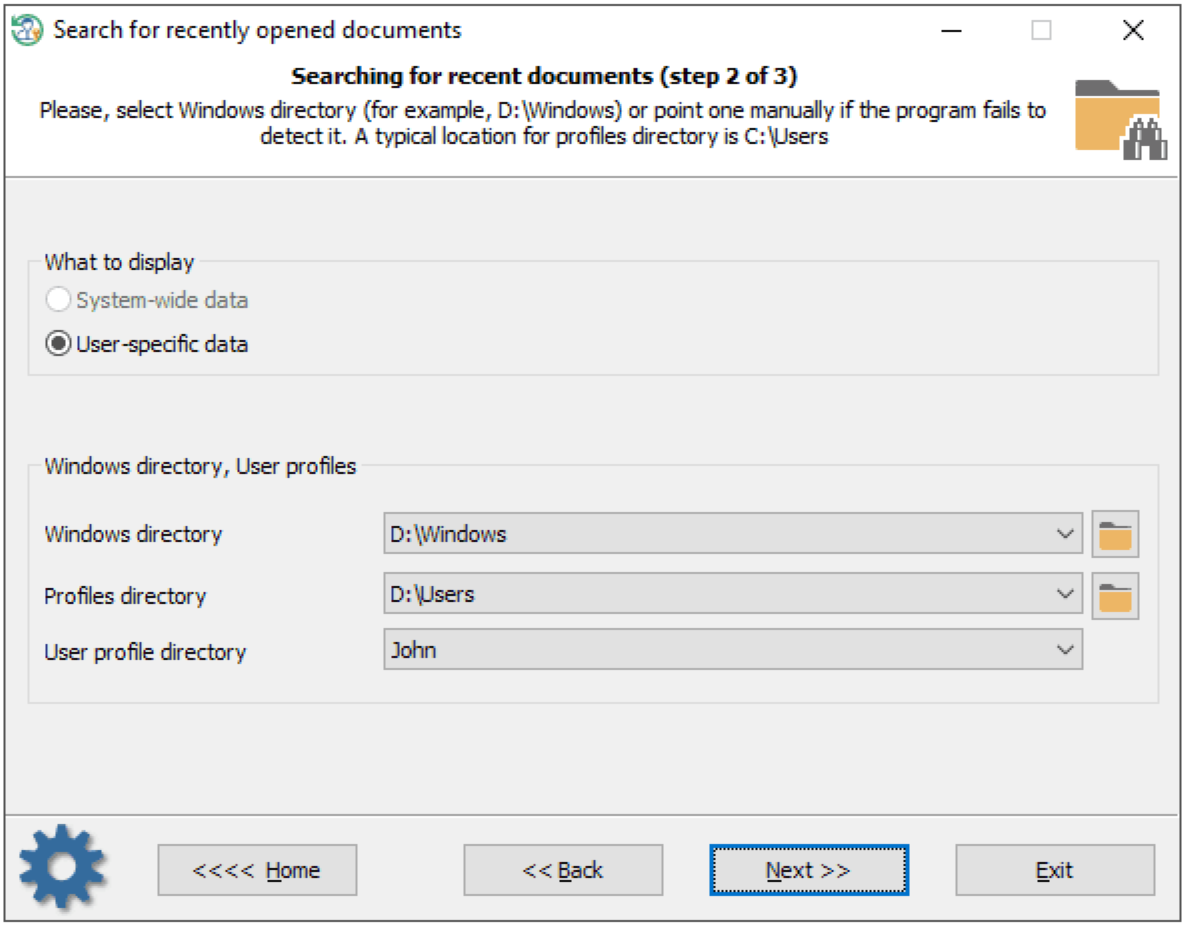
The extracted networks usually contain the date they were created at and the last connection date. To sort the list by dates, click one of the correspondent column.

3.6.6 Search for recently opened documents

Windows OS keeps track of all opened documents and saves links to them to a Microsoft Windows-specific ('Recent') folder in the user profile. 'C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent' is a special folder, where Windows stores the links to recently used documents. You can control the Windows behavior at Start Menu > Settings > Personalization > Start, by toggling the '*Show recently opened items*' option.

This program's feature is aimed to browse through the recent file list and view the names of the files that have been opened recently and saved to the Windows 'Recent' folder.

Selecting user profile



Search for recently opened documents

Searching for recent documents (step 2 of 3)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it. A typical location for profiles directory is C:\Users

What to display

○ System-wide data

● User-specific data

Windows directory, User profiles

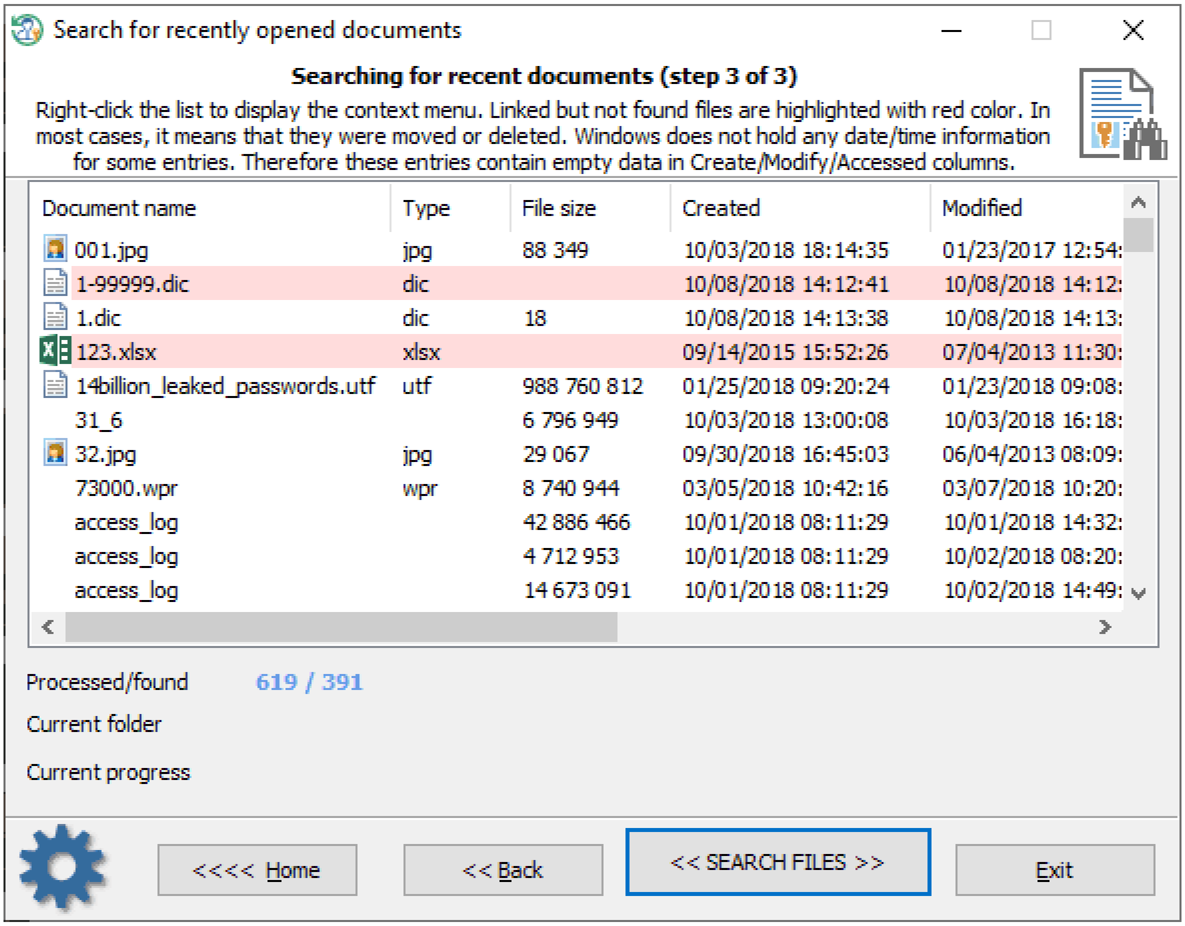
Windows directory: D:\Windows

Profiles directory: D:\Users

User profile directory: John

Select the user profile whose documents you want to analyze.

View recently opened documents



Searching for recent documents (step 3 of 3)

Right-click the list to display the context menu. Linked but not found files are highlighted with red color. In most cases, it means that they were moved or deleted. Windows does not hold any date/time information for some entries. Therefore these entries contain empty data in Create/Modify/Accessed columns.

Document name	Type	File size	Created	Modified
001.jpg	jpg	88 349	10/03/2018 18:14:35	01/23/2017 12:54:
1-99999.dic	dic		10/08/2018 14:12:41	10/08/2018 14:12:
1.dic	dic	18	10/08/2018 14:13:38	10/08/2018 14:13:
123.xlsx	xlsx		09/14/2015 15:52:26	07/04/2013 11:30:
14billion_leaked_passwords.utf	utf	988 760 812	01/25/2018 09:20:24	01/23/2018 09:08:
31_6		6 796 949	10/03/2018 13:00:08	10/03/2018 16:18:
32.jpg	jpg	29 067	09/30/2018 16:45:03	06/04/2013 08:09:
73000.wpr	wpr	8 740 944	03/05/2018 10:42:16	03/07/2018 10:20:
access_log		42 886 466	10/01/2018 08:11:29	10/01/2018 14:32:
access_log		4 712 953	10/01/2018 08:11:29	10/02/2018 08:20:
access_log		14 673 091	10/01/2018 08:11:29	10/02/2018 14:49:

Processed/found 619 / 391

Current folder

Current progress

Click the << *SEARCH FILES* >> button and wait patiently until the program finds the last opened files and fills in the table.

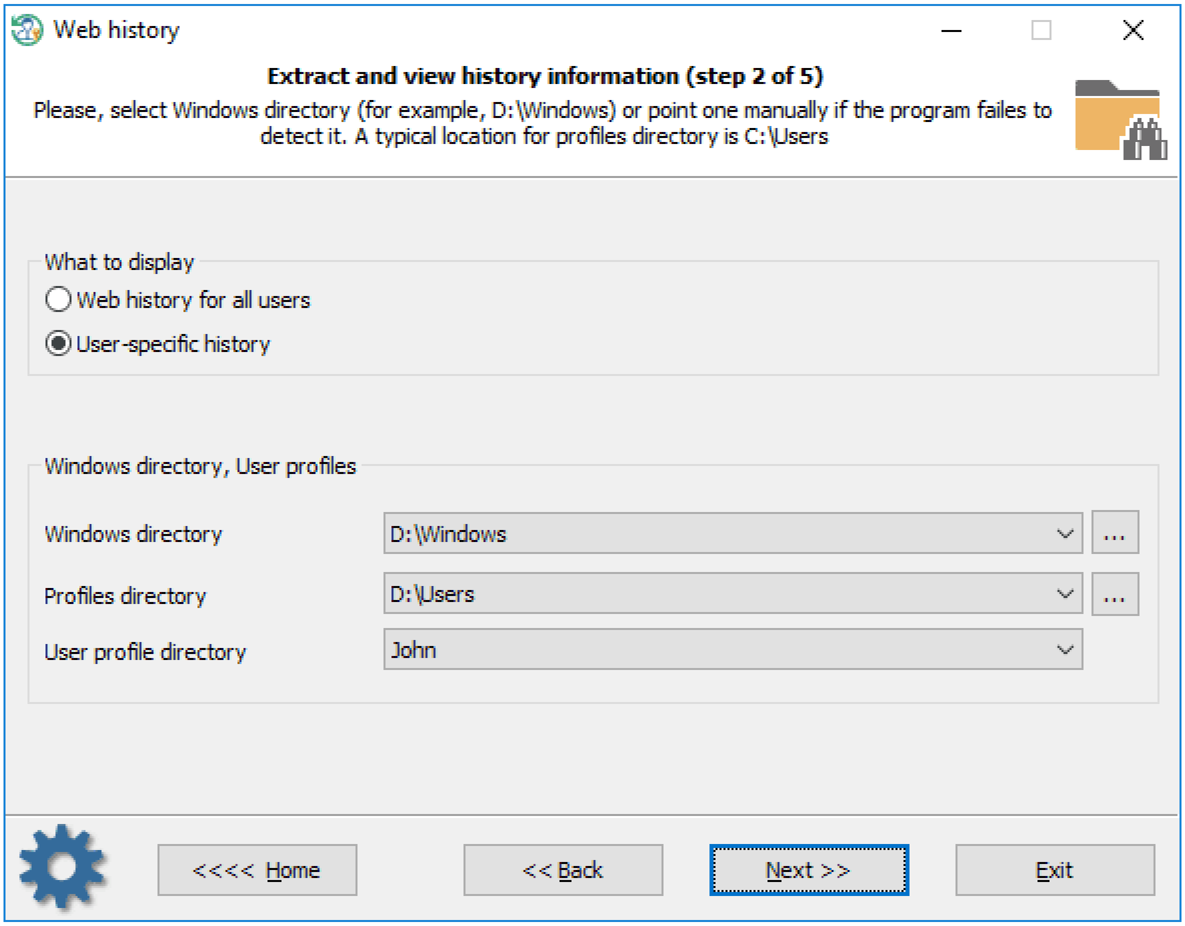
In order to hide the unnecessary items, right-click on the list of found files and select the appropriate menu.

Files that no longer exist (for example, were moved or deleted) but still have links to them are marked with red color.

3.6.7 View web history

The Web history allows you to extract and collect statistics of visited Web pages, saved cookies, stored form autocompletion data and saved passwords. The program supports all popular browsers: Internet Explorer, Edge, Opera, browsers based on Mozilla source code (Firefox, SeaMonkey, etc.), Chromium (Google Chrome, YandexBrowser, 360 Extreme Explorer, etc.)

Selecting data source



Extract and view history information (step 2 of 5)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program failes to detect it. A typical location for profiles directory is C:\Users

What to display

○ Web history for all users

● User-specific history

Windows directory, User profiles

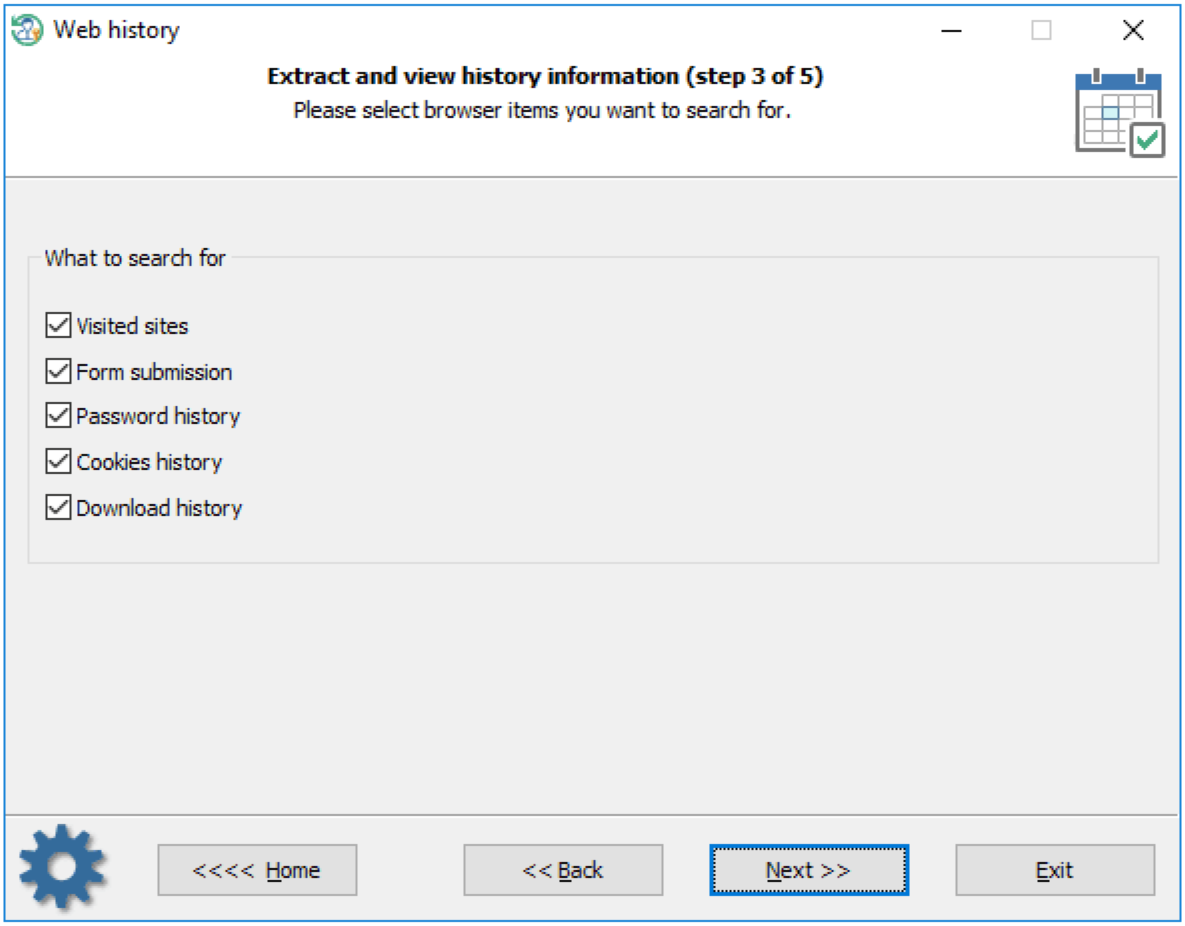
Windows directory: D:\Windows

Profiles directory: D:\Users

User profile directory: John

Initially, RWP offers to select the data source where to search. This is either a specific user's profile or profiles for all users.

What to search for



Extract and view history information (step 3 of 5)
Please select browser items you want to search for.

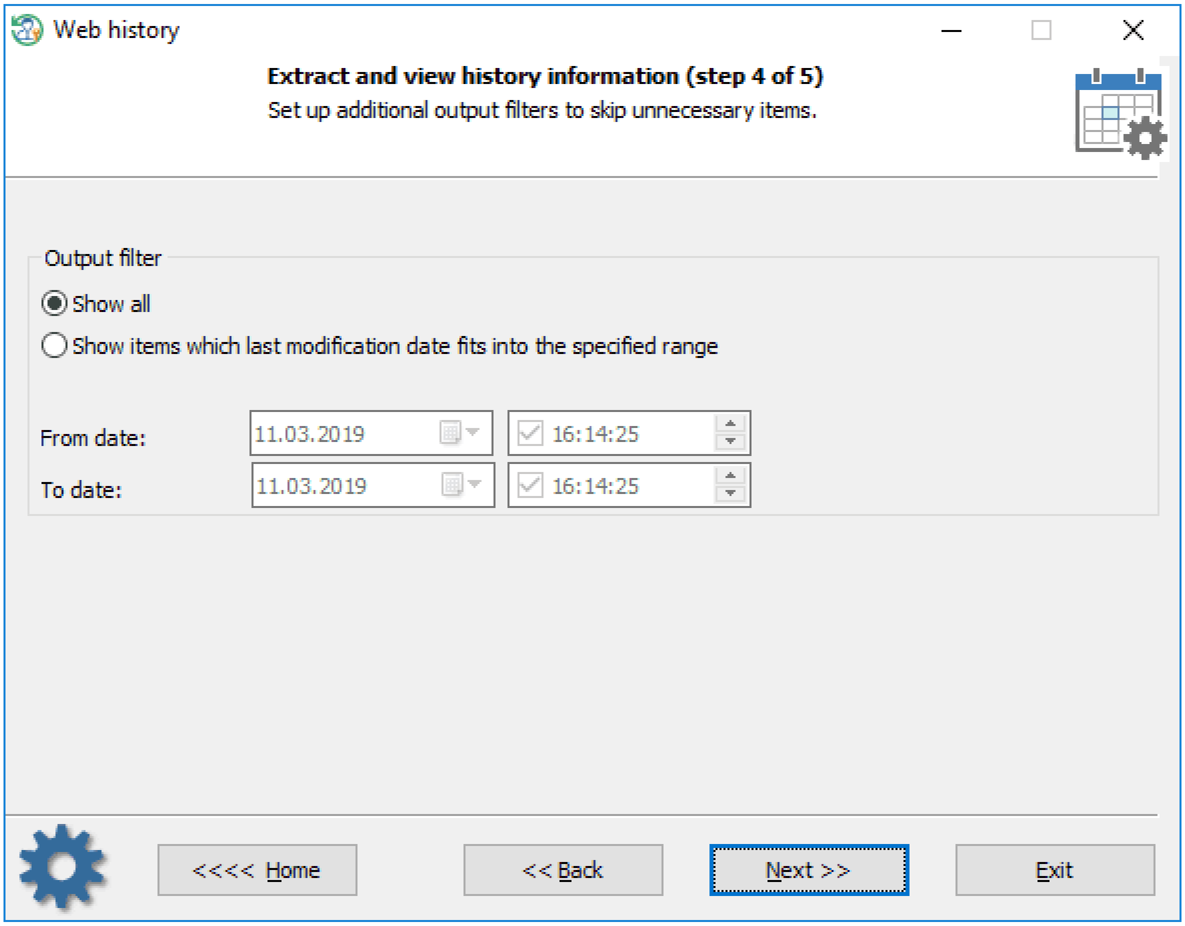
What to search for

☑ Visited sites
☑ Form submission
☑ Password history
☑ Cookies history
☑ Download history

By default, the program tries to search for the following items, you can turn on/off each of them separately:

- The list of visited URLs
- Form auto-completion data
- Logon names and passwords (if ones can be decrypted instantly only)
- Cookies. May be used for determining what sites were visited and when, whether the user was logged in and so on
- Download history. Note that not all browser keep this information

Setting up time filters



Extract and view history information (step 4 of 5)

Set up additional output filters to skip unnecessary items.

Output filter

● Show all

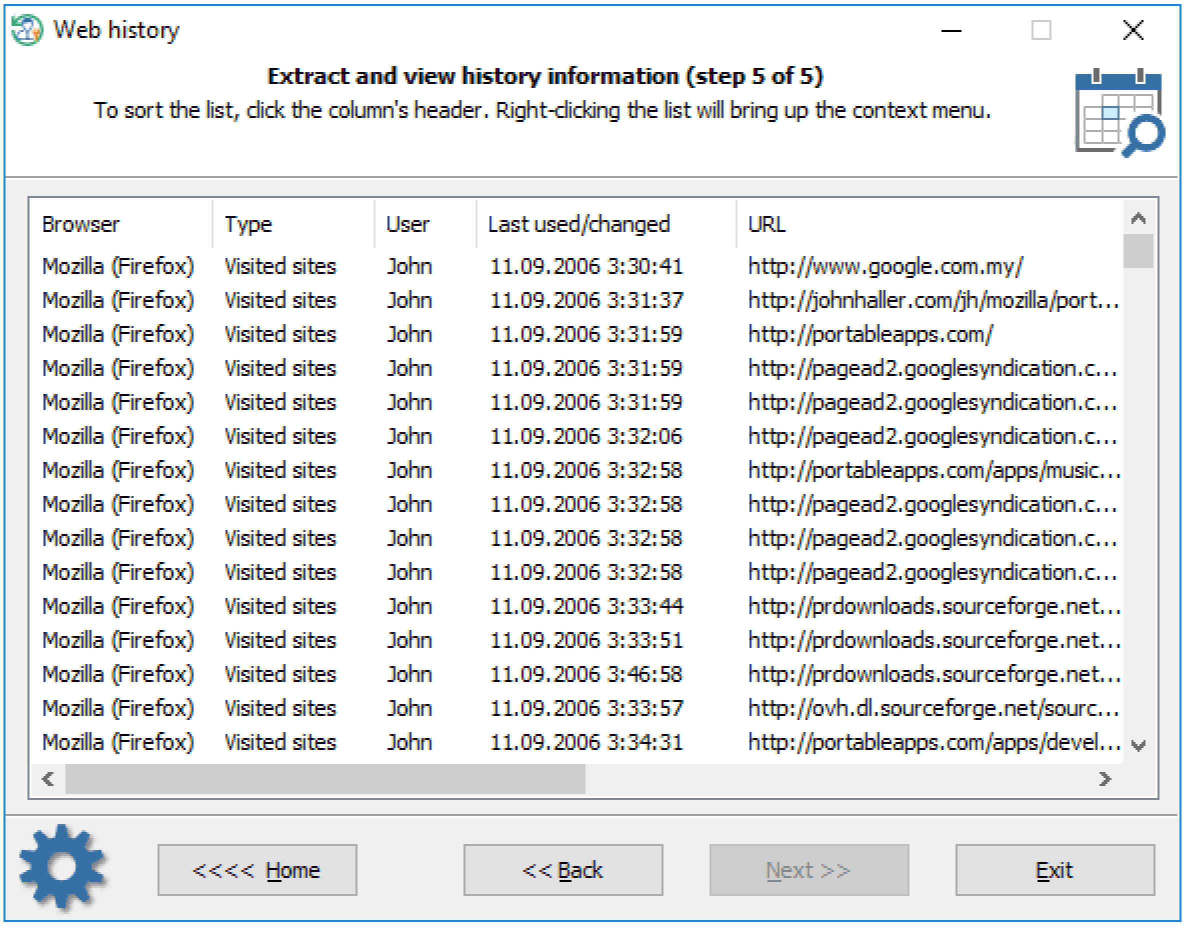
○ Show items which last modification date fits into the specified range

From date: 11.03.2019 ☑ 16:14:25

To date: 11.03.2019 ☑ 16:14:25

You can set up an additional time filter to skip out-dated or unnecessary items.

Web history



Extract and view history information (step 5 of 5)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu.

Browser	Type	User	Last used/changed	URL
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:30:41	http://www.google.com.my/
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:31:37	http://johnhaller.com/jh/mozilla/port...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:31:59	http://portableapps.com/
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:31:59	http://pagead2.googlesyndication.c...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:31:59	http://pagead2.googlesyndication.c...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:32:06	http://pagead2.googlesyndication.c...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:32:58	http://portableapps.com/apps/music...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:32:58	http://pagead2.googlesyndication.c...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:32:58	http://pagead2.googlesyndication.c...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:32:58	http://pagead2.googlesyndication.c...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:33:44	http://prdownloads.sourceforge.net...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:33:51	http://prdownloads.sourceforge.net...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:46:58	http://prdownloads.sourceforge.net...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:33:57	http://ovh.dl.sourceforge.net/sourc...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:34:31	http://portableapps.com/apps/devel...

The statistics can be copied to the clipboard or saved to a file. Using the context menu, you can also hide some items that are not of interest to you.

Where do browsers store their lists of visited URLs?

Internet Explorer
Visited places are stored in index.dat file. The index.dat contains different records: visited URLs and local files, web mail accesses, cookies, etc. The database file has it's own format (Client UrlCache MMF) and was first introduced in Internet Explorer 5. The format of index.dat file was not changed much since that time, the physical location, however, may vary:
C:\Users\<USERNAME>\AppData\Local\Microsoft\History
C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\History
C:\Users\<USERNAME>\AppData\Roaming\Microsoft\Internet Explorer\UserData
Older OSes use different paths to keep the file.

Internet Explorer - typed in URLs
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

Microsoft Edge

Similar to Internet Explorer, Microsoft Edge keeps the history of the Web browsing, cache, cookies, along with other infornation in a single file called WebCacheV01.dat which seems to be is the successor of the index.dat. The WebCacheV01.dat is located at the following path:
C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\WebCache

Opera (older versions)
The browser history is kept in global_history.dat, global.dat, vlink4.dat files in the current Opera's profile. The files have a different format (depends on browser version).

Chrome (along with Chromium-based browsers)
All visited URLs are kept in SQLite database called history. The location of the history is different and depends on the browser. For example:
C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default

Firefox (along with Mozilla-based browsers)
This is either a history.dat file (a mork format) or a places.sqlite file in newer versions. A typical location is C:\Users\<USERNAME>\AppData\Roaming\Mozilla\<PROGRAM>\Profiles. For example:
C:\Users\<USERNAME>\AppData\Roaming\Mozilla\Firefox\Profiles\owec6tnk.default

Where do browsers store the form autocompletion data?

Internet Explorer
Internet Explorer v4-6 keep autocompletion data in a special location of the user registry called protected storage. Even though encrypted, it is easy to decrypt and view because decryption keys are stored along with encrypted data. The registry location of the storage provider:
HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

Internet Explorer v7-9 use a different and interesting technique. Instead of encrypting user-sensitive data with a static secret key (IE 4-6) which can be figured out easily, IE 7-9 use the source URL address as the encryption key to protect the data. Thus without knowing the Web page a certain data belong to, you will not be able to decrypt the data. More details can be found here. RWP does not support extracting IE 7-9 form autocompletion data. Use our PIEPR for that. Here's the registry location where the encrypted data is stored:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage1
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\FormData

Internet Explorer v10+ and Microsoft Edge have even better protection. All data entries are kept in Windows Vault files and protected with DPAPI. There's no chance to decrypt it unless providing the owner logon password and master key file.
A tricky part is that RWP can decrypt the data/passwords instantly if the browser has saved it under the system account. The Vault location for the user data:
C:\Users\<USERNAME>\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28

Opera (older versions)
The form autocompletion data can be found in the following files:
C:\Users\<USERNAME>\AppData\Roaming\Opera\Profile\typed_history.xml
C:\Users\<USERNAME>\AppData\Roaming\Opera\Profile\search_field_history.dat

Chrome (and Chromium-based browsers)
The form submission data is kept in history and Web Data files, both have SQLite format. A typical location for the Chrome browser is:
C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default

Firefox (and Mozilla-based browsers)
This is either a formhistory.dat file (older versions of the browser) or formhistory.sqlite file. A typical location is C:\Users\<USERNAME>\AppData\Roaming\Mozilla\<PROGRAM>\Profiles. Like this:
C:\Users\<USERNAME>\AppData\Roaming\Mozilla\Firefox\Profiles\owec6tnk.default\formhistory.sqlite

Where do browsers store their passwords?

Internet Explorer
Internet Explorer v4-6 keep Web passwords in the protected storage.
HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

Internet Explorer v7-9 passwords are kept in the following registry key:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2

Internet Explorer v10 default location for the saved passwords:
C:\Users\<USERNAME>\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28

Some versions of IE can also save HTTP basic authentication passwords in the 'Credentials store' (Windows Vista and higher OSes). The DPAPI is used to protect the entries there.
C:\Users\<USERNAME>\AppData\Roaming\Microsoft\Credentials

The program is smart enough to extract some extra data stored in other locations. For example, the Reset Windows Password can parse Chrome databases to look for Internet Explorer items that are kept there after data migration.

Opera (older versions)
All passwords are stored in wand.dat file in encrypted form along with decryption keys. The passwords can easily be decrypted unless a Master password is set.
C:\Users\<USERNAME>\AppData\Roaming\Opera\Profile\wand.dat

Chrome (and Chromium-based browsers)
Chromium-based browsers protect user passwords with DPAPI in Windows and store them in Login Data file which actually is an SQLite database. A typical database location for Google Chrome:
C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default\Login data

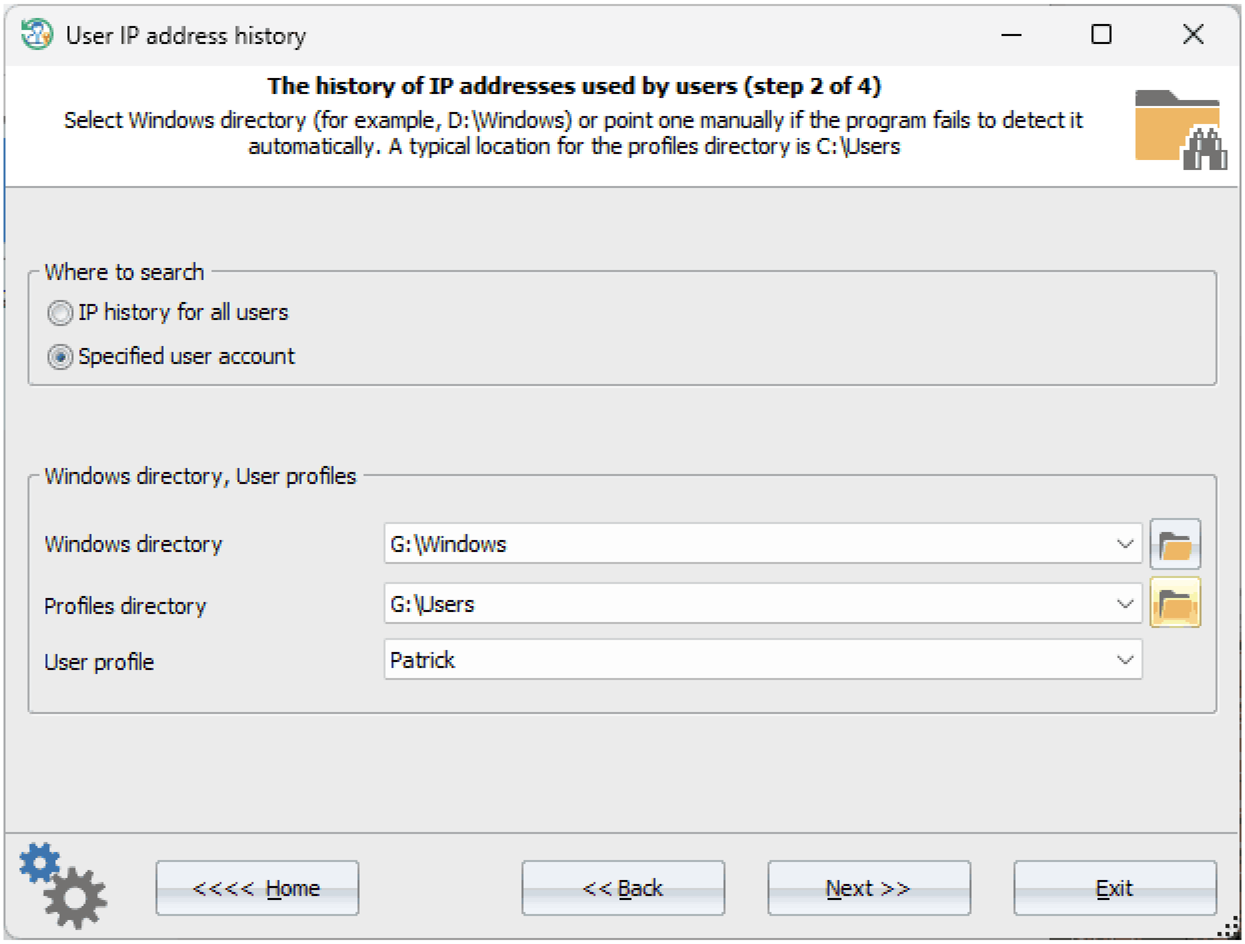
Firefox (and Mozilla-based browsers)
Mozilla had a long way evolving the password storage format. Initially, it was a simple textual file signons.txt. Then in version 2 it came signons2.txt which had the "#2c" prefix at the beginning of the file. Then signons3.txt with the "#2d" prefix in version 3, etc. Next the signons.sqlite database came into a play. But it's not the end of the story. Firefox v32.x and higher has new storage for passwords - logins.json which is actually a JSON format file. In spite of apparent diversity, data protection is almost the same.
A typical location for the files is:
C:\Users\<USERNAME>\AppData\Roaming\Mozilla\<PROGRAM>\Profiles\<PROFILE>.

3.6.8 User IP address history

Introducing a cutting-edge and unparalleled feature (not available in any other program at the time) that empowers you to uncover the history of external IP addresses associated with any user account within the Windows operating system. This groundbreaking capability allows for in-depth analysis of users' network activities, providing insights into the specific IP addresses through which they have accessed the network and the corresponding timestamps.

Contrary to Microsoft's assertion that IP address history is not stored within the system, evidence suggests otherwise. Despite the dispersed nature of this information across the system, it has been revealed that the decryption and retrieval of external IP data for any user account is indeed achievable, shedding light on a previously obscure aspect of system operations.

Choosing user account



User IP address history

The history of IP addresses used by users (step 2 of 4)

Select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it automatically. A typical location for the profiles directory is C:\Users

Where to search

○ IP history for all users

● Specified user account

Windows directory, User profiles

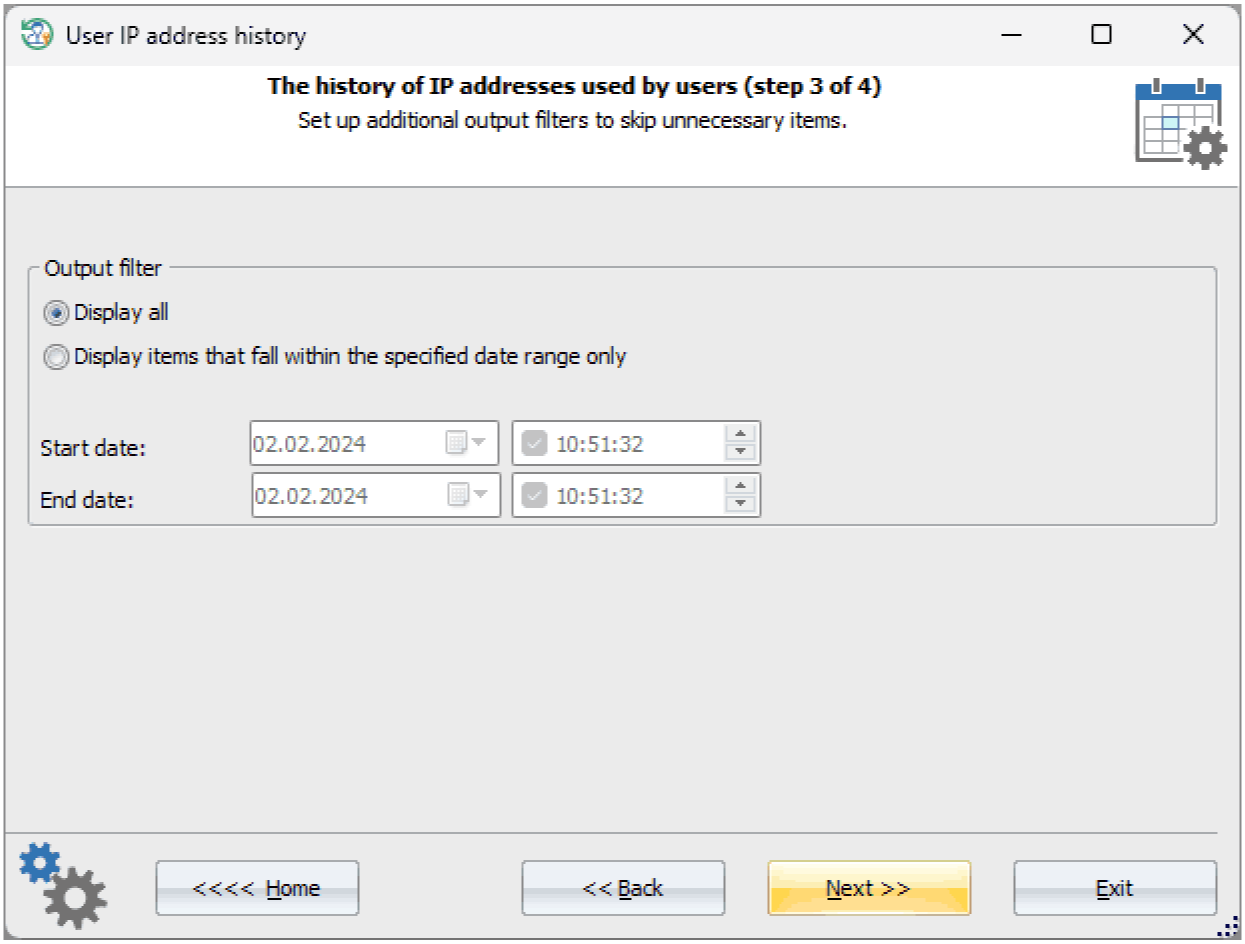
Windows directory: G:\Windows

Profiles directory: G:\Users

User profile: Patrick

Select a user account for which the IP address history needs to be extracted.

Time filters



User IP address history

The history of IP addresses used by users (step 3 of 4)

Set up additional output filters to skip unnecessary items.

Output filter

● Display all

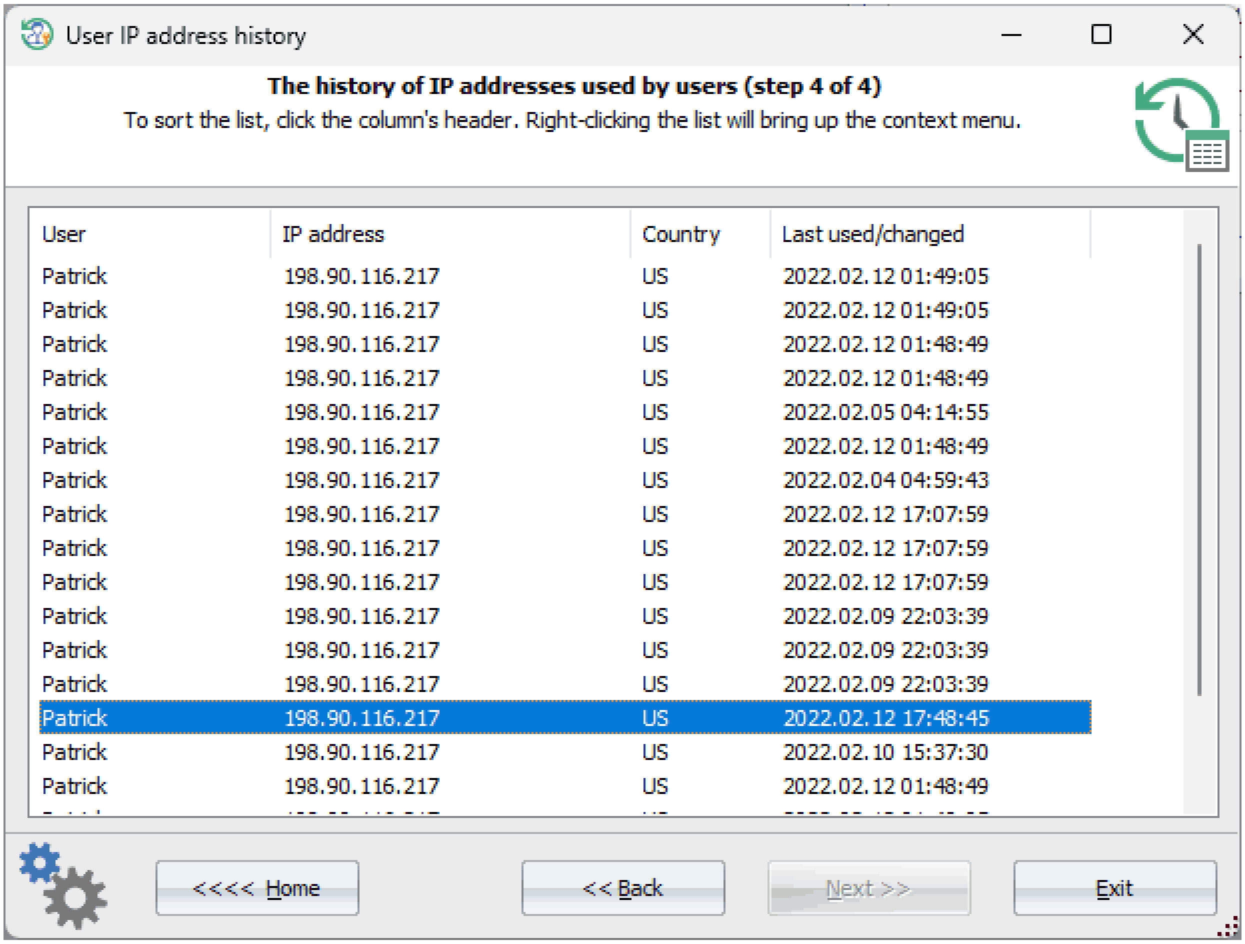
○ Display items that fall within the specified date range only

Start date: 02.02.2024 10:51:32

End date: 02.02.2024 10:51:32

In the next step of the wizard, select the period for which you want to retrieve the information. Or click the '*Display all*' to output all available entries.

User IP address history



The history of IP addresses used by users (step 4 of 4)
To sort the list, click the column's header. Right-clicking the list will bring up the context menu.

User	IP address	Country	Last used/changed
Patrick	198.90.116.217	US	2022.02.12 01:49:05
Patrick	198.90.116.217	US	2022.02.12 01:49:05
Patrick	198.90.116.217	US	2022.02.12 01:48:49
Patrick	198.90.116.217	US	2022.02.12 01:48:49
Patrick	198.90.116.217	US	2022.02.05 04:14:55
Patrick	198.90.116.217	US	2022.02.12 01:48:49
Patrick	198.90.116.217	US	2022.02.04 04:59:43
Patrick	198.90.116.217	US	2022.02.12 17:07:59
Patrick	198.90.116.217	US	2022.02.12 17:07:59
Patrick	198.90.116.217	US	2022.02.12 17:07:59
Patrick	198.90.116.217	US	2022.02.09 22:03:39
Patrick	198.90.116.217	US	2022.02.09 22:03:39
Patrick	198.90.116.217	US	2022.02.09 22:03:39
Patrick	198.90.116.217	US	2022.02.12 17:48:45
Patrick	198.90.116.217	US	2022.02.10 15:37:30
Patrick	198.90.116.217	US	2022.02.12 01:48:49

The program extracts users' IP history from several Windows locations, including those that require further decryption. During this process, you may be prompted for the user's logon password.
The decrypted IP history can be copied to the clipboard or saved as an HTML report.

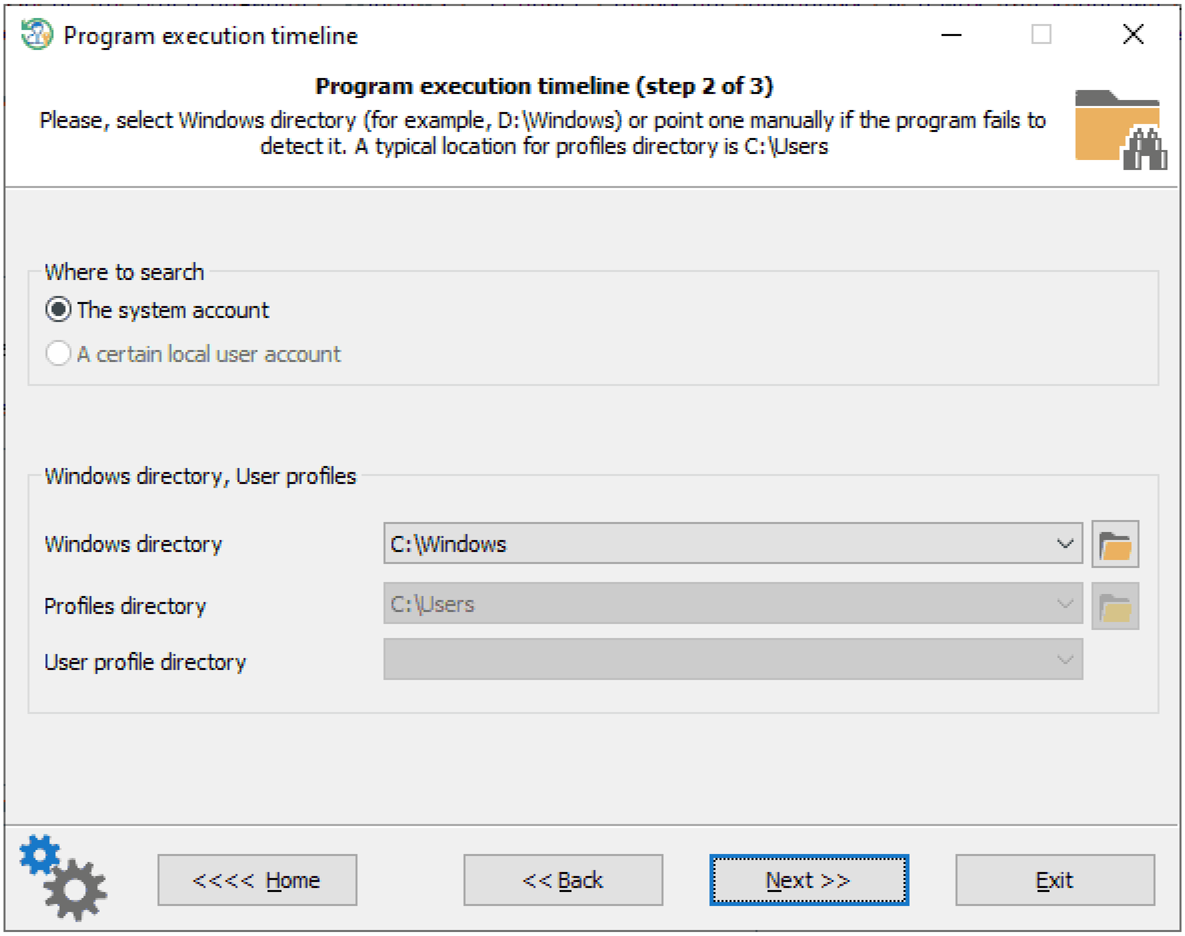
3.7 Forensics

3.7.1 View program execution timeline

It would not be a big surprise to know that there are a lot of artifacts that contain information about recently opened documents or launched files in Windows. The AmCache is one of them which stores data about every program that has been started or installed in the system earlier. The AmCache is available starting with Windows 7. Older operating systems use a BCF format to save data about executed programs. Physically, both formats are simple files located in the %WINDIR%\appcompat\Programs folder. The AmCache.hve is a registry hive that provides a timeline of which program was executed and when, while the RecentFileCache.bcf stands for a simple Binary Cache File.

The program supports both formats, however the old BCF format contains no information about the execution time.

Choosing Windows directory



Program execution timeline

Program execution timeline (step 2 of 3)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it. A typical location for profiles directory is C:\Users

Where to search

● The system account

○ A certain local user account

Windows directory, User profiles

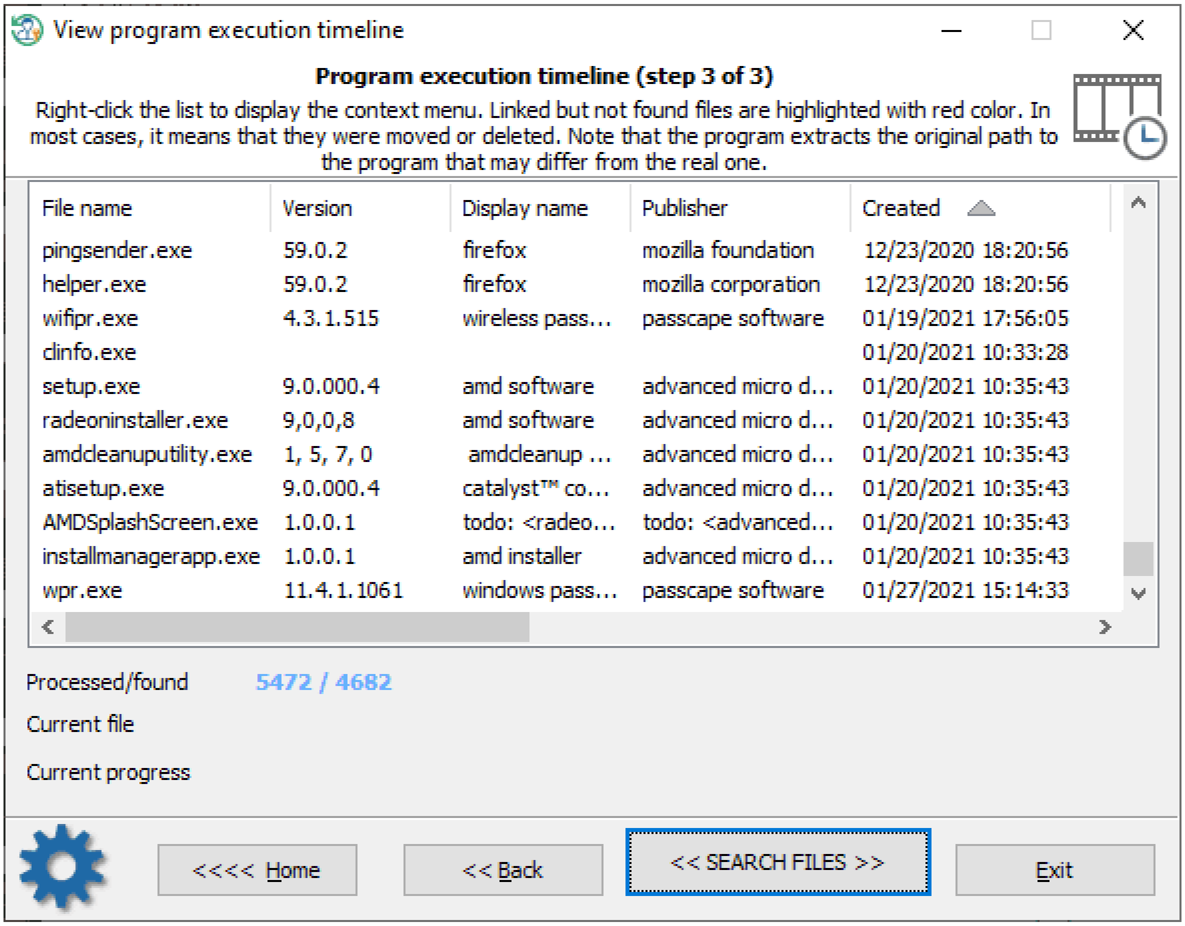
Windows directory: C:\Windows

Profiles directory: C:\Users

User profile directory:

Select the Windows directory detected by the program.

View program execution timeline



View program execution timeline

Program execution timeline (step 3 of 3)

Right-click the list to display the context menu. Linked but not found files are highlighted with red color. In most cases, it means that they were moved or deleted. Note that the program extracts the original path to the program that may differ from the real one.

File name	Version	Display name	Publisher	Created
pingsender.exe	59.0.2	firefox	mozilla foundation	12/23/2020 18:20:56
helper.exe	59.0.2	firefox	mozilla corporation	12/23/2020 18:20:56
wifipr.exe	4.3.1.515	wireless pass...	passcape software	01/19/2021 17:56:05
clinfo.exe				01/20/2021 10:33:28
setup.exe	9.0.000.4	amd software	advanced micro d...	01/20/2021 10:35:43
radeoninstaller.exe	9,0,0,8	amd software	advanced micro d...	01/20/2021 10:35:43
amdcleanuputility.exe	1, 5, 7, 0	amdcleanup ...	advanced micro d...	01/20/2021 10:35:43
atisetup.exe	9.0.000.4	catalyst™ co...	advanced micro d...	01/20/2021 10:35:43
AMDSplashScreen.exe	1.0.0.1	todo: <radeo...	todo: <advanced...	01/20/2021 10:35:43
installmanagerapp.exe	1.0.0.1	amd installer	advanced micro d...	01/20/2021 10:35:43
wpr.exe	11.4.1.1061	windows pass...	passcape software	01/27/2021 15:14:33

Processed/found 5472 / 4682

Current file

Current progress

Now it's time to hit the << *SEARCH FILES* >> button and wait for the program to locate the files to fill in the table.

In order to wipe out any unnecessary file from the list of found items, right-click the list and select the appropriate menu.

If the program fails to locate files Windows links to from within the AmCache database, it marks the files with red color.

3.7.2 Windows activity timeline

Timeline is a comparatively new function of Windows 10 that is first introduced with version 1803. It shows your past activities and things you were working on earlier. Such as the applications you opened, the files you used, the websites you browsed, etc. In Windows 10, you can manage your timeline activity history in Start -> Settings -> Privacy -> Activity history. If you want to stop Windows collecting your activity, just clear the check-box next to the *'Show my activity history on this device'*.

The **<USER_PROFILE>\AppData\Local\ConnectedDevicesPlatform** directory is a home for multiple **CPDS** files. A **CPDS** file most likely stands for **C**onnected **P**latform **D**evice **S**ettings. This is a JSON-format file containing settings for managing the Timeline profile. Apart from the general settings, the above directory holds up to three .cpds files corresponding to the local account, domain, or Microsoft account of the user profile.

Windows 10 Timeline stores user activity in 'ActivitiesCache.db' file, which, in fact, is an SQLite database. You can find the database at the following location:

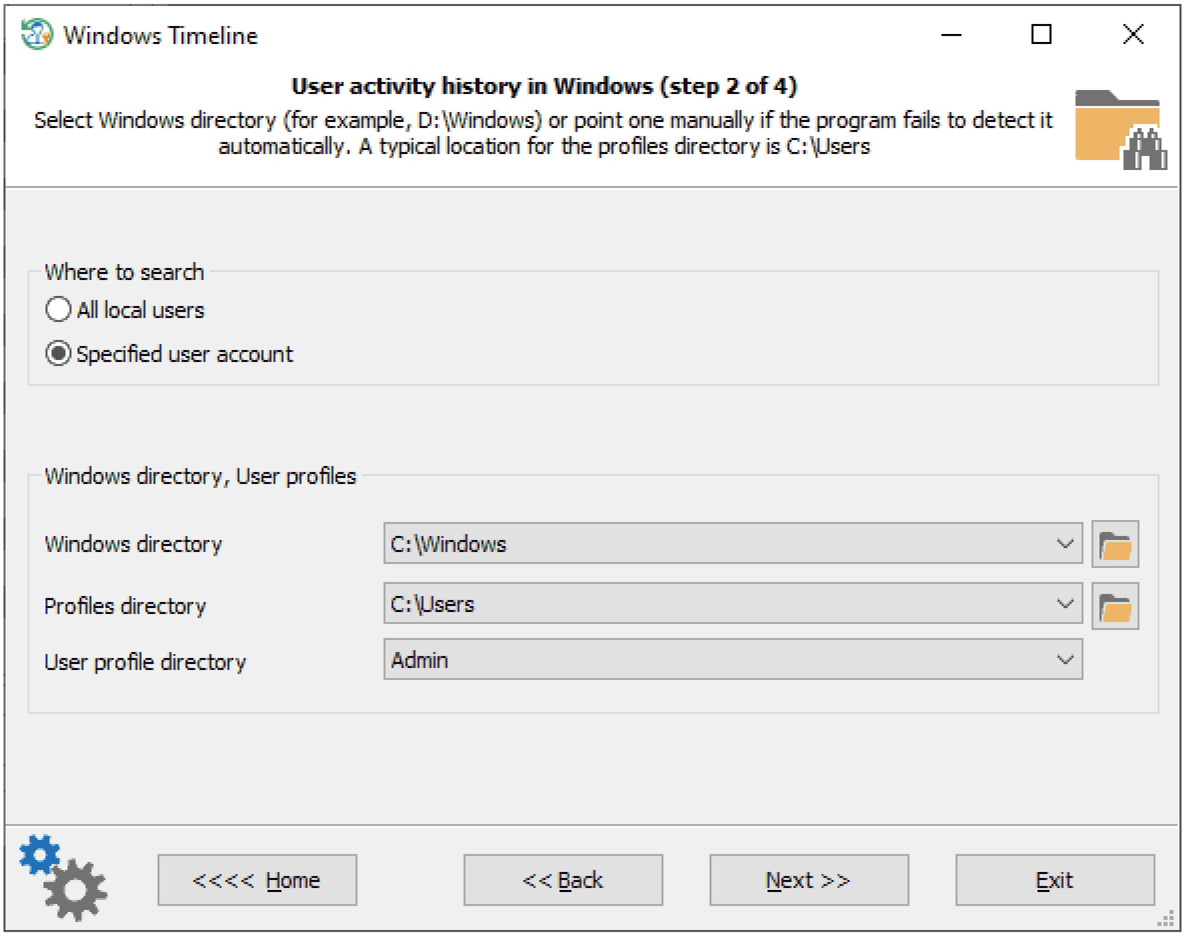
<USER_PROFILE>\AppData\Local\ConnectedDevicesPlatform\<PROFILE_NAME>\ActivitiesCache.db

Almost all information related to the user activity incorporated into two tables: **Activity_PackageId** and **Activity**. By default, the data records live for 30 days until they are marked as deleted.

Reset Windows Password allows you to display the user activity data stored by the Windows timeline for any user in a human-readable form. It also extracts some additional information, such as what program a certain user was working on and how long, the documents he/she was opening from within the application, active and total usage time, active device, etc.

It is much easier to use the Windows activity timeline feature rather than analyzing the data manually. The 3-step workflow process guides you to select the initial user account, set up additional time filters and display the user activity timeline. Simple as 1-2-3.

Selecting Windows timeline account



Windows Timeline

User activity history in Windows (step 2 of 4)

Select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it automatically. A typical location for the profiles directory is C:\Users

Where to search

○ All local users

● Specified user account

Windows directory, User profiles

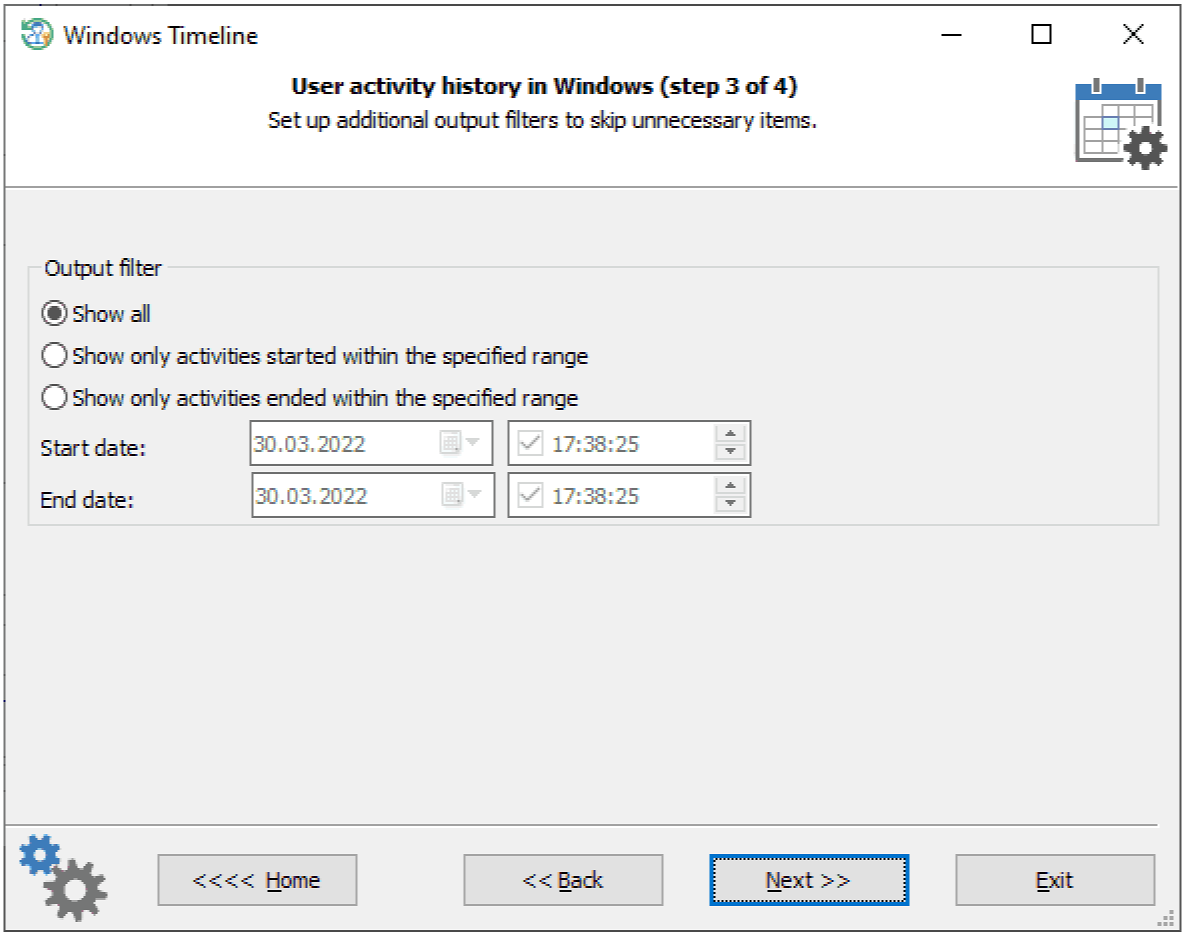
Windows directory: C:\Windows

Profiles directory: C:\Users

User profile directory: Admin

Select the user on which activity history you need to view. By default, all users.

Setting activity timeline display filters



Windows Timeline

User activity history in Windows (step 3 of 4)

Set up additional output filters to skip unnecessary items.

Output filter

● Show all

○ Show only activities started within the specified range

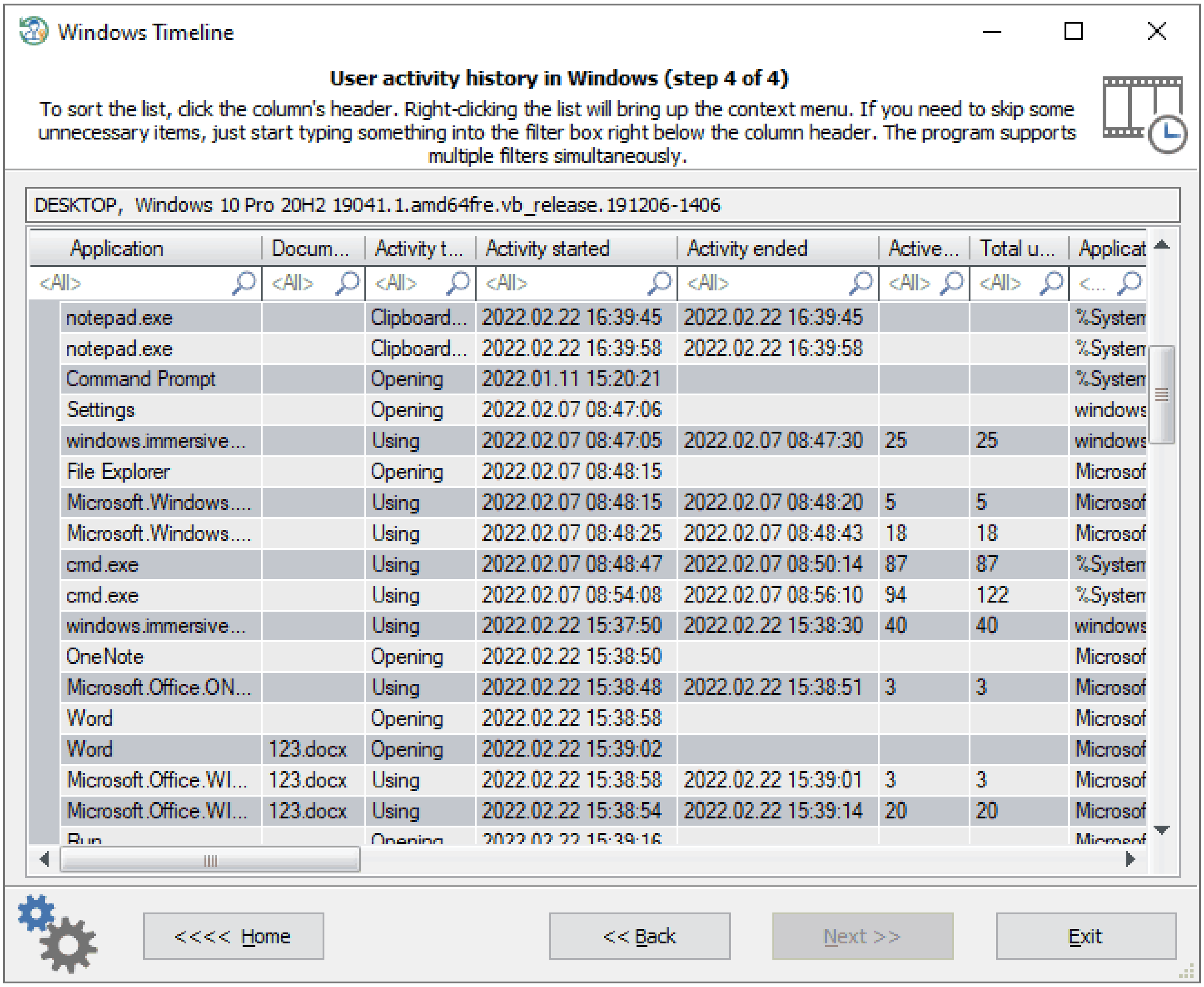
○ Show only activities ended within the specified range

Start date: 30.03.2022 ☑ 17:38:25

End date: 30.03.2022 ☑ 17:38:25

You can set up additional time filters to skip showing unnecessary activities.

Windows activity timeline



User activity history in Windows (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

DESKTOP, Windows 10 Pro 20H2 19041.1.amd64fre.vb_release.191206-1406

Application	Docum...	Activity t...	Activity started	Activity ended	Active...	Total u...	Applicat
<All>	<All>	<All>	<All>	<All>	<All>	<All>	<...
notepad.exe		Clipboard...	2022.02.22 16:39:45	2022.02.22 16:39:45			%Systen
notepad.exe		Clipboard...	2022.02.22 16:39:58	2022.02.22 16:39:58			%Systen
Command Prompt		Opening	2022.01.11 15:20:21				%Systen
Settings		Opening	2022.02.07 08:47:06				windows
windows.immersive...		Using	2022.02.07 08:47:05	2022.02.07 08:47:30	25	25	windows
File Explorer		Opening	2022.02.07 08:48:15				Microsof
Microsoft.Windows....		Using	2022.02.07 08:48:15	2022.02.07 08:48:20	5	5	Microsof
Microsoft.Windows....		Using	2022.02.07 08:48:25	2022.02.07 08:48:43	18	18	Microsof
cmd.exe		Using	2022.02.07 08:48:47	2022.02.07 08:50:14	87	87	%Systen
cmd.exe		Using	2022.02.07 08:54:08	2022.02.07 08:56:10	94	122	%Systen
windows.immersive...		Using	2022.02.22 15:37:50	2022.02.22 15:38:30	40	40	windows
OneNote		Opening	2022.02.22 15:38:50				Microsof
Microsoft.Office.ON...		Using	2022.02.22 15:38:48	2022.02.22 15:38:51	3	3	Microsof
Word		Opening	2022.02.22 15:38:58				Microsof
Word	123.docx	Opening	2022.02.22 15:39:02				Microsof
Microsoft.Office.WI...	123.docx	Using	2022.02.22 15:38:58	2022.02.22 15:39:01	3	3	Microsof
Microsoft.Office.WI...	123.docx	Using	2022.02.22 15:38:54	2022.02.22 15:39:14	20	20	Microsof
Run		Opening	2022.02.22 15:39:16				Microsof

The Excel-like table allows displaying the data most conveniently. You can sort the table by clicking a column header. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

Here is a brief description of what information every table's column holds.

Application - a short text description of the application used to generate the user activity
Document name - a file that was opening/editing within the application
Activity type - a type of operation. For example: sending a notification, authentication, opening application/file/URL, using application/file/URL, clipboard copy/paste, system operation.
Activity started - initial time the activity began
Activity ended - when the activity finished
Active usage - how much time (in seconds) the application was focused and used intensively
Total usage - how much time (in seconds) the application used in total
Application path - full path to the application
Document location - full path to the document (that was opening/editing in application)
Parent application - parent application for current user activity. For example, for a clipboard paste operation, this is an application where the data was copied from.

Source host - URL address representing the cross-platform identity mapping for the application
Clipboard content - content of the Windows clipboard buffer. Only if the **Activity type** is **Clipboard content**.
User - the name of the user. Note that one user profile may hold 3 **Account types**. Thus, this column may contain up to 3 different names for a single user profile.
Account type - the type of the user: local, domain or Microsoft account
User status - shows if the user is engaged with the application
User timezone - the time zone in which the device used to generate the activity was located at activity start time
Device - a name of the device (including its model, type and manufacture) used to generate the user activity
Status - a status code used to identify the activity object: active, updated, deleted or ignored

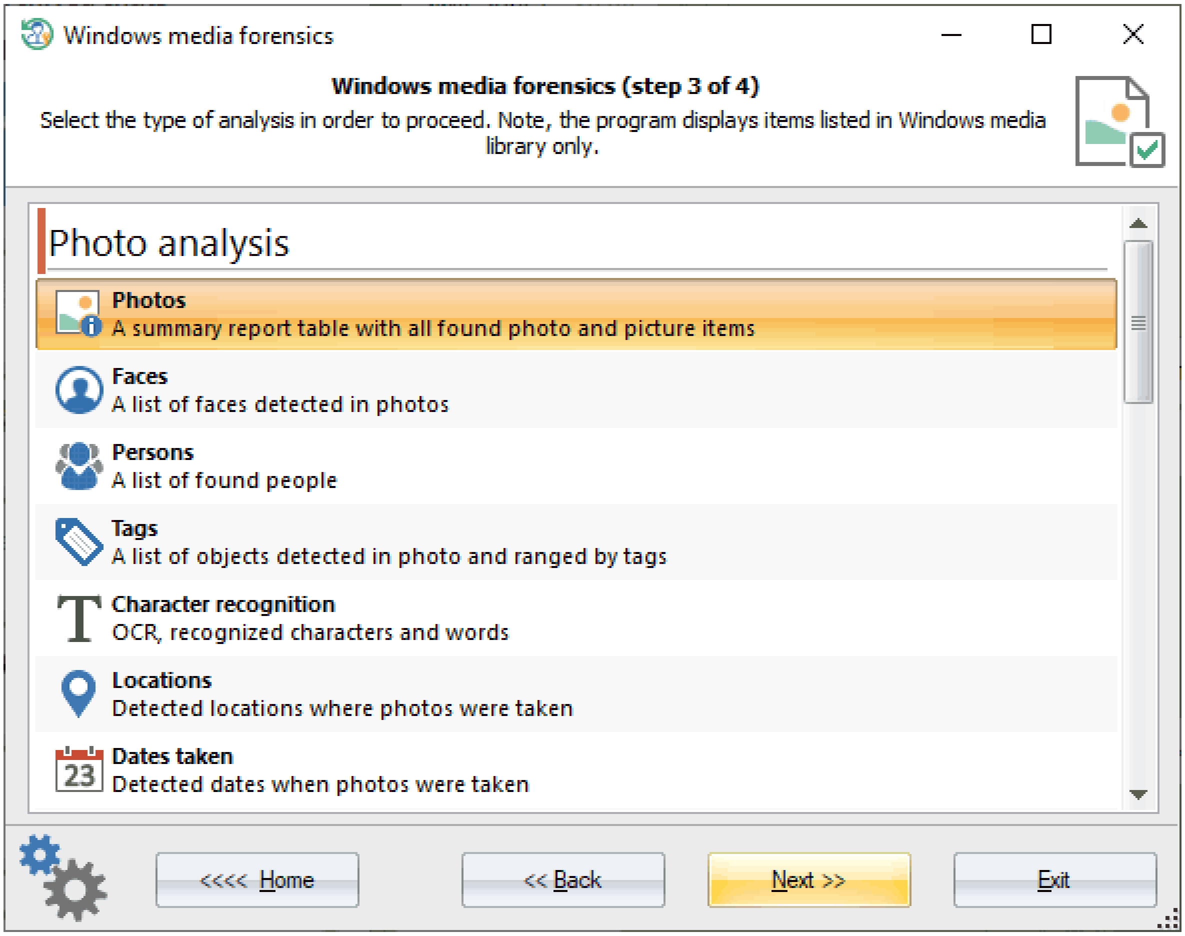
3.7.3 Windows Media forensics

The **Windows Media Forensics** tool analyzes and displays in a human-readable format Windows photo and video artifacts stored by the Windows Photos application. The Windows Photo library provides a heap of information that could be handy for investigators in digital forensic analysis.

The Windows Photos is available in Windows 10 and later OSes and located at:
C:\Users\%username%
\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\LocalState\MediaDb.v1.sqlite

Additional Photo, Video and Media databases can be found at the following locations:
C:\Users\%username%\AppData\Local\Packages\Microsoft.ZuneVideo_8wekyb3d8bbwe
C:\Users\%username%\AppData\Local\Packages\Microsoft.ZuneMusic_8wekyb3d8bbwe

You can use the program's Backup feature to save the data for future analysis.



Windows media forensics

Windows media forensics (step 3 of 4)

Select the type of analysis in order to proceed. Note, the program displays items listed in Windows media library only.

Photo analysis

Photos
A summary report table with all found photo and picture items

Faces
A list of faces detected in photos

Persons
A list of found people

Tags
A list of objects detected in photo and ranged by tags

Character recognition
OCR, recognized characters and words

Locations
Detected locations where photos were taken

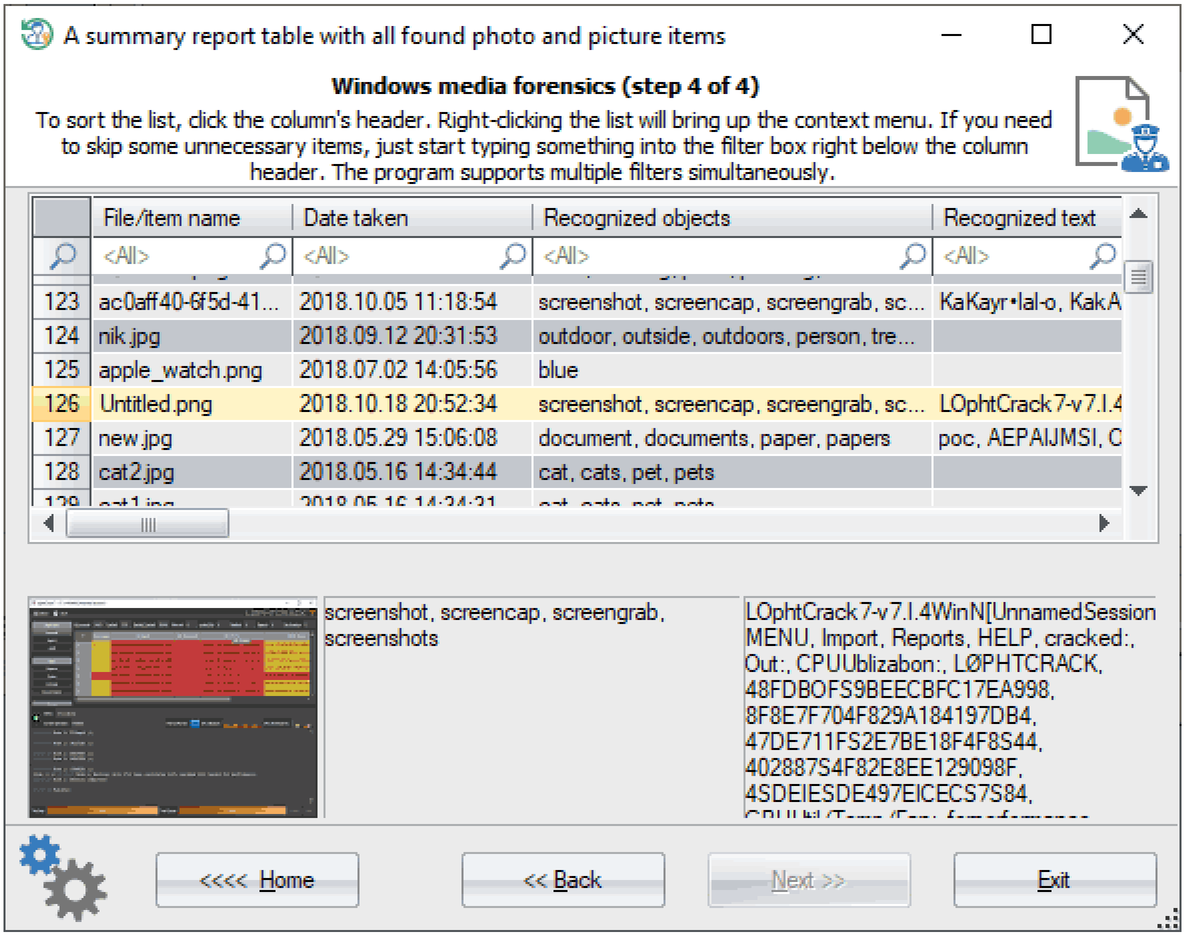
Dates taken
Detected dates when photos were taken

The **Windows Media Forensics** tool consists of several parts:

- Image library
- Video library
- User actions
- Photo library (**Photos** related information)
- Photo library action
- Media player library (**Media Player** related info)
- Media player library actions

3.7.3.1 Image analysis

3.7.3.1.1 Images



A summary report table with all found photo and picture items

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	File/item name	Date taken	Recognized objects	Recognized text
	<All>	<All>	<All>	<All>
123	ac0aff40-6f5d-41...	2018.10.05 11:18:54	screenshot, screencap, screengrab, sc...	KaKayr•lal-o, KakA
124	nik.jpg	2018.09.12 20:31:53	outdoor, outside, outdoors, person, tre...	
125	apple_watch.png	2018.07.02 14:05:56	blue	
126	Untitled.png	2018.10.18 20:52:34	screenshot, screencap, screengrab, sc...	LOphtCrack7-v7.I.4
127	new.jpg	2018.05.29 15:06:08	document, documents, paper, papers	poc, AEPAIJMSI, C
128	cat2.jpg	2018.05.16 14:34:44	cat, cats, pet, pets	
129	cat1.jpg	2018.05.16 14:34:31	cat, cats, pet, pets	

screenshot, screencap, screengrab, screenshots

LOphtCrack7-v7.I.4WinN[UnnamedSession MENU, Import, Reports, HELP, cracked:, Out:, CPUUblizabon:, LØPHTCRACK, 48FDBOFS9BEECBFC17EA998, 8F8E7F704F829A184197DB4, 47DE711FS2E7BE18F4F8S44, 402887S4F82E8EE129098F, 4SDEIESDE497EICECS7S84,

This report contains a general information on photo and picture items. Namely:

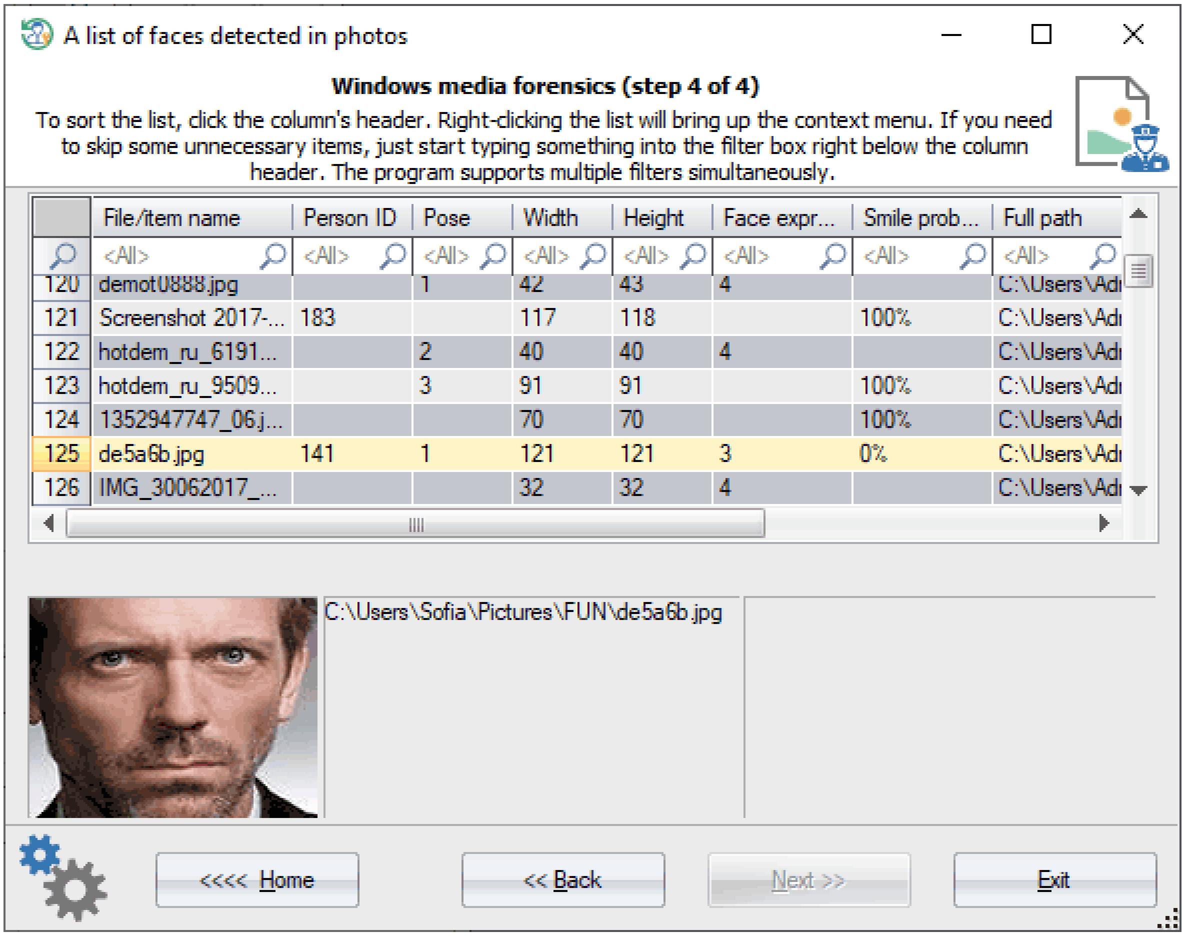
- The name of the file
- Date taken
- Recognized objects (ranged by pre-defined tags)
- Text recognized by the OCR engine. Note that international characters are not recognized properly if the source OS has no corresponding language installed.
- The number of detected faces
- File size
- Image width
- Image height
- Location country
- Location region
- Latitude
- Longitude
- Image caption
- Full path to the file
- Image author
- Image copyright
- Path to the duplicate, if found
- Image quality score
- Camera manufacturer

- Camera model
- Camera F-number
- Camera focal length
- Camera ISO speed
- Camera exposure time
- Application used for image editing
- Last created/modified/edited
- Last time the image viewed in the library
- Album name the image belongs to

The report table contains filter boxes located right below column headers. These filters can be used to sort out unnecessary items or to search for certain images fast. For example, if you need to check if there are any screenshots with credit cards, just type in 'visa' into the 'Recognized text' filter to find all image files that contain the word 'visa'.

You can use the context menu to copy certain data or the entire text into the clipboard, to save the report or to create a zip archive with selected items.

3.7.3.1.2 Faces



A list of faces detected in photos

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	File/item name	Person ID	Pose	Width	Height	Face expr...	Smile prob...	Full path
	<All>	<All>	<All>	<All>	<All>	<All>	<All>	<All>
120	demot0888.jpg		1	42	43	4		C:\Users\Adı
121	Screenshot 2017-...	183		117	118		100%	C:\Users\Adı
122	hotdem_ru_6191...		2	40	40	4		C:\Users\Adı
123	hotdem_ru_9509...		3	91	91		100%	C:\Users\Adı
124	1352947747_06j...			70	70		100%	C:\Users\Adı
125	de5a6b.jpg	141	1	121	121	3	0%	C:\Users\Adı
126	IMG_30062017_...			32	32	4		C:\Users\Adı

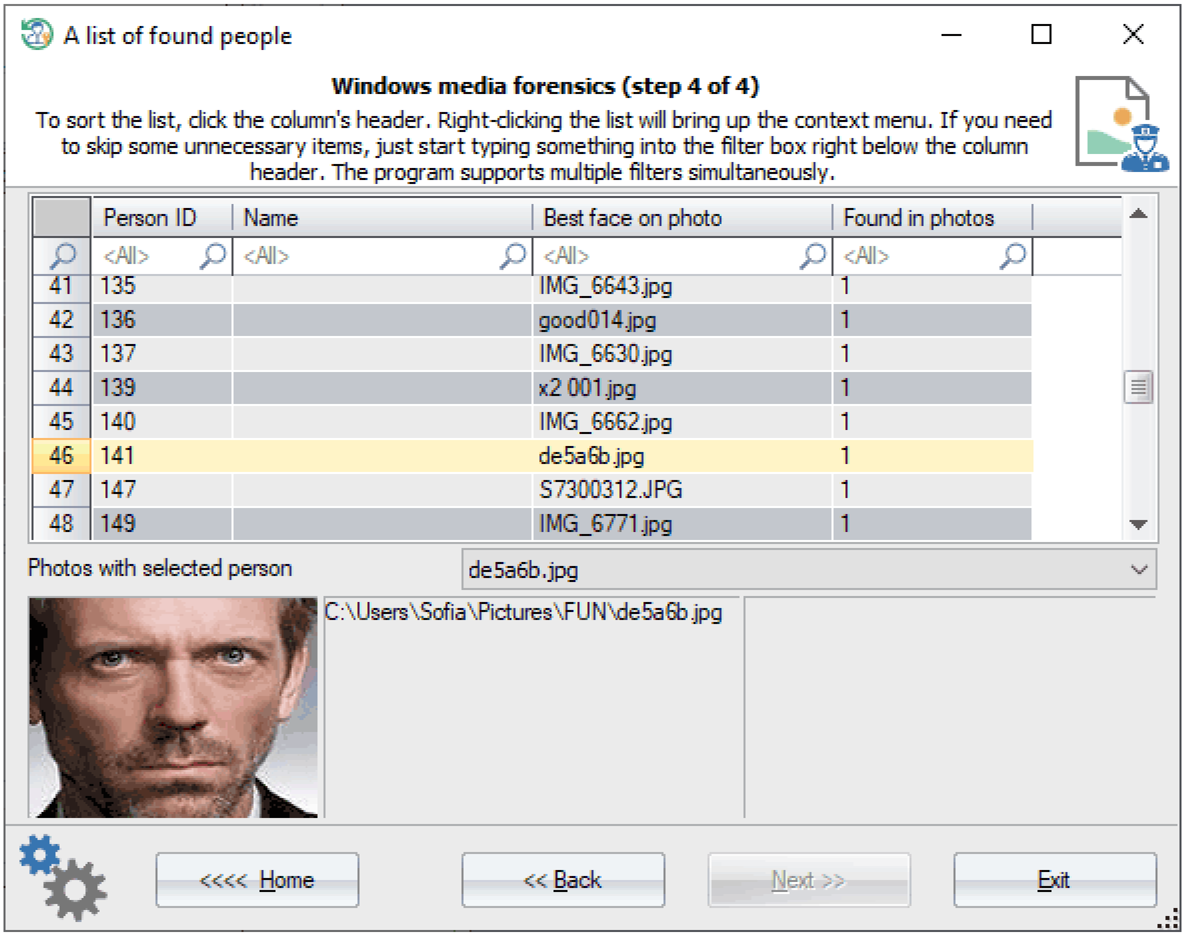
C:\Users\Sofia\Pictures\FUN\de5a6b.jpg

The **Faces** report provides a list of found faces and their properties:

- The name of the image file where the face was found
- Person identity
- Face position
- Face width
- Face height
- Face expression
- Smile probability
- Full path to the file

To find other faces related to this person, use the Persons report instead.

3.7.3.1.3 Persons



Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Person ID	Name	Best face on photo	Found in photos
	<All>	<All>	<All>	<All>
41	135		IMG_6643.jpg	1
42	136		good014.jpg	1
43	137		IMG_6630.jpg	1
44	139		x2 001.jpg	1
45	140		IMG_6662.jpg	1
46	141		de5a6b.jpg	1
47	147		S7300312.JPG	1
48	149		IMG_6771.jpg	1

Photos with selected person: de5a6b.jpg

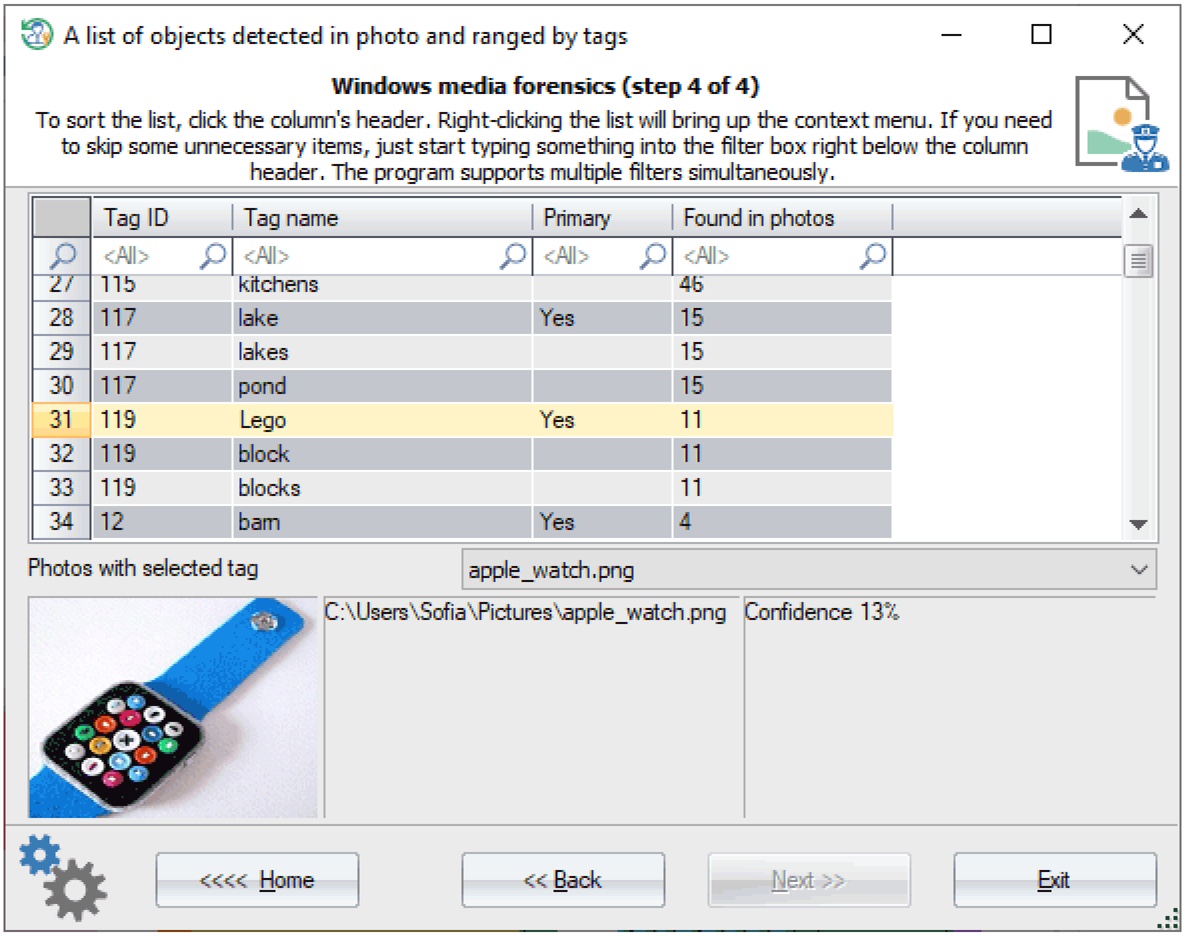
C:\Users\Sofia\Pictures\FUN\de5a6b.jpg

The **Persons** report displays people grouped by the person identity. A person contains:

- Person ID
- Name (displayed only if the user has set it explicitly)
- Image file that contains the most quality photo
- Found in photos

To view more photos with that person, click the person's ID, then select the image file from the drop-down box below the table.

3.7.3.1.4 Tags



A list of objects detected in photo and ranged by tags

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Tag ID	Tag name	Primary	Found in photos
	<All>	<All>	<All>	<All>
27	115	kitchens		46
28	117	lake	Yes	15
29	117	lakes		15
30	117	pond		15
31	119	Lego	Yes	11
32	119	block		11
33	119	blocks		11
34	12	barn	Yes	4

Photos with selected tag: apple_watch.png

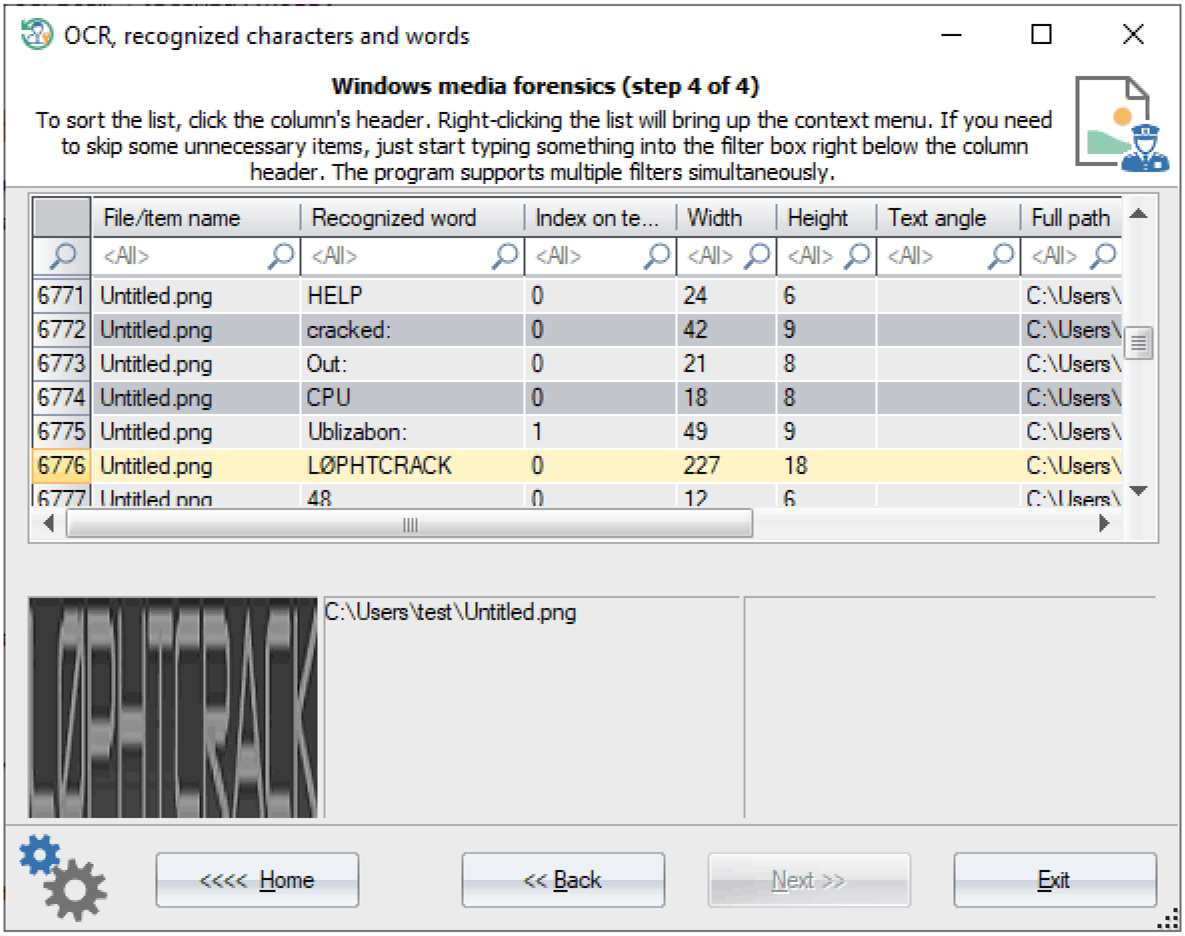
C:\Users\Sofia\Pictures\apple_watch.png

Confidence 13%

The **Tags** table displays a list of objects and photos related to the objects. Every tag has the following properties:

- Tags ID
- Short name of the tag
- Primary or not
- Found in photos

3.7.3.1.5 Character recognition


OCR, recognized characters and words

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	File/item name	Recognized word	Index on te...	Width	Height	Text angle	Full path
	<All>	<All>	<All>	<All>	<All>	<All>	<All>
6771	Untitled.png	HELP	0	24	6		C:\Users\
6772	Untitled.png	cracked:	0	42	9		C:\Users\
6773	Untitled.png	Out:	0	21	8		C:\Users\
6774	Untitled.png	CPU	0	18	8		C:\Users\
6775	Untitled.png	Ublizabon:	1	49	9		C:\Users\
6776	Untitled.png	LØPHTCRACK	0	227	18		C:\Users\
6777	Untitled.png	48	0	12	6		C:\Users\

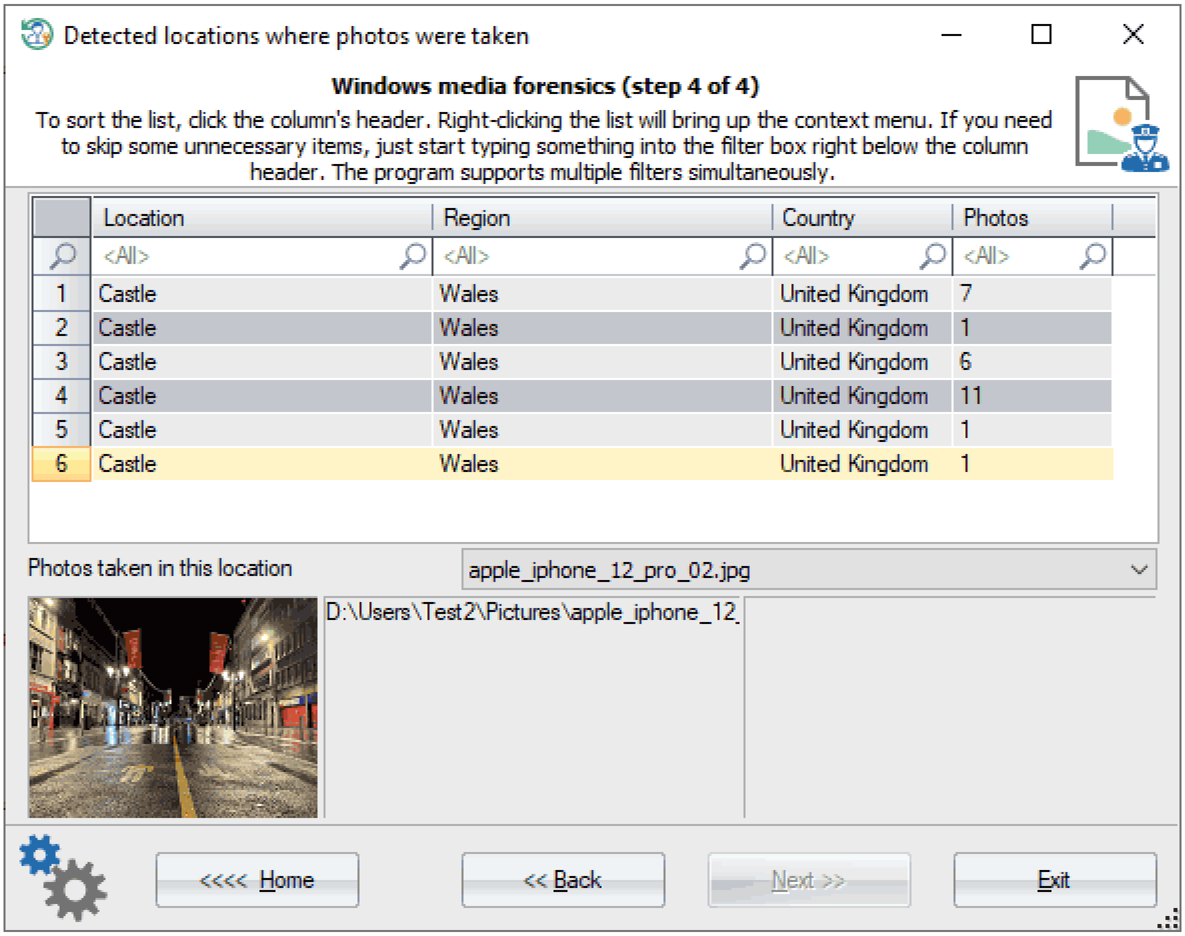
C:\Users\test\Untitled.png

The Windows Photo has a simple optical character recognition engine. You can use the **OCR** feature to view text and its properties found in photos:

- File name of the image file
- Recognized word
- Word index on a text line
- Width of the word (in pixels)
- Word height
- Text angle
- Full path to the image file

A funny thing is that apart from the obvious usage, this feature can be used to identify some kinds of watermarks in images.

3.7.3.1.6 Locations



Detected locations where photos were taken

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Location	Region	Country	Photos
	<All>	<All>	<All>	<All>
1	Castle	Wales	United Kingdom	7
2	Castle	Wales	United Kingdom	1
3	Castle	Wales	United Kingdom	6
4	Castle	Wales	United Kingdom	11
5	Castle	Wales	United Kingdom	1
6	Castle	Wales	United Kingdom	1

Photos taken in this location: apple_iphone_12_pro_02.jpg

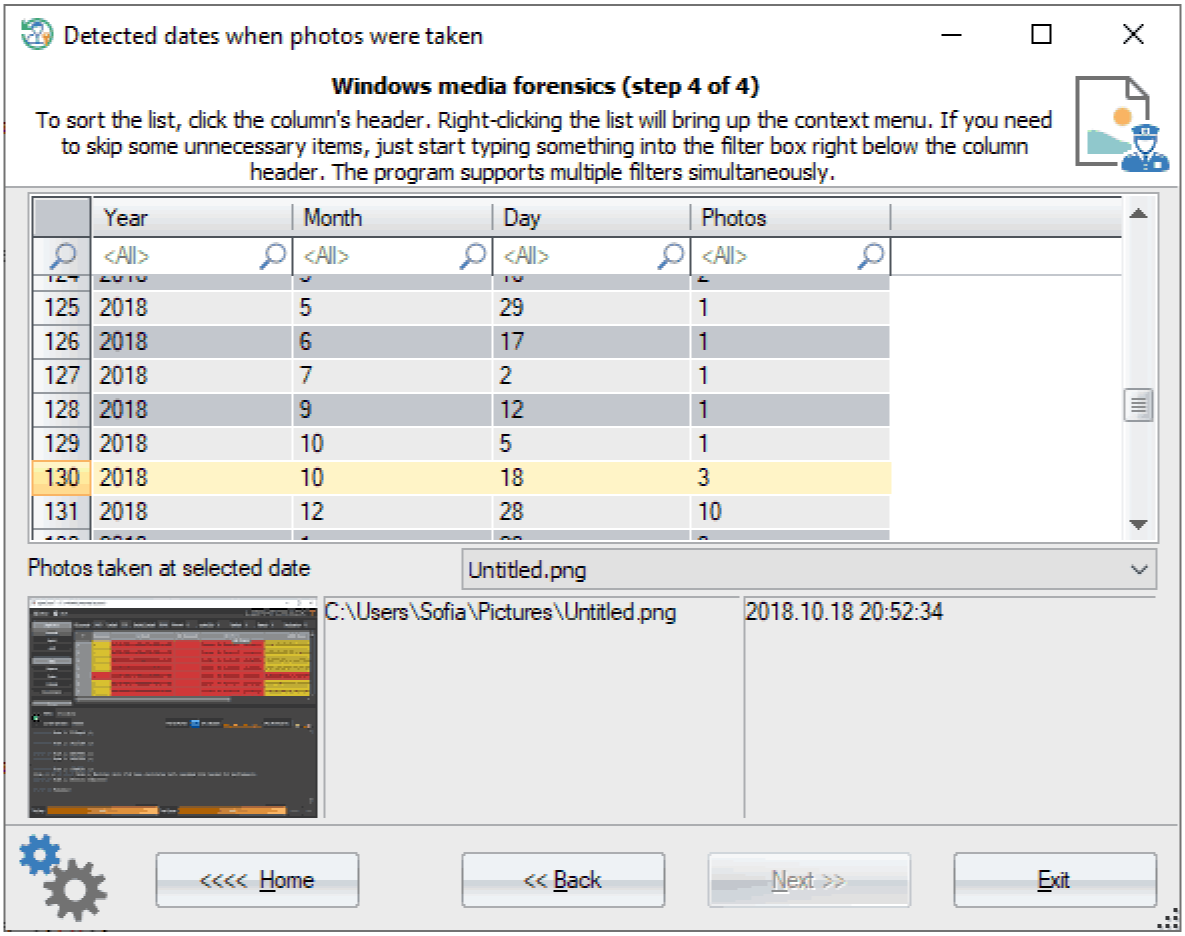
D:\Users\Test2\Pictures\apple_iphone_12_

If initial images contains any EXIF tags related to location, this information is used to populate the **Location** table:

- Location
- Region
- Country
- Photos related to this location

Most mobile devices store metadata with location information in photos they create.

3.7.3.1.7 Dates taken



Detected dates when photos were taken

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

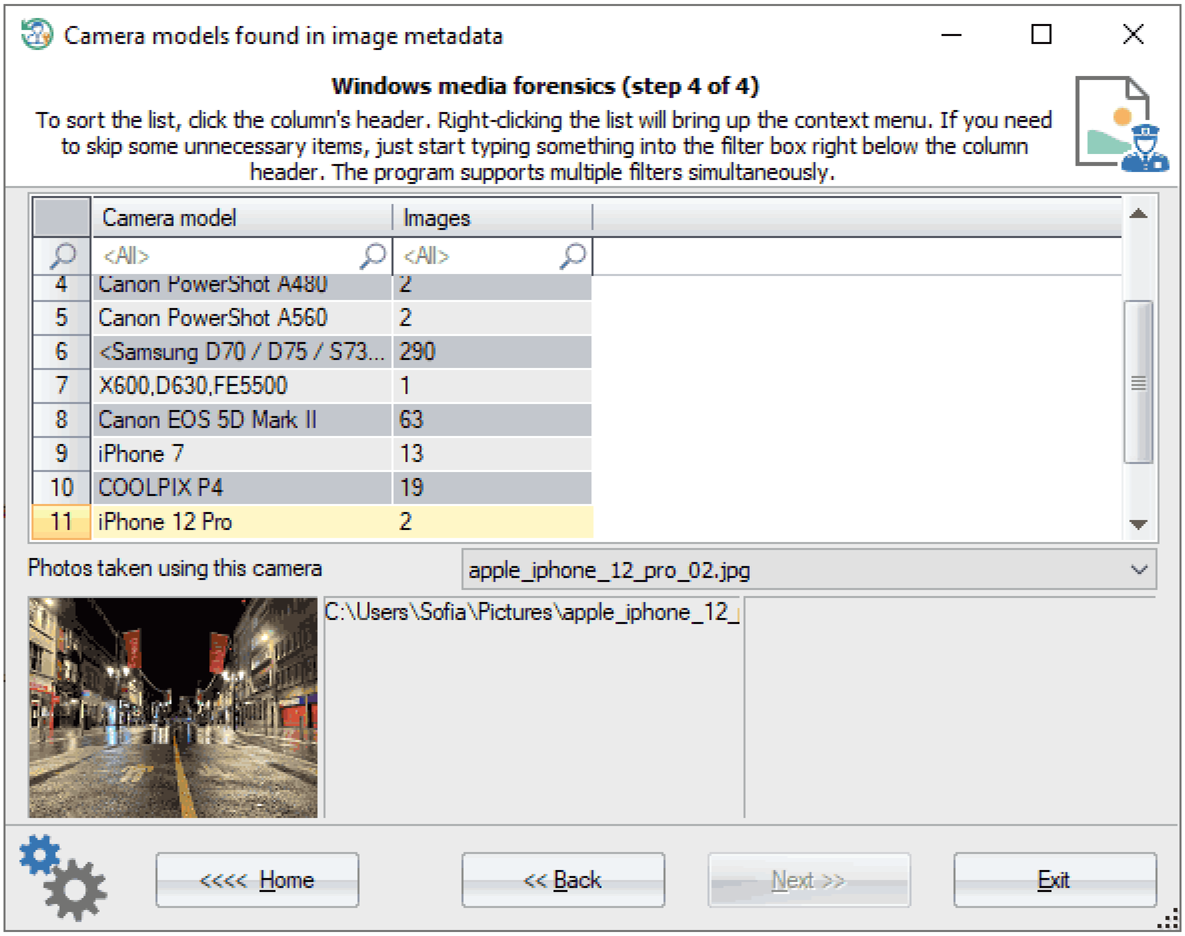
	Year	Month	Day	Photos
	<All>	<All>	<All>	<All>
125	2018	5	29	1
126	2018	6	17	1
127	2018	7	2	1
128	2018	9	12	1
129	2018	10	5	1
130	2018	10	18	3
131	2018	12	28	10

Photos taken at selected date: Untitled.png

C:\Users\Sofia\Pictures\Untitled.png 2018.10.18 20:52:34

The **Date taken** report is convenient if you need to display the time the images were taken and the photos of a certain date.

3.7.3.1.8 Camera models



Camera models found in image metadata

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

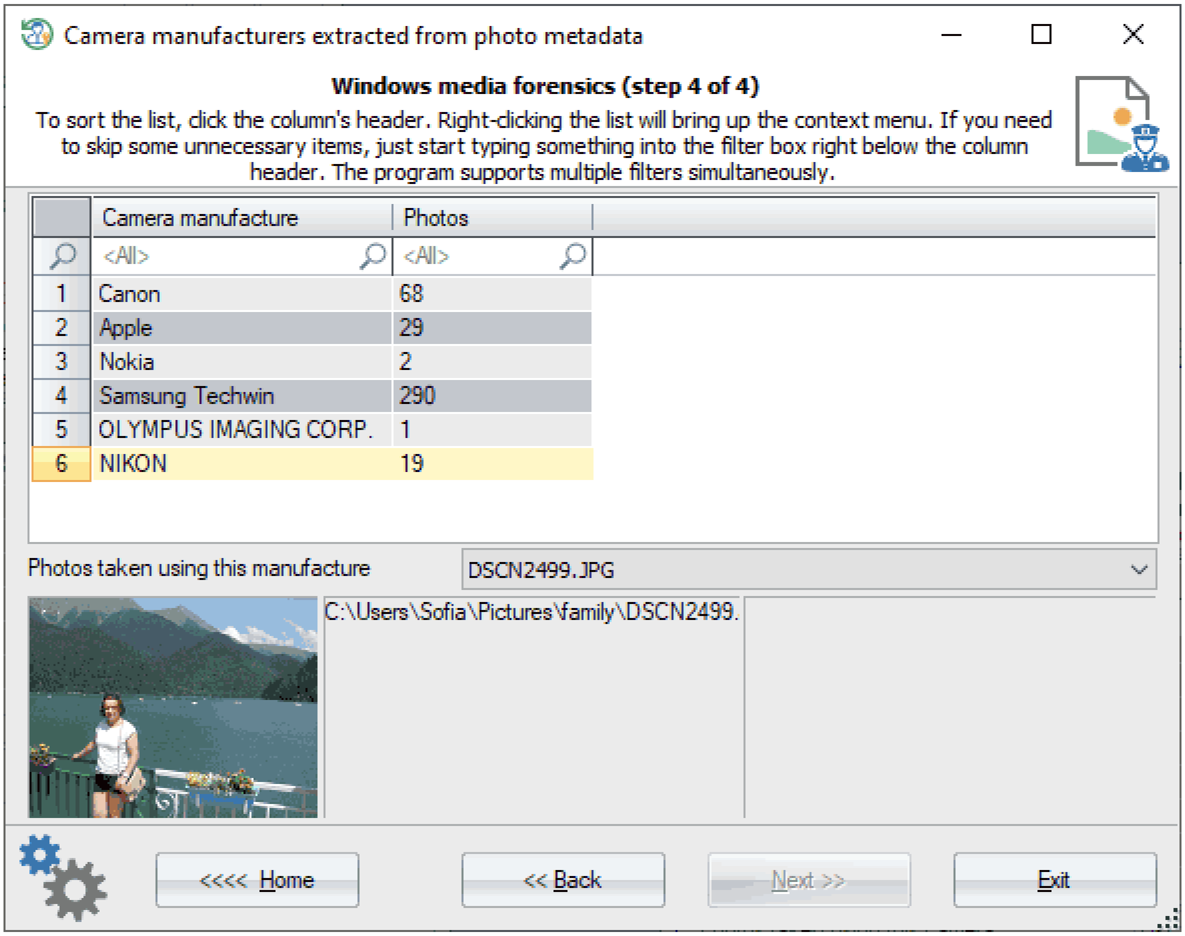
	Camera model	Images
	<All>	<All>
4	Canon PowerShot A480	2
5	Canon PowerShot A560	2
6	<Samsung D70 / D75 / S73...	290
7	X600,D630,FE5500	1
8	Canon EOS 5D Mark II	63
9	iPhone 7	13
10	COOLPIX P4	19
11	iPhone 12 Pro	2

Photos taken using this camera: apple_iphone_12_pro_02.jpg

C:\Users\Sofia\Pictures\apple_iphone_12_

This report groups images by camera models that were used for taking pictures.

3.7.3.1.9 Camera manufacturers



Camera manufacturers extracted from photo metadata

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

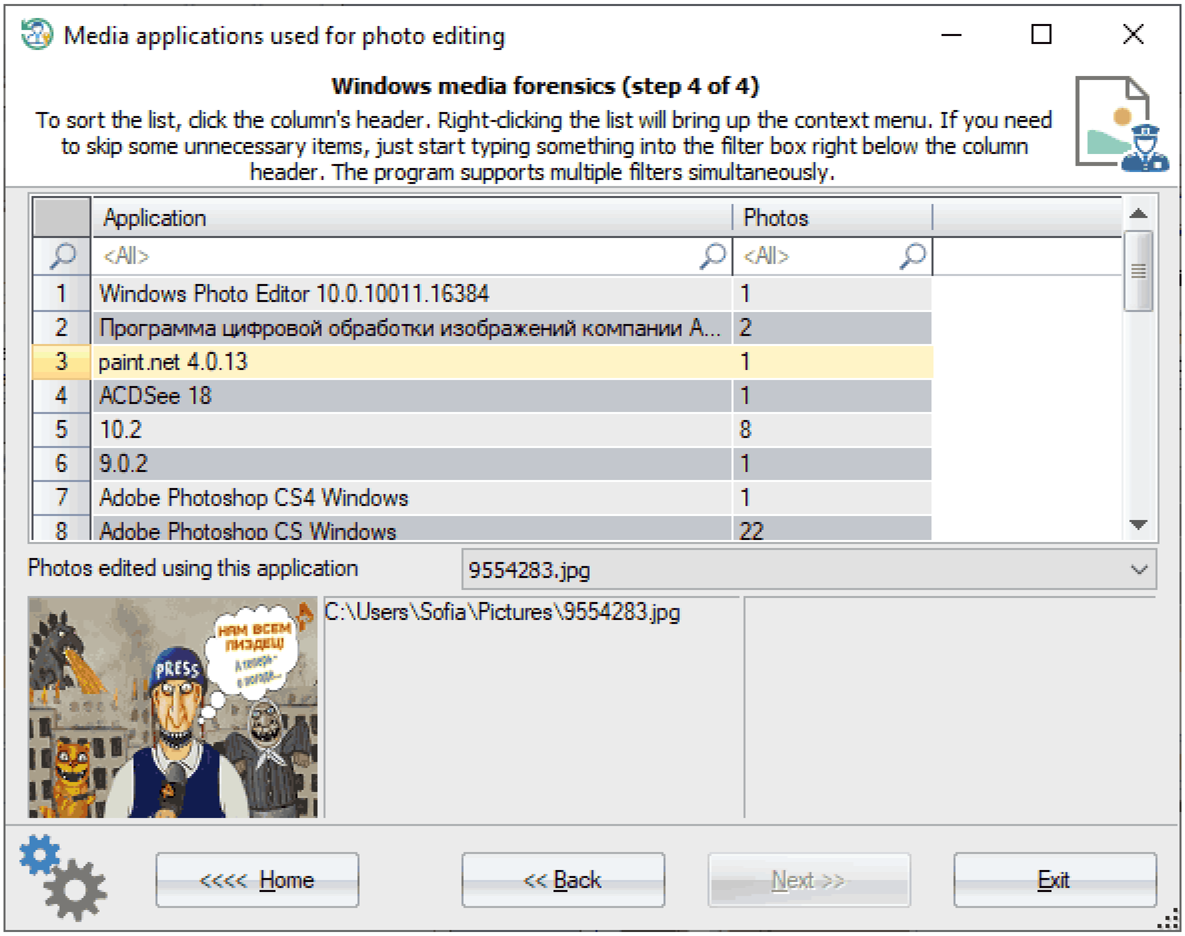
	Camera manufacture	Photos
	<All>	<All>
1	Canon	68
2	Apple	29
3	Nokia	2
4	Samsung Techwin	290
5	OLYMPUS IMAGING CORP.	1
6	NIKON	19

Photos taken using this manufacture: DSCN2499.JPG

C:\Users\Sofia\Pictures\family\DSCN2499.

The same as previous, but items are grouped together by camera manufacturers.

3.7.3.1.10 Multimedia applications



Media applications used for photo editing

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

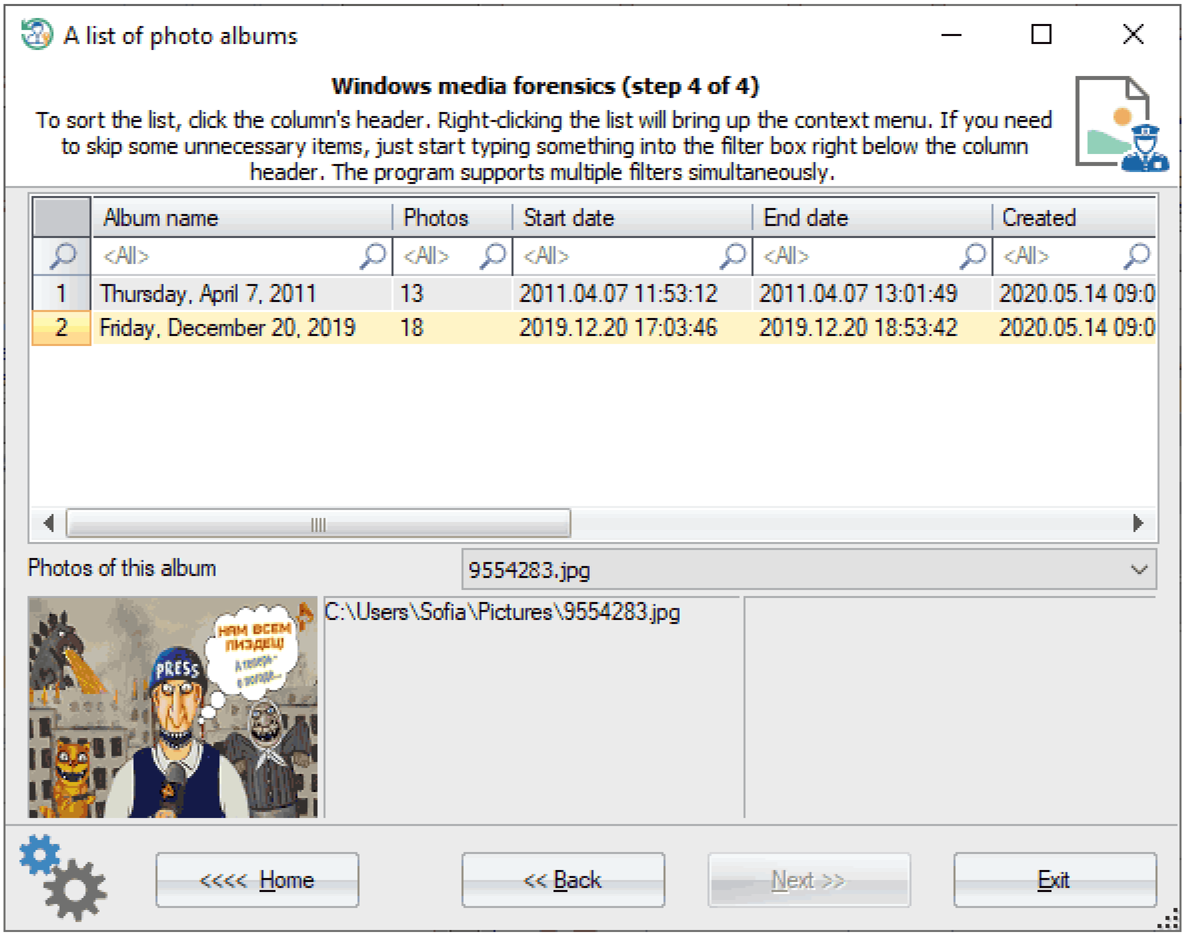
	Application	Photos
	<All>	<All>
1	Windows Photo Editor 10.0.10011.16384	1
2	Программа цифровой обработки изображений компании А...	2
3	paint.net 4.0.13	1
4	ACDSee 18	1
5	10.2	8
6	9.0.2	1
7	Adobe Photoshop CS4 Windows	1
8	Adobe Photoshop CS Windows	22

Photos edited using this application: 9554283.jpg

C:\Users\Sofia\Pictures\9554283.jpg

This report creates a list of all found image editing software and associated picture elements.

3.7.3.1.11 Albums



A list of photo albums

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Album name	Photos	Start date	End date	Created
	<All>	<All>	<All>	<All>	<All>
1	Thursday, April 7, 2011	13	2011.04.07 11:53:12	2011.04.07 13:01:49	2020.05.14 09:0
2	Friday, December 20, 2019	18	2019.12.20 17:03:46	2019.12.20 18:53:42	2020.05.14 09:0

Photos of this album: 9554283.jpg

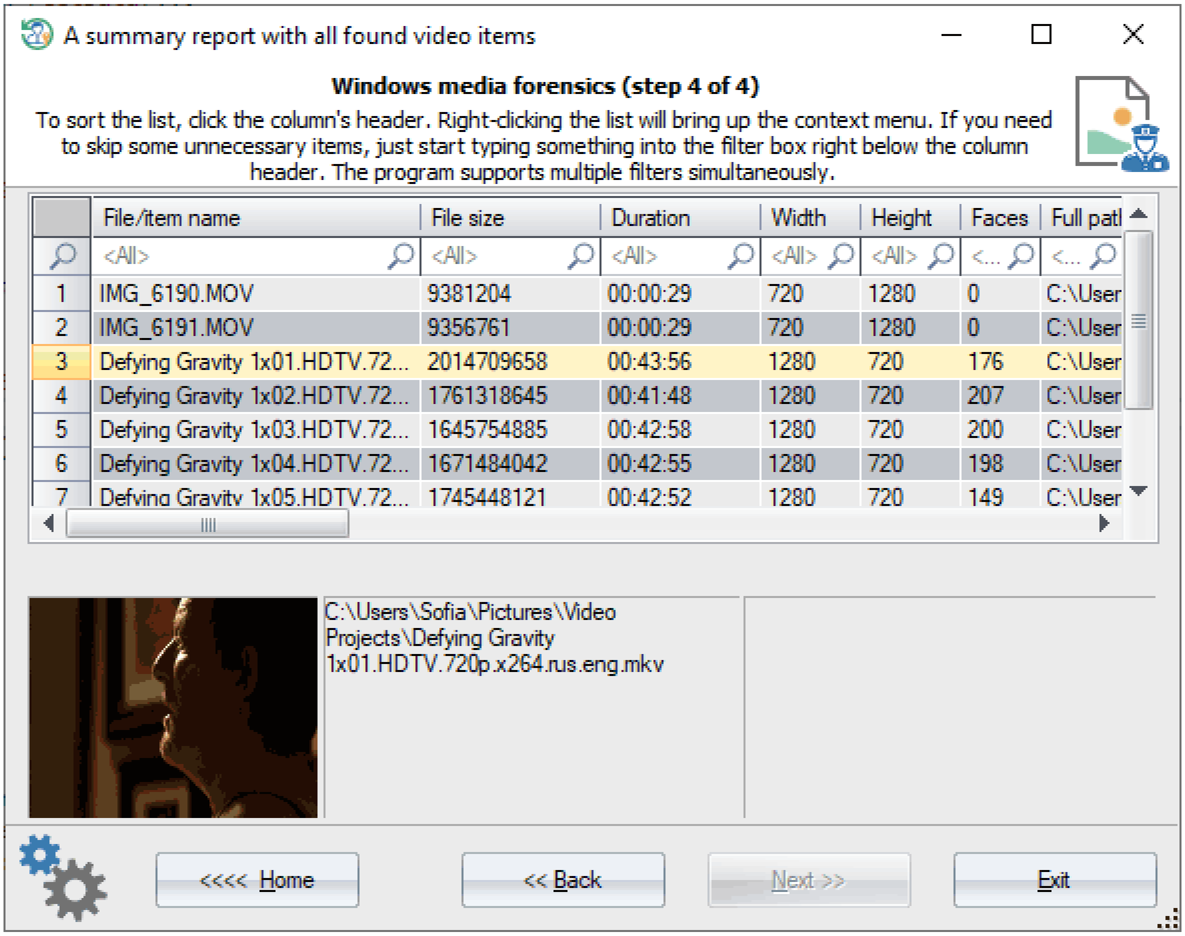
C:\Users\Sofia\Pictures\9554283.jpg

This report displays albums generated by the Windows Photo application.

3.7.3.2 Video analysis

Enter topic text here.

3.7.3.2.1 Video items



A summary report with all found video items

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

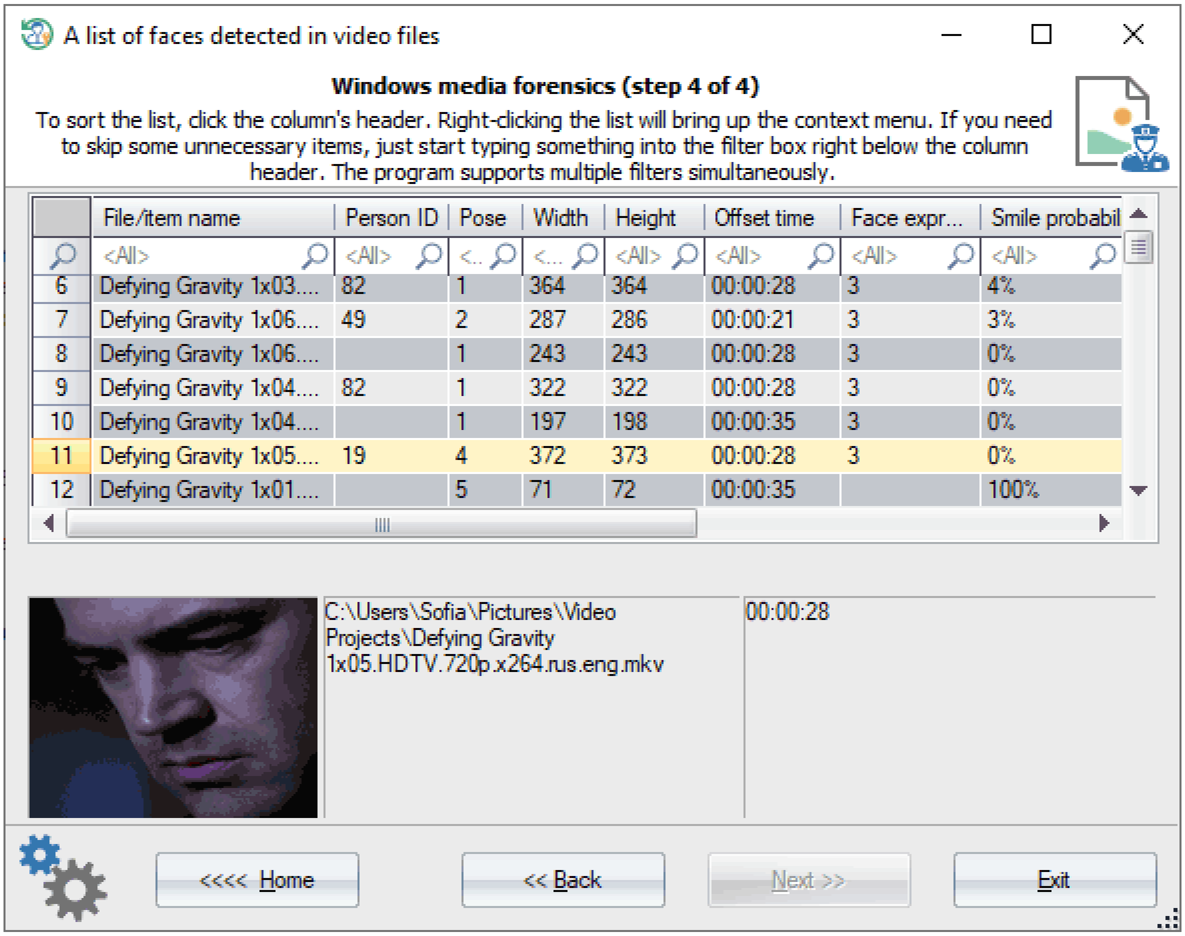
	File/item name	File size	Duration	Width	Height	Faces	Full patl
	<All>	<All>	<All>	<All>	<All>	<...	<...
1	IMG_6190.MOV	9381204	00:00:29	720	1280	0	C:\User
2	IMG_6191.MOV	9356761	00:00:29	720	1280	0	C:\User
3	Defying Gravity 1x01.HDTV.72...	2014709658	00:43:56	1280	720	176	C:\User
4	Defying Gravity 1x02.HDTV.72...	1761318645	00:41:48	1280	720	207	C:\User
5	Defying Gravity 1x03.HDTV.72...	1645754885	00:42:58	1280	720	200	C:\User
6	Defying Gravity 1x04.HDTV.72...	1671484042	00:42:55	1280	720	198	C:\User
7	Defying Gravity 1x05.HDTV.72...	1745448121	00:42:52	1280	720	149	C:\User

C:\Users\Sofia\Pictures\Video Projects\Defying Gravity 1x01.HDTV.720p.x264.rus.eng.mkv

The **Video** report includes a general info of the video elements in the Windows photo gallery. Namely:

- The name of the video file
- File size
- Video duration
- Width and height of the video
- The number of faces detected
- Full path to the file
- Video author
- Video copyright
- Video caption
- Path to the duplicate, if found
- Date produced or compiled
- Last created/modified/edited
- Last time the video viewed in library
- Album name the video belongs to

3.7.3.2.2 Faces



Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	File/item name	Person ID	Pose	Width	Height	Offset time	Face expr...	Smile probabil
	<All>	<All>	<...	<...	<All>	<All>	<All>	<All>
6	Defying Gravity 1x03....	82	1	364	364	00:00:28	3	4%
7	Defying Gravity 1x06....	49	2	287	286	00:00:21	3	3%
8	Defying Gravity 1x06....		1	243	243	00:00:28	3	0%
9	Defying Gravity 1x04....	82	1	322	322	00:00:28	3	0%
10	Defying Gravity 1x04....		1	197	198	00:00:35	3	0%
11	Defying Gravity 1x05....	19	4	372	373	00:00:28	3	0%
12	Defying Gravity 1x01....		5	71	72	00:00:35		100%

C:\Users\Sofia\Pictures\Video Projects\Defying Gravity 1x05.HDTV.720p.x264.rus.eng.mkv

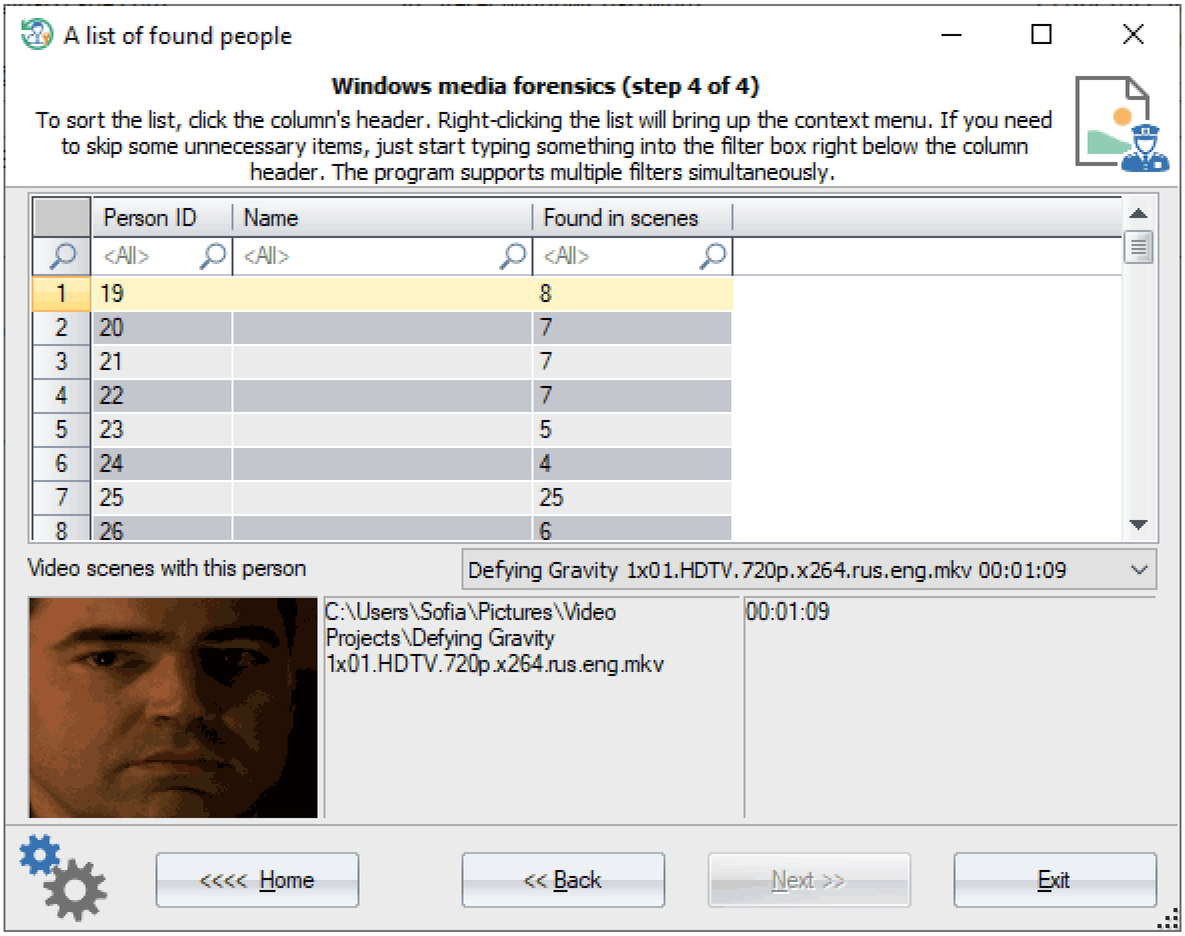
00:00:28

The **Video faces** report extracts faces off the video items and displays their properties:

- The name of the video file where the face was found
- Person identity
- Face position
- Face width
- Face height
- Time on video where it was found
- Face expression
- Smile probability
- Full path to the file

Click the face picture in order to view the full scene it was found at.

3.7.3.2.3 Persons



A list of found people

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Person ID	Name	Found in scenes
	<All>	<All>	<All>
1	19		8
2	20		7
3	21		7
4	22		7
5	23		5
6	24		4
7	25		25
8	26		6

Video scenes with this person: Defying Gravity 1x01.HDTV.720p.x264.rus.eng.mkv 00:01:09

C:\Users\Sofia\Pictures\Video Projects\Defying Gravity 1x01.HDTV.720p.x264.rus.eng.mkv

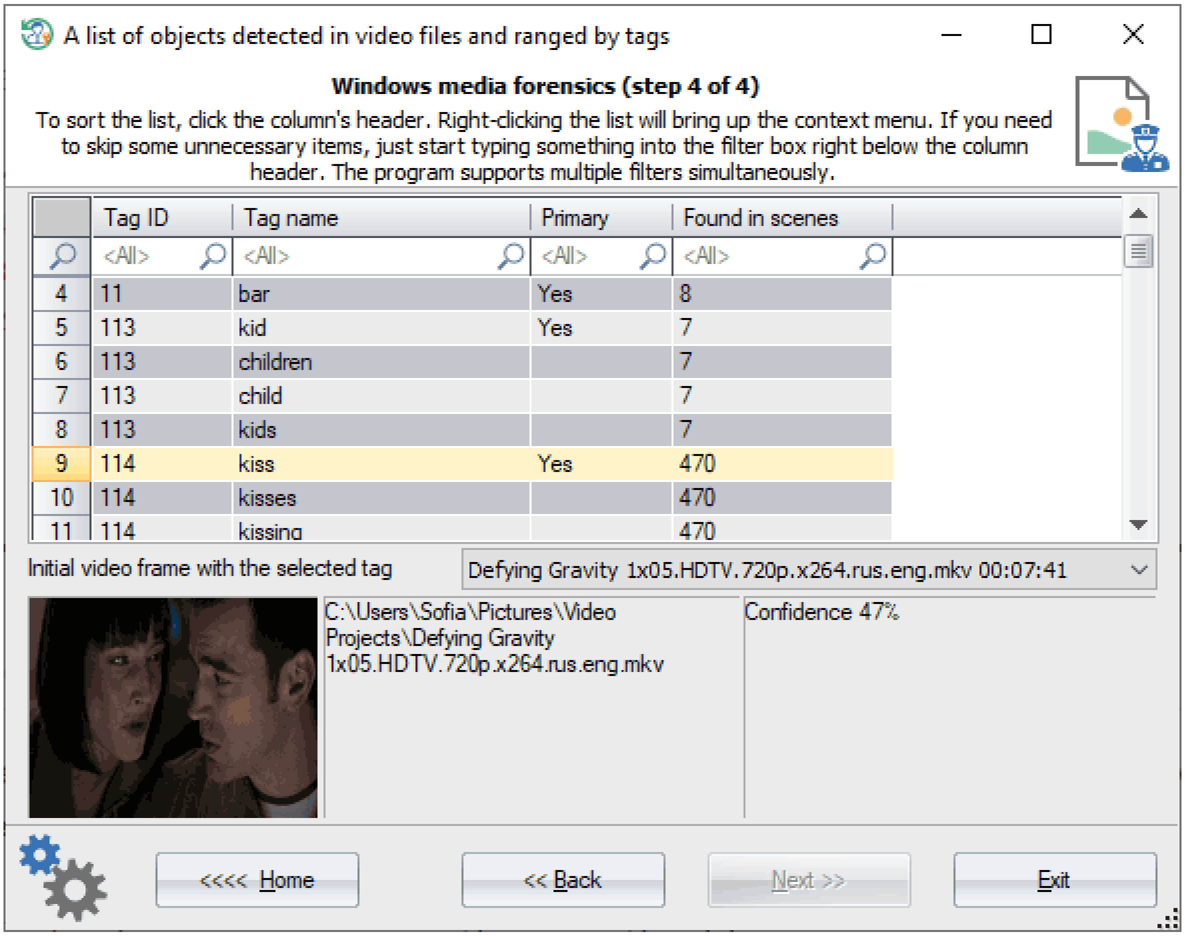
00:01:09

This report behaves exactly as one used to identify people in the photos, except that it works for video files instead. It has only 3 fields:

- Person Identity
- Person name, empty if the user has not set it explicitly
- The number of scenes with this face

To view scenes with this person, first select it and then choose a scene from the combo-box below the table.

3.7.3.2.4 Tags



A list of objects detected in video files and ranged by tags

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Tag ID	Tag name	Primary	Found in scenes
	<All>	<All>	<All>	<All>
4	11	bar	Yes	8
5	113	kid	Yes	7
6	113	children		7
7	113	child		7
8	113	kids		7
9	114	kiss	Yes	470
10	114	kisses		470
11	114	kissing		470

Initial video frame with the selected tag: Defying Gravity 1x05.HDTV.720p.x264.rus.eng.mkv 00:07:41

C:\Users\Sofia\Pictures\Video Projects\Defying Gravity 1x05.HDTV.720p.x264.rus.eng.mkv

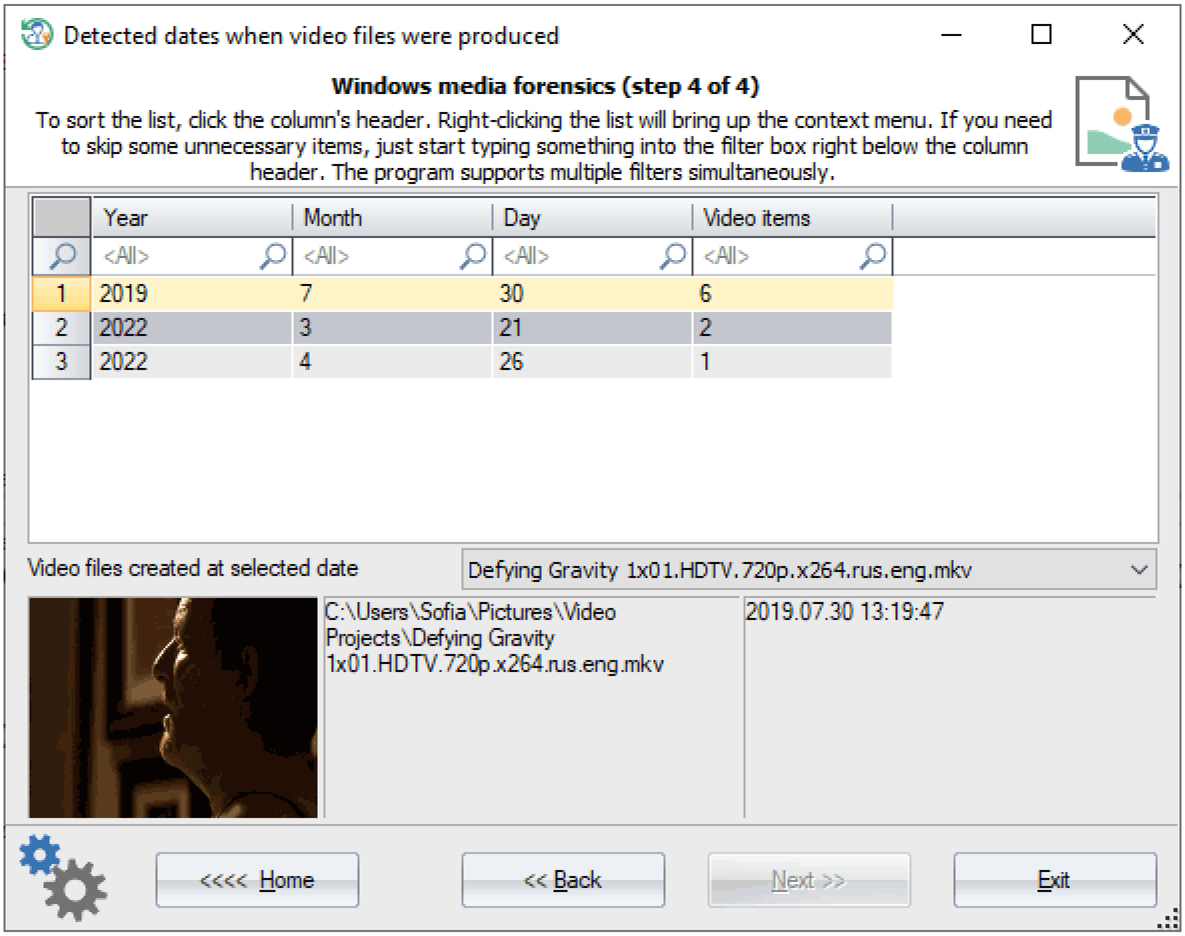
Confidence 47%

The **Tags** table groups video items by found tags. Every tag has the following properties:

- Tags ID
- Short name of the tag
- Primary or not
- Found in video scenes

The combo-box under the table holds the list of video items along with the scene time where the tag was detected. First come scenes with the most reliable coincidence.

3.7.3.2.5 Dates produced



Detected dates when video files were produced

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Year	Month	Day	Video items
	<All>	<All>	<All>	<All>
1	2019	7	30	6
2	2022	3	21	2
3	2022	4	26	1

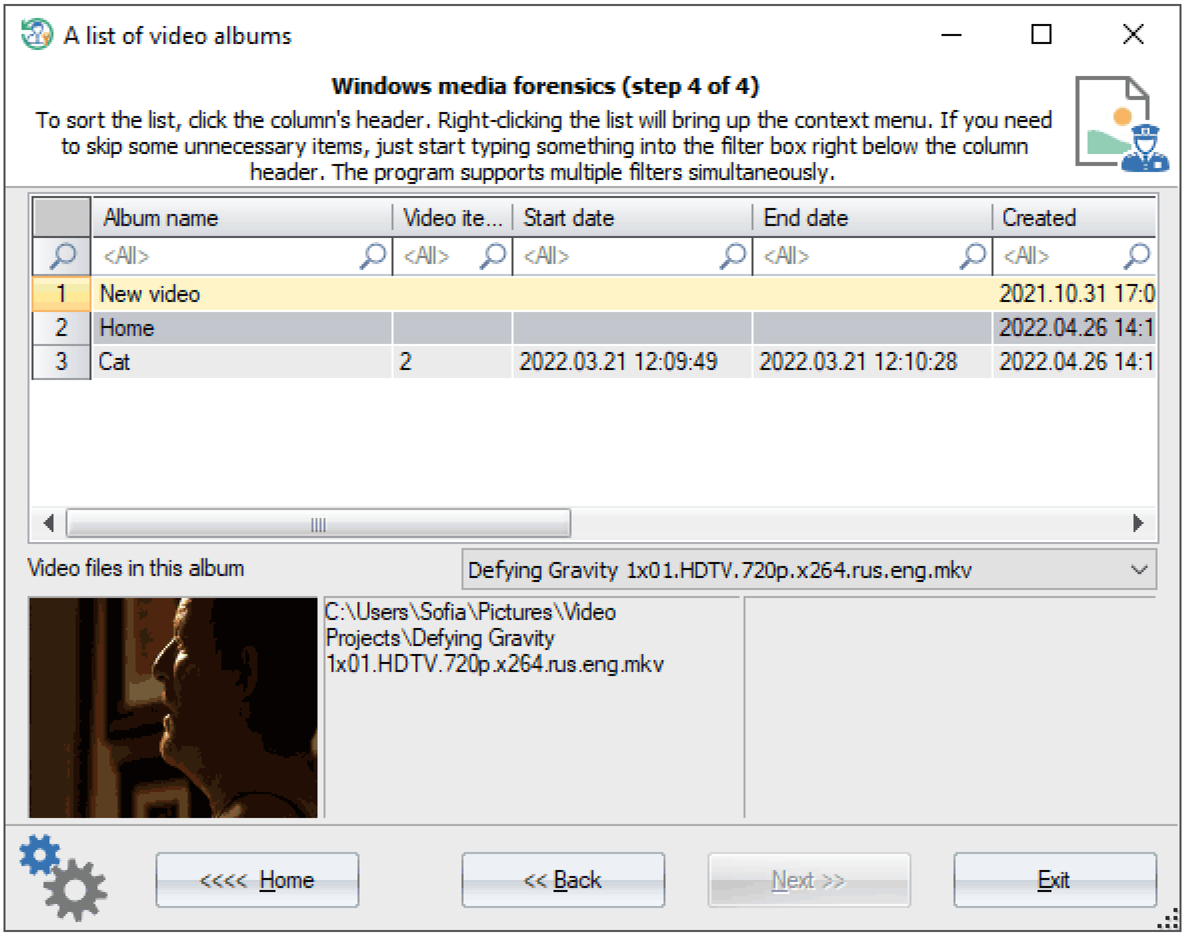
Video files created at selected date: Defying Gravity 1x01.HDTV.720p.x264.rus.eng.mkv

C:\Users\Sofia\Pictures\Video Projects\Defying Gravity 1x01.HDTV.720p.x264.rus.eng.mkv

2019.07.30 13:19:47

The **Date produced** report is convenient if you need to group the video items by the time they produced/compiled.

3.7.3.2.6 Albums



Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Album name	Video ite...	Start date	End date	Created
	<All>	<All>	<All>	<All>	<All>
1	New video				2021.10.31 17:0
2	Home				2022.04.26 14:1
3	Cat	2	2022.03.21 12:09:49	2022.03.21 12:10:28	2022.04.26 14:1

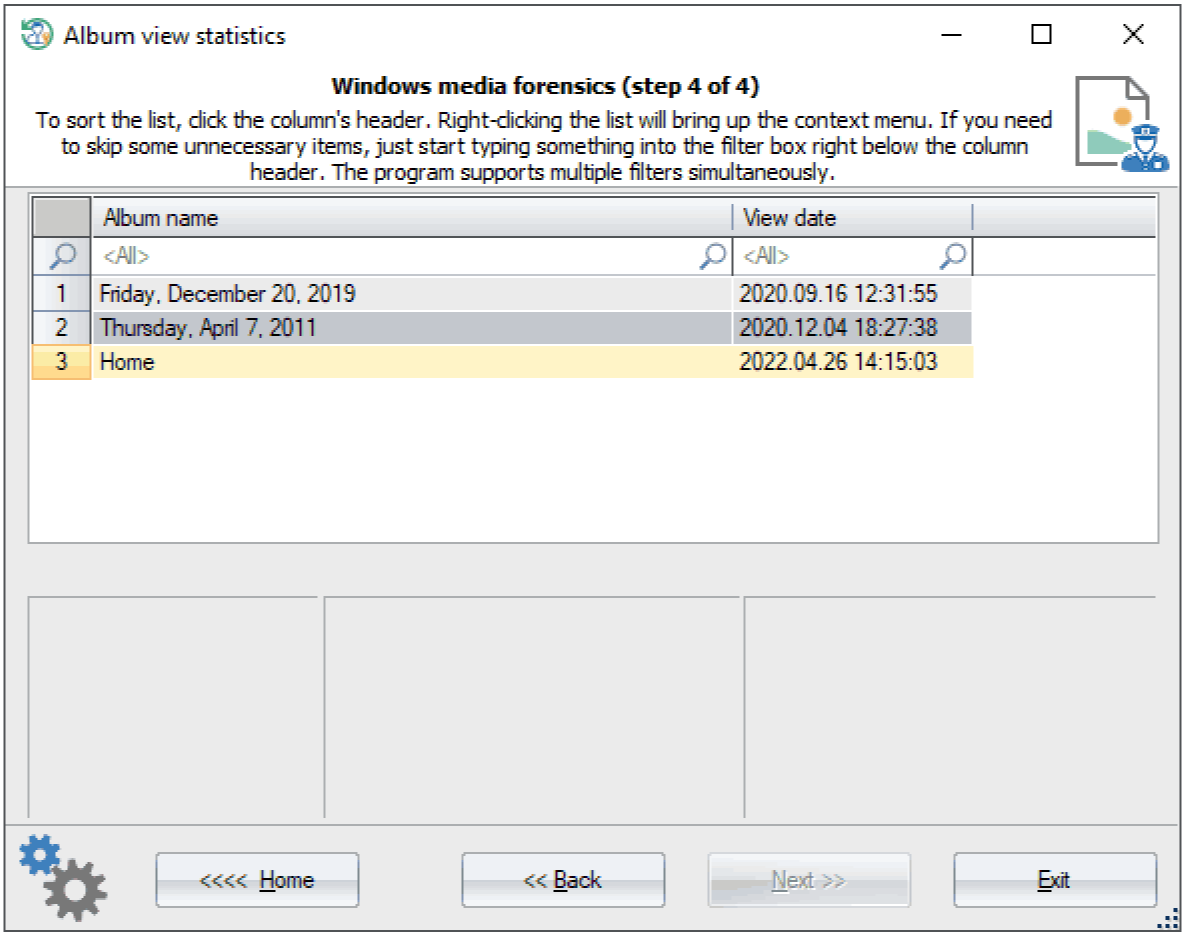
Video files in this album: Defying Gravity 1x01.HDTV.720p.x264.rus.eng.mkv

C:\Users\Sofia\Pictures\Video Projects\Defying Gravity 1x01.HDTV.720p.x264.rus.eng.mkv

This report displays video albums generated by the Windows Photo.

3.7.3.3 User actions

3.7.3.3.1 Album views



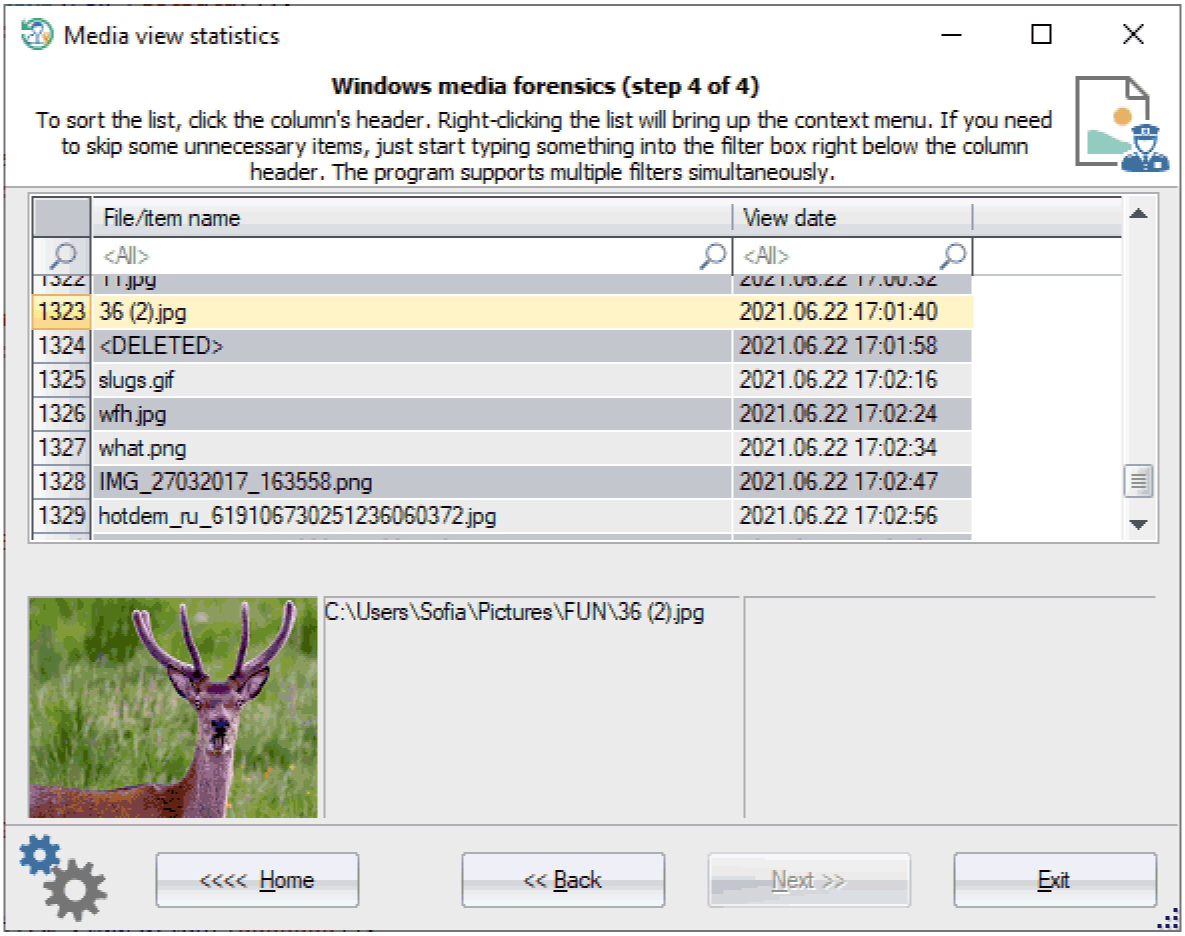
Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Album name	View date
	<All>	<All>
1	Friday, December 20, 2019	2020.09.16 12:31:55
2	Thursday, April 7, 2011	2020.12.04 18:27:38
3	Home	2022.04.26 14:15:03

Statistics on photo and video albums.

3.7.3.3.2 File views



Windows media forensics (step 4 of 4)

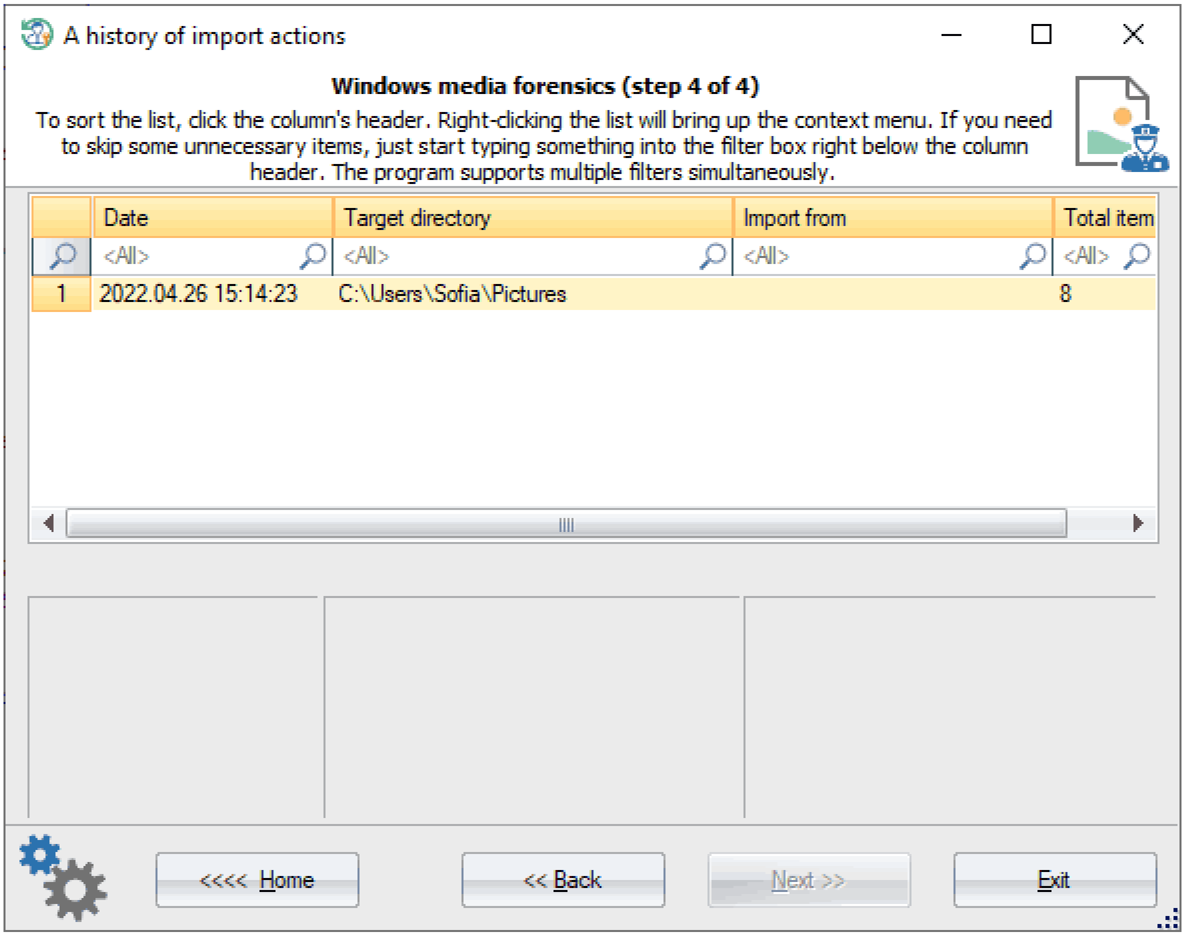
To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	File/item name	View date
	<All>	<All>
1322	11.jpg	2021.06.22 17:00:32
1323	36 (2).jpg	2021.06.22 17:01:40
1324	<DELETED>	2021.06.22 17:01:58
1325	slugs.gif	2021.06.22 17:02:16
1326	wfh.jpg	2021.06.22 17:02:24
1327	what.png	2021.06.22 17:02:34
1328	IMG_27032017_163558.png	2021.06.22 17:02:47
1329	hotdem_ru_619106730251236060372.jpg	2021.06.22 17:02:56

C:\Users\Sofia\Pictures\FUN\36 (2).jpg

Statistics on photo and video file views in the Windows Photo library.

3.7.3.3.3 Import history



A history of import actions

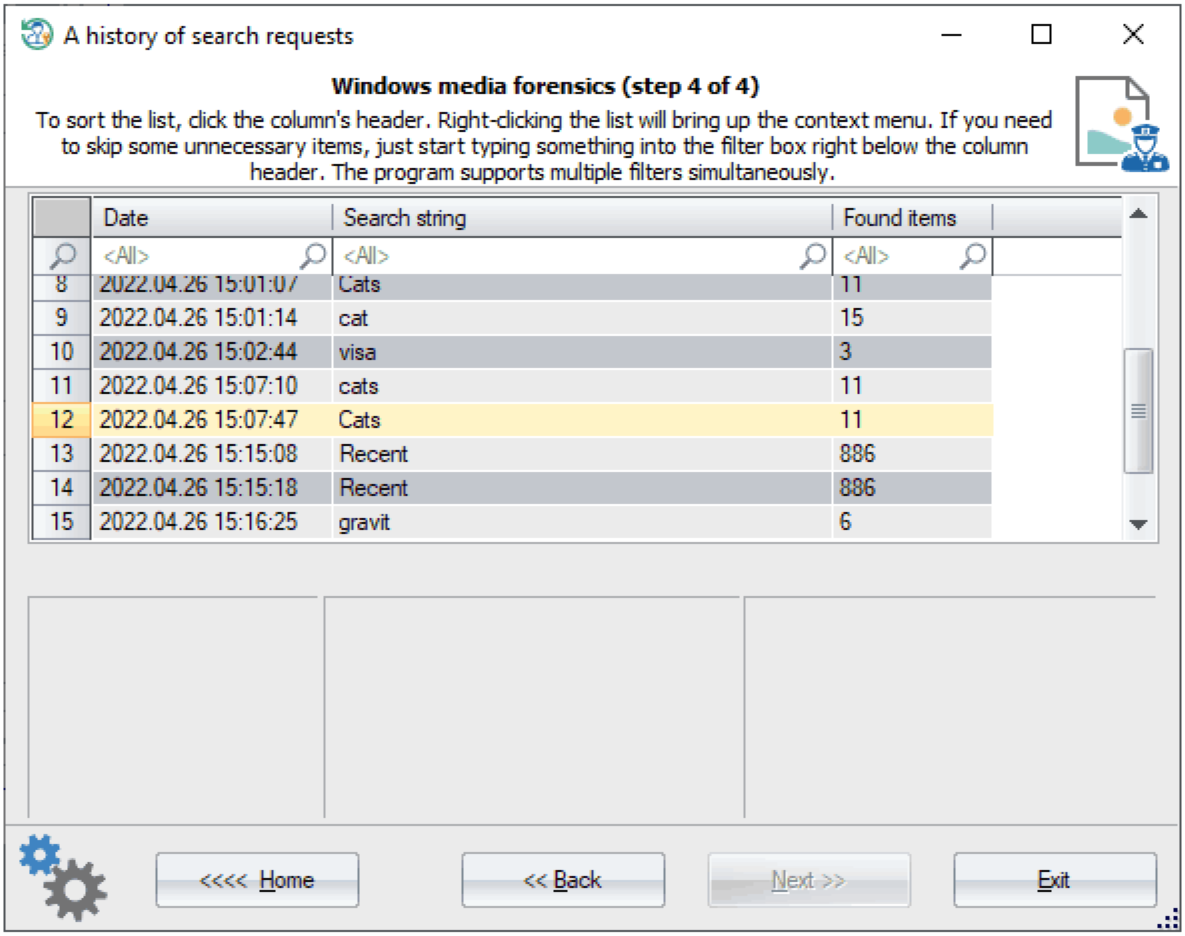
Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Date	Target directory	Import from	Total item
	<All>	<All>	<All>	<All>
1	2022.04.26 15:14:23	C:\Users\Sofia\Pictures		8

The history of import operations in the Windows Photo library.

3.7.3.3.4 Search history



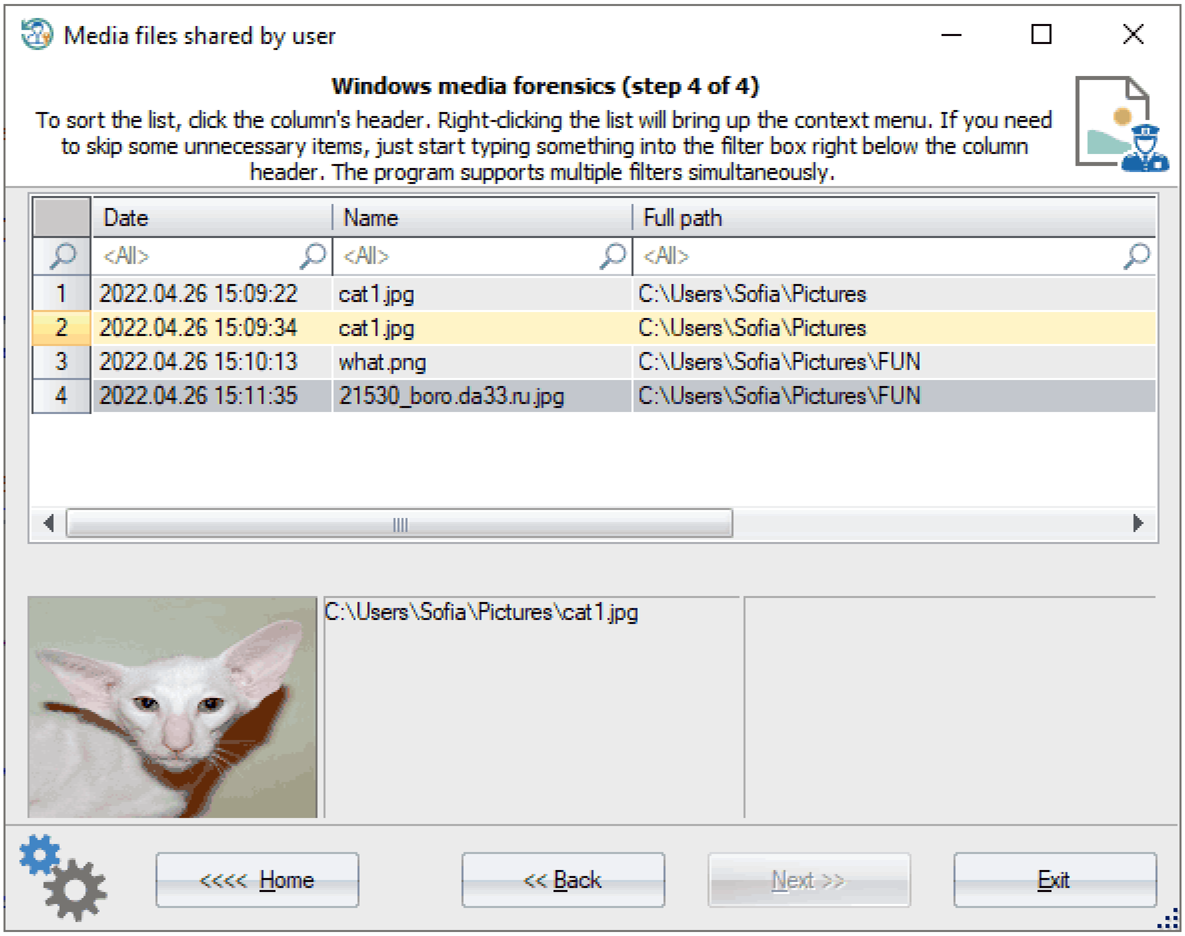
Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Date	Search string	Found items
	<All>	<All>	<All>
8	2022.04.26 15:01:07	Cats	11
9	2022.04.26 15:01:14	cat	15
10	2022.04.26 15:02:44	visa	3
11	2022.04.26 15:07:10	cats	11
12	2022.04.26 15:07:47	Cats	11
13	2022.04.26 15:15:08	Recent	886
14	2022.04.26 15:15:18	Recent	886
15	2022.04.26 15:16:25	gravit	6

The history of search queries in the Windows Photo.

3.7.3.3.5 Shared items



Media files shared by user

Windows media forensics (step 4 of 4)

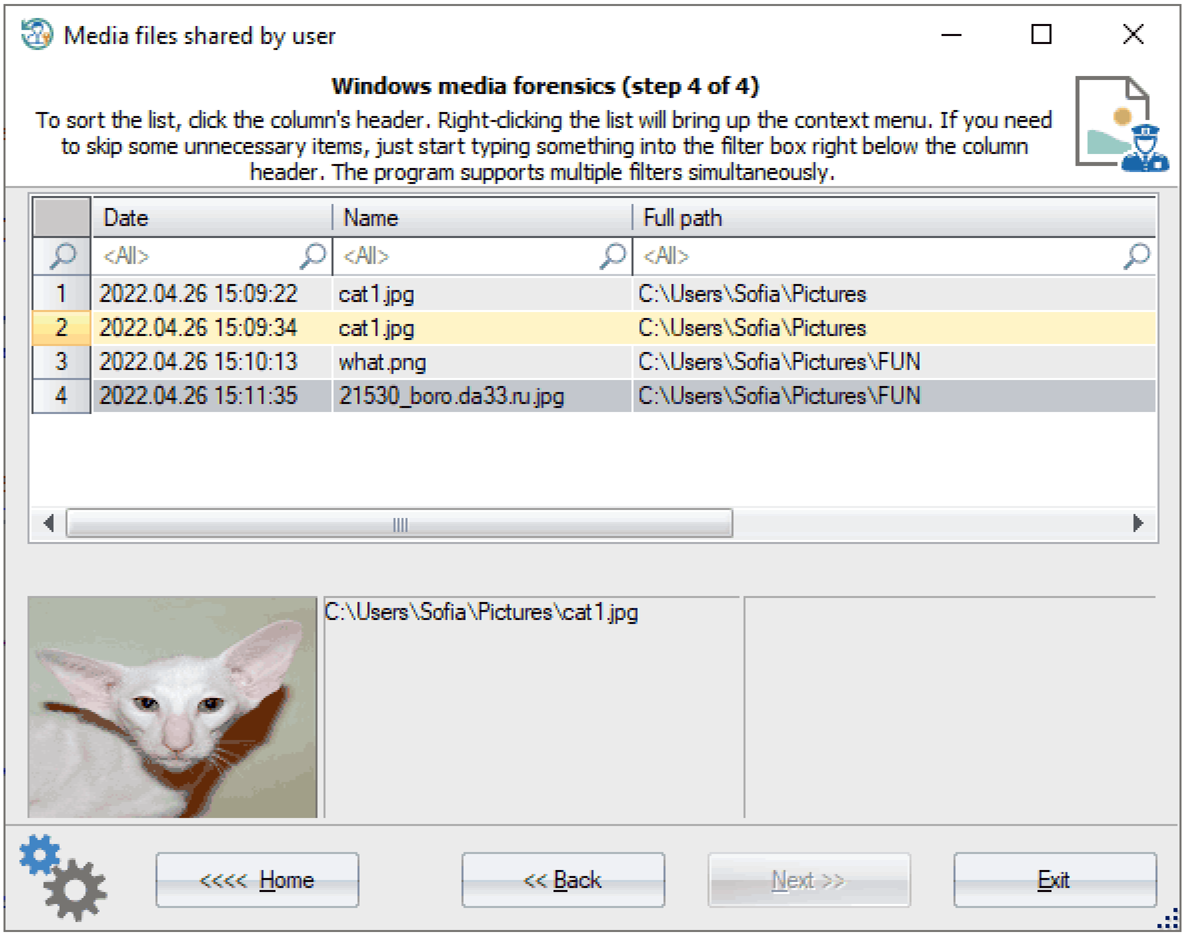
To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Date	Name	Full path
	<All>	<All>	<All>
1	2022.04.26 15:09:22	cat1.jpg	C:\Users\Sofia\Pictures
2	2022.04.26 15:09:34	cat1.jpg	C:\Users\Sofia\Pictures
3	2022.04.26 15:10:13	what.png	C:\Users\Sofia\Pictures\FUN
4	2022.04.26 15:11:35	21530_boro.da33.ru.jpg	C:\Users\Sofia\Pictures\FUN

C:\Users\Sofia\Pictures\cat1.jpg

The history of the items user shared from the Windows Photo library.

3.7.3.3.6 Printed items



Media files shared by user

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

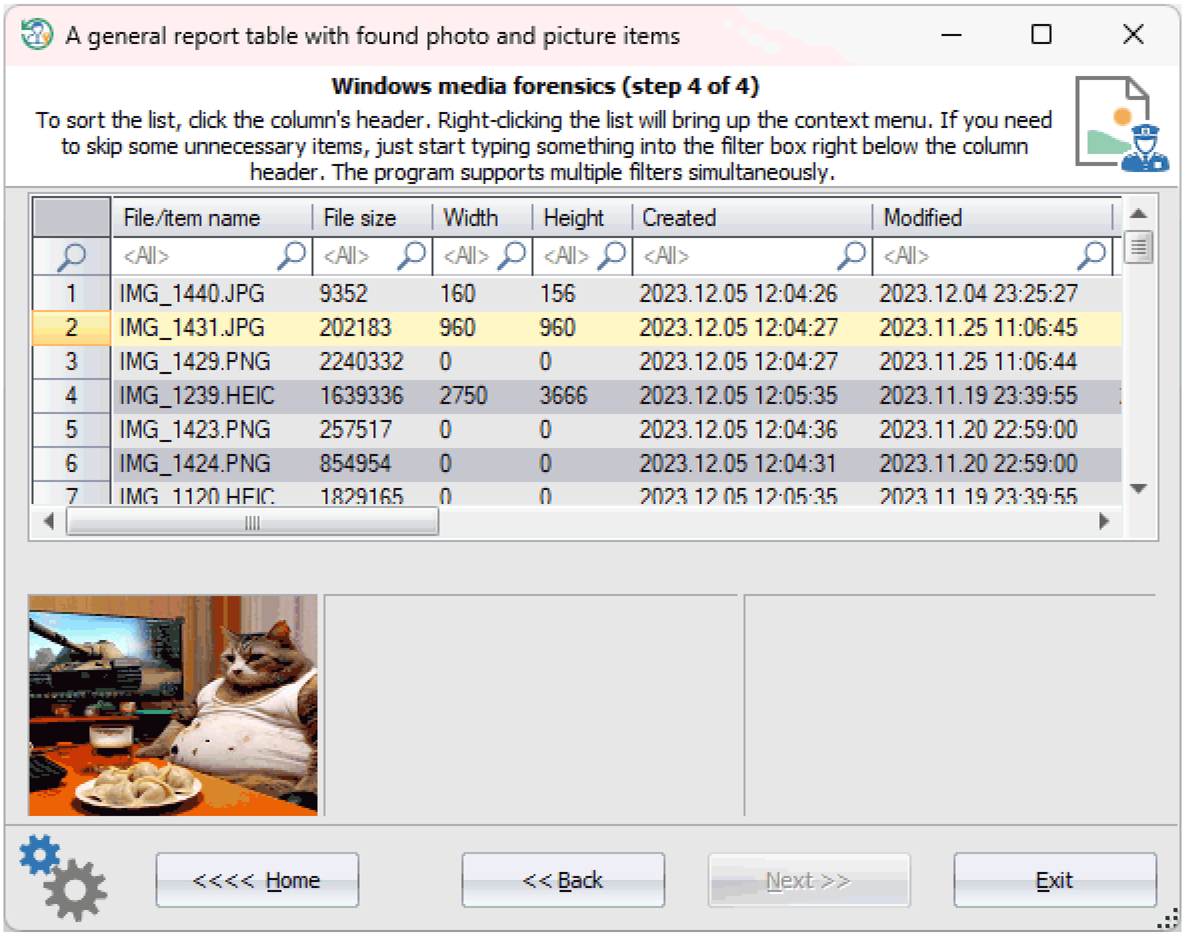
	Date	Name	Full path
	<All>	<All>	<All>
1	2022.04.26 15:09:22	cat1.jpg	C:\Users\Sofia\Pictures
2	2022.04.26 15:09:34	cat1.jpg	C:\Users\Sofia\Pictures
3	2022.04.26 15:10:13	what.png	C:\Users\Sofia\Pictures\FUN
4	2022.04.26 15:11:35	21530_boro.da33.ru.jpg	C:\Users\Sofia\Pictures\FUN

C:\Users\Sofia\Pictures\cat1.jpg

The history of the items user printed in the Windows Photo library.

3.7.3.4 Photo library

3.7.3.4.1 Images



A general report table with found photo and picture items

Windows media forensics (step 4 of 4)

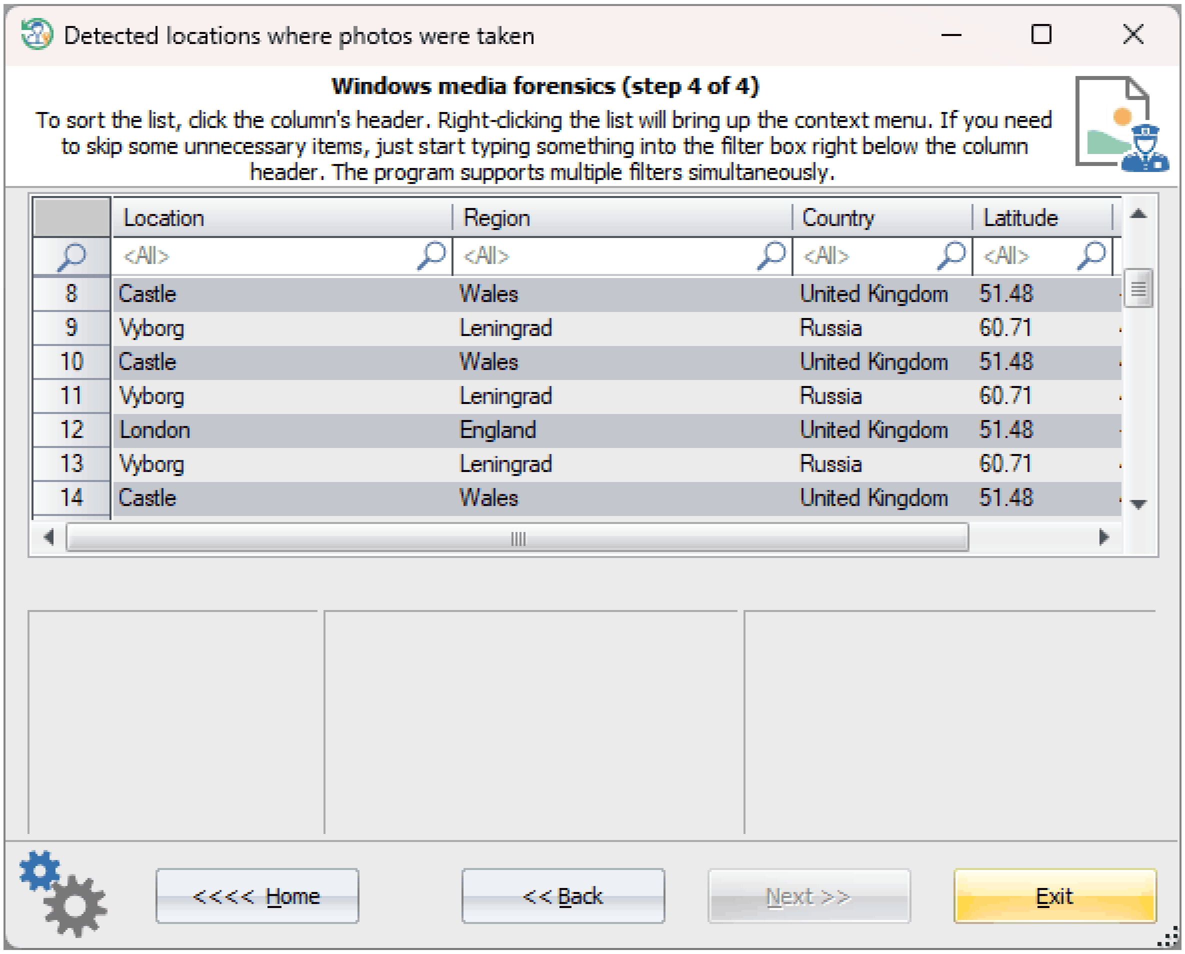
To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	File/item name	File size	Width	Height	Created	Modified
	<All>	<All>	<All>	<All>	<All>	<All>
1	IMG_1440.JPG	9352	160	156	2023.12.05 12:04:26	2023.12.04 23:25:27
2	IMG_1431.JPG	202183	960	960	2023.12.05 12:04:27	2023.11.25 11:06:45
3	IMG_1429.PNG	2240332	0	0	2023.12.05 12:04:27	2023.11.25 11:06:44
4	IMG_1239.HEIC	1639336	2750	3666	2023.12.05 12:05:35	2023.11.19 23:39:55
5	IMG_1423.PNG	257517	0	0	2023.12.05 12:04:36	2023.11.20 22:59:00
6	IMG_1424.PNG	854954	0	0	2023.12.05 12:04:31	2023.11.20 22:59:00
7	IMG_1120.HEIC	1829165	0	0	2023.12.05 12:05:35	2023.11.19 23:39:55

This report contains information about the images stored in the **Photos** app (Windows 10 and newer OSes only):

- File name
- File size
- Picture width
- Picture height
- Creation and last modification dates
- Date takes
- Date of adding to the library
- Full path
- Latitude
- Longitude
- Tags, if any

3.7.3.4.2 Places



Windows media forensics (step 4 of 4)

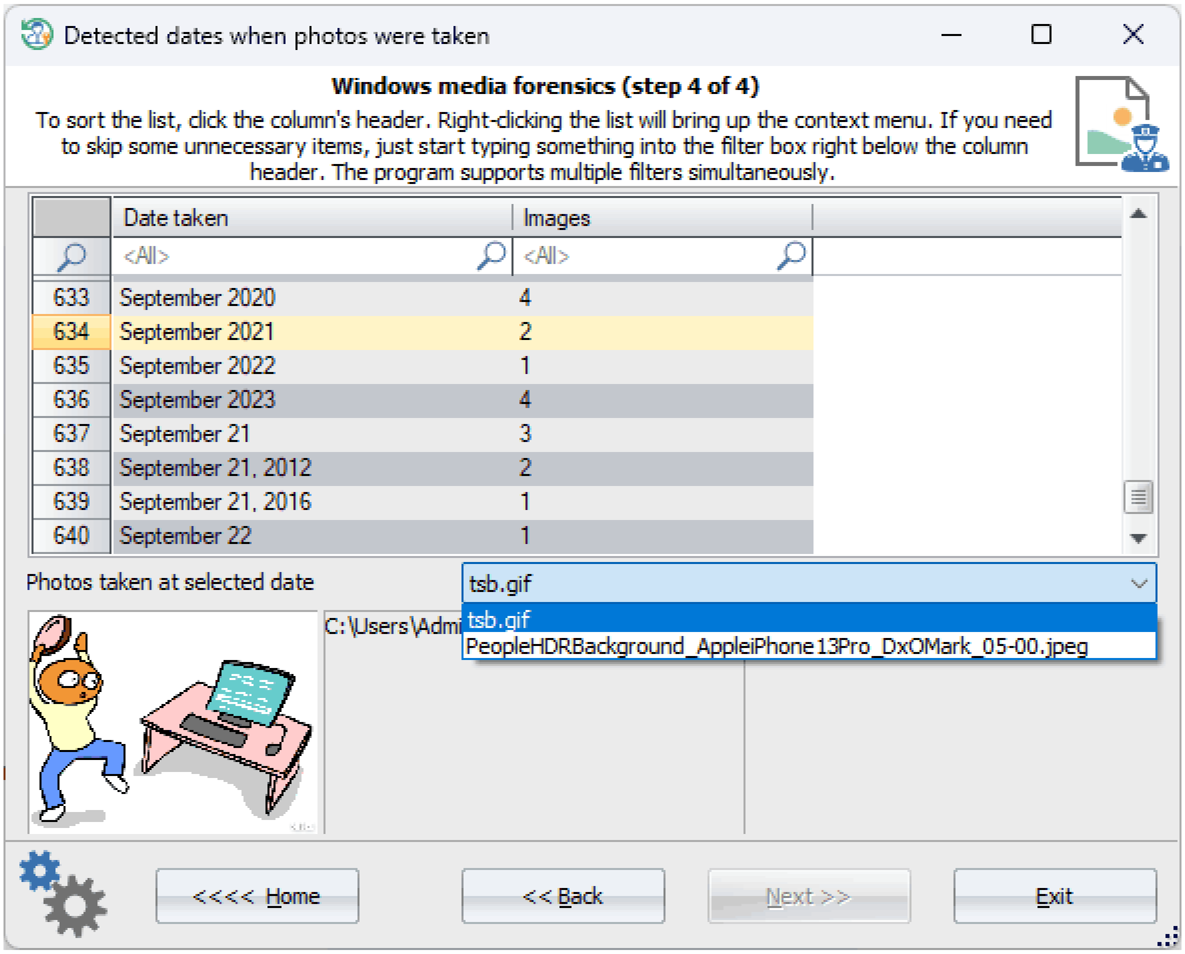
To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Location	Region	Country	Latitude
	<All>	<All>	<All>	<All>
8	Castle	Wales	United Kingdom	51.48
9	Vyborg	Leningrad	Russia	60.71
10	Castle	Wales	United Kingdom	51.48
11	Vyborg	Leningrad	Russia	60.71
12	London	England	United Kingdom	51.48
13	Vyborg	Leningrad	Russia	60.71
14	Castle	Wales	United Kingdom	51.48

Most mobile devices store metadata about the location where photos were taken. If such information is available, it will be displayed in this table, namely:

- Exact location
- Region
- Country
- Latitude
- Longitude

3.7.3.4.3 Dates taken



Detected dates when photos were taken

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Date taken	Images
	<All>	<All>
633	September 2020	4
634	September 2021	2
635	September 2022	1
636	September 2023	4
637	September 21	3
638	September 21, 2012	2
639	September 21, 2016	1
640	September 22	1

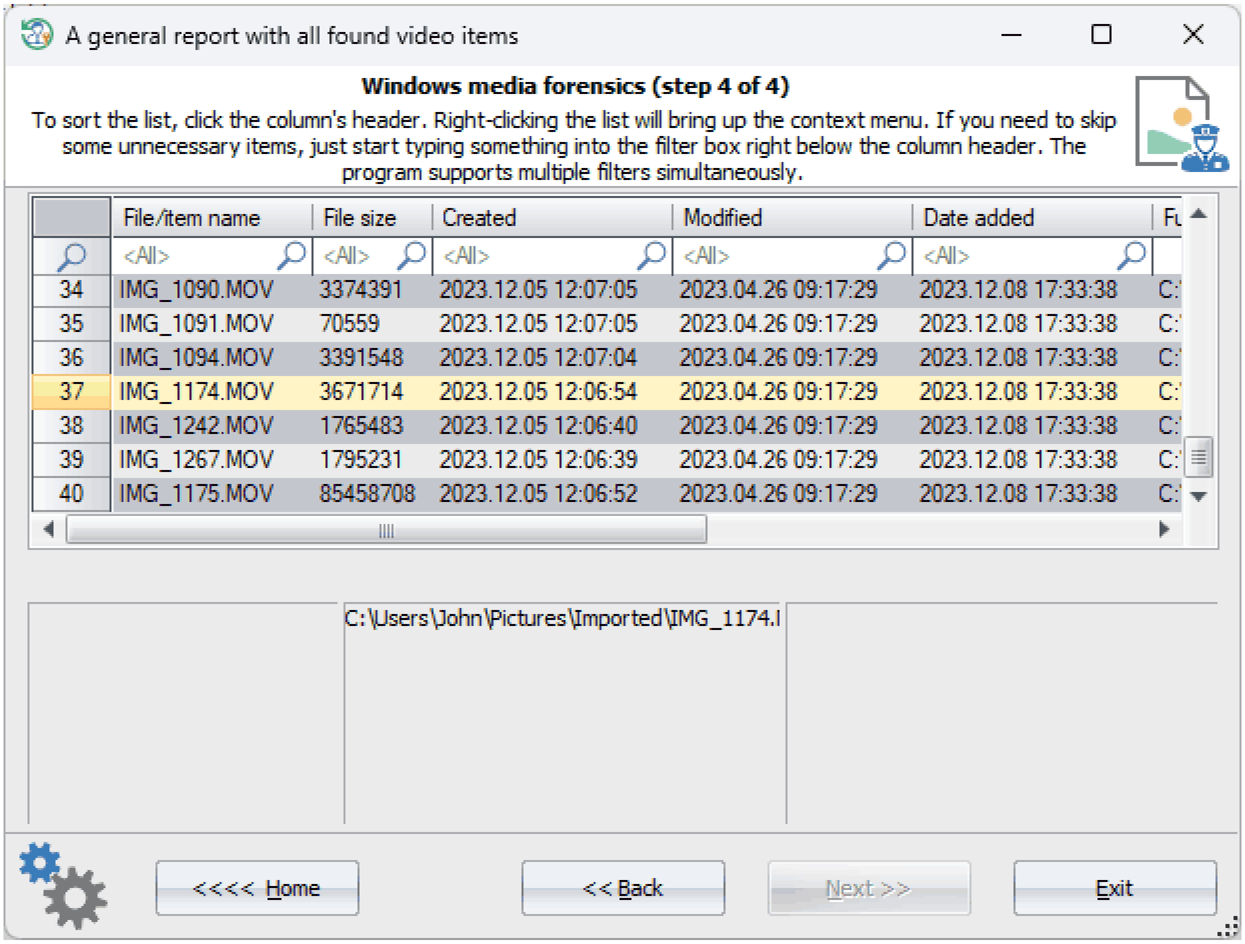
Photos taken at selected date: tsb.gif

tsb.gif
PeopleHDRBackground_AppleiPhone13Pro_DxOMark_05-00.jpeg

C:\Users\Admi

This report groups the photos and images by the date they were taken. In the table, you can choose to group them by years or months and inspect which photos were taken during the selected period.

3.7.3.4.4 Video items



A general report with all found video items

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	File/item name	File size	Created	Modified	Date added	Fu
	<All>	<All>	<All>	<All>	<All>	
34	IMG_1090.MOV	3374391	2023.12.05 12:07:05	2023.04.26 09:17:29	2023.12.08 17:33:38	C:\
35	IMG_1091.MOV	70559	2023.12.05 12:07:05	2023.04.26 09:17:29	2023.12.08 17:33:38	C:\
36	IMG_1094.MOV	3391548	2023.12.05 12:07:04	2023.04.26 09:17:29	2023.12.08 17:33:38	C:\
37	IMG_1174.MOV	3671714	2023.12.05 12:06:54	2023.04.26 09:17:29	2023.12.08 17:33:38	C:\
38	IMG_1242.MOV	1765483	2023.12.05 12:06:40	2023.04.26 09:17:29	2023.12.08 17:33:38	C:\
39	IMG_1267.MOV	1795231	2023.12.05 12:06:39	2023.04.26 09:17:29	2023.12.08 17:33:38	C:\
40	IMG_1175.MOV	85458708	2023.12.05 12:06:52	2023.04.26 09:17:29	2023.12.08 17:33:38	C:\

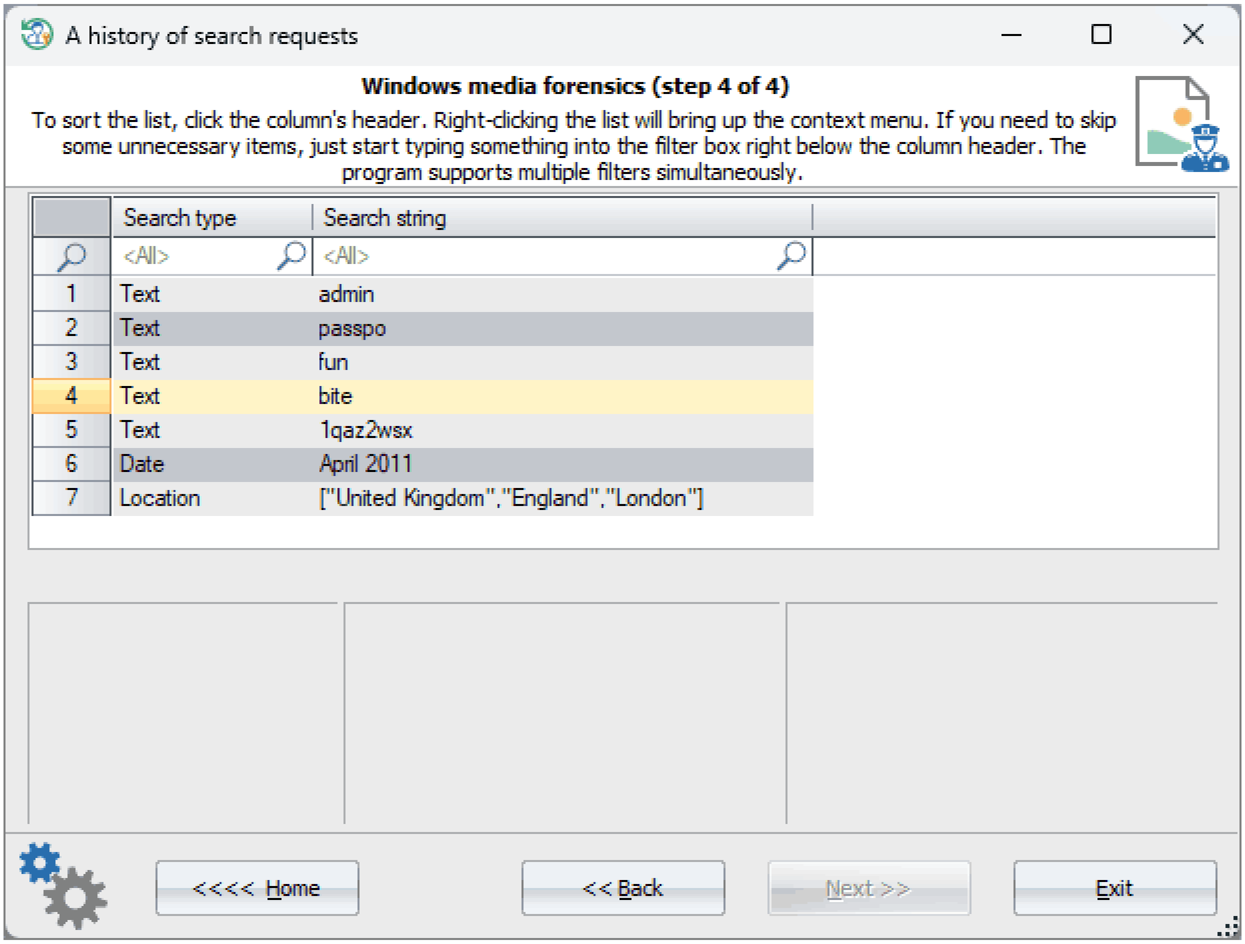
C:\Users\John\Pictures\Imported\IMG_1174.I

The video report includes information about the video elements stored in the **Photos**. Namely:

- Video file name
- File size
- Date of creation and last modification
- Full path on the disk
- Video duration

3.7.3.5 Photo library actions

3.7.3.5.1 Search history



Windows media forensics (step 4 of 4)

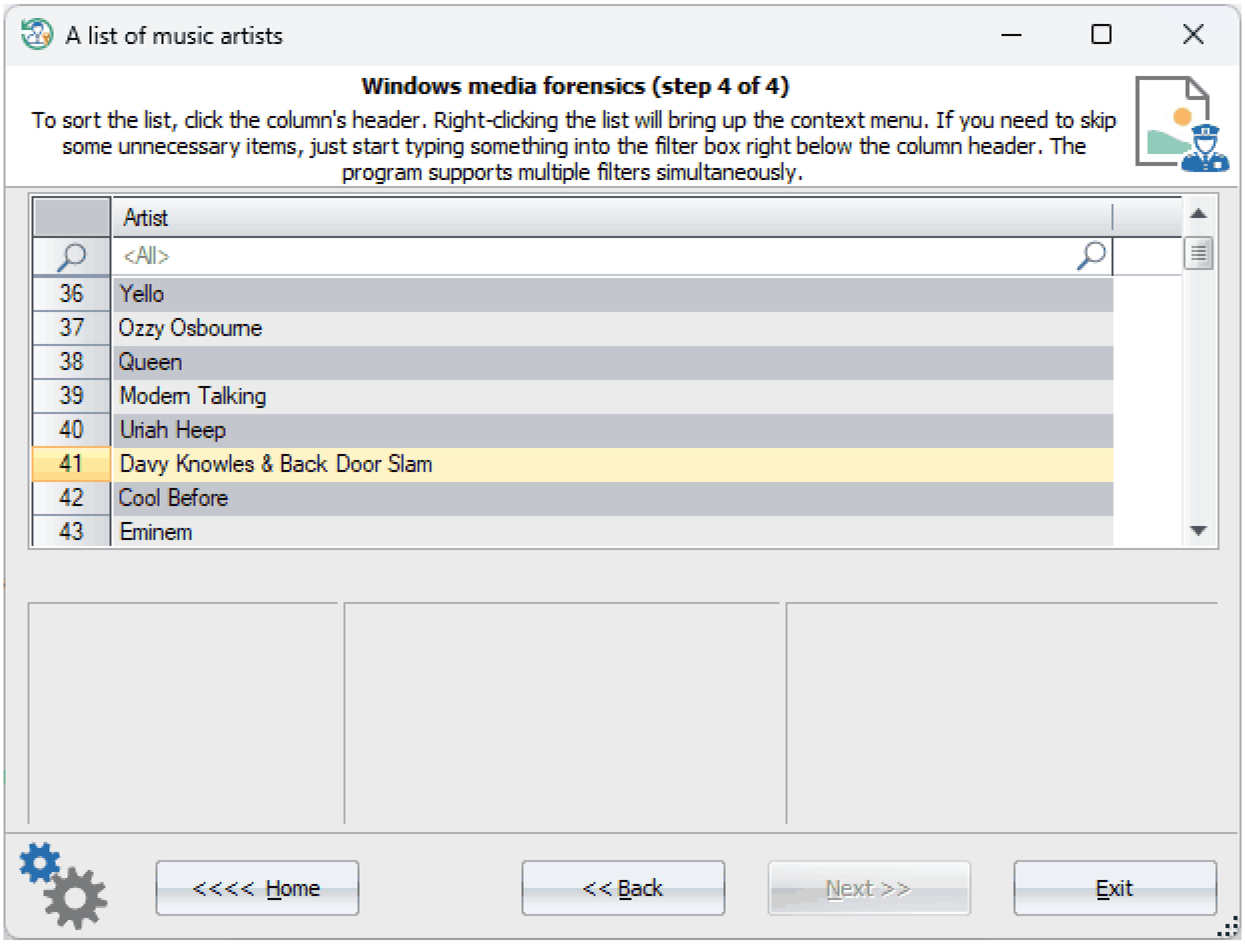
To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Search type	Search string
	<All>	<All>
1	Text	admin
2	Text	passpo
3	Text	fun
4	Text	bite
5	Text	1qaz2wsx
6	Date	April 2011
7	Location	["United Kingdom","England","London"]

A history of search queries performed in the **Photos** application.

3.7.3.6 Media Player library

3.7.3.6.1 Artists



A list of music artists

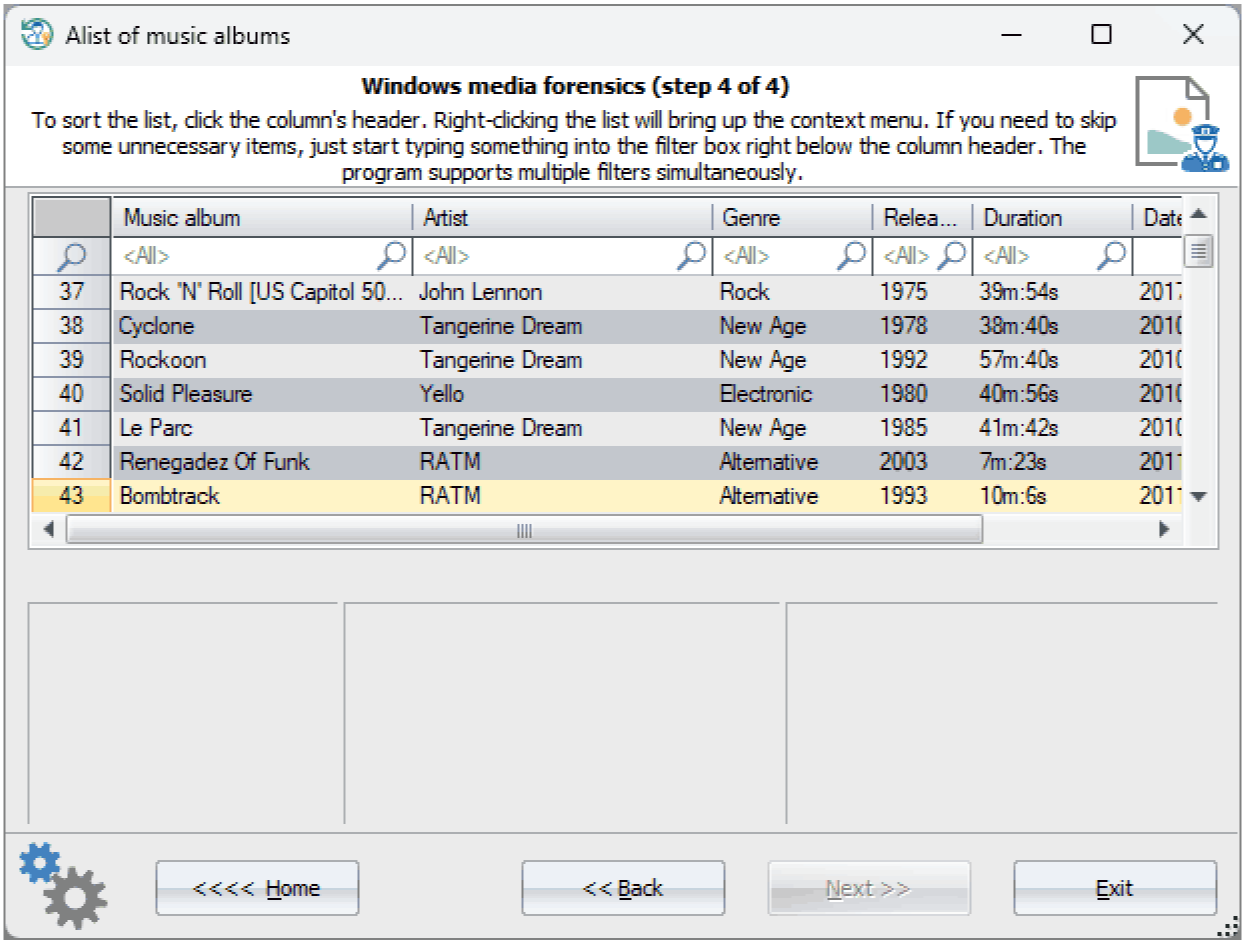
Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Artist
	<All>
36	Yello
37	Ozzy Osbourne
38	Queen
39	Modern Talking
40	Uriah Heep
41	Davy Knowles & Back Door Slam
42	Cool Before
43	Eminem

This report contains a list of artists stored in the **Media Player** (not Windows Media Player).

3.7.3.6.2 Albums



Windows media forensics (step 4 of 4)

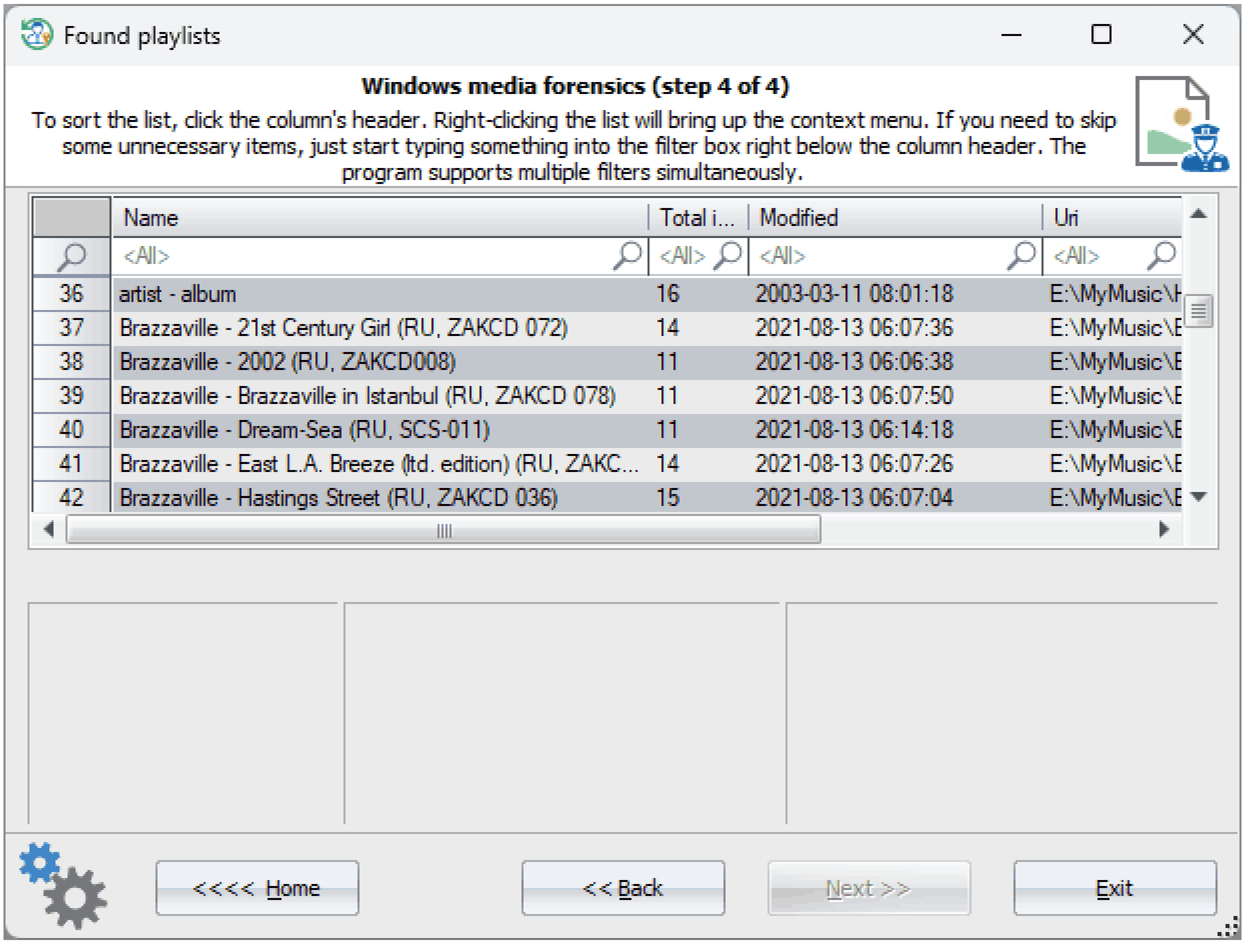
To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Music album	Artist	Genre	Relea...	Duration	Date
	<All>	<All>	<All>	<All>	<All>	
37	Rock 'N' Roll [US Capitol 50...	John Lennon	Rock	1975	39m:54s	2017
38	Cyclone	Tangerine Dream	New Age	1978	38m:40s	2010
39	Rockoon	Tangerine Dream	New Age	1992	57m:40s	2010
40	Solid Pleasure	Yello	Electronic	1980	40m:56s	2010
41	Le Parc	Tangerine Dream	New Age	1985	41m:42s	2010
42	Renegadez Of Funk	RATM	Alternative	2003	7m:23s	2011
43	Bombtrack	RATM	Alternative	1993	10m:6s	2011

The full list of all albums stored in the **Media Player**. This table contains:

- Music album
- Artist
- Genre
- Release date
- Duration of the album
- Data it was added to computer

3.7.3.6.3 Playlists



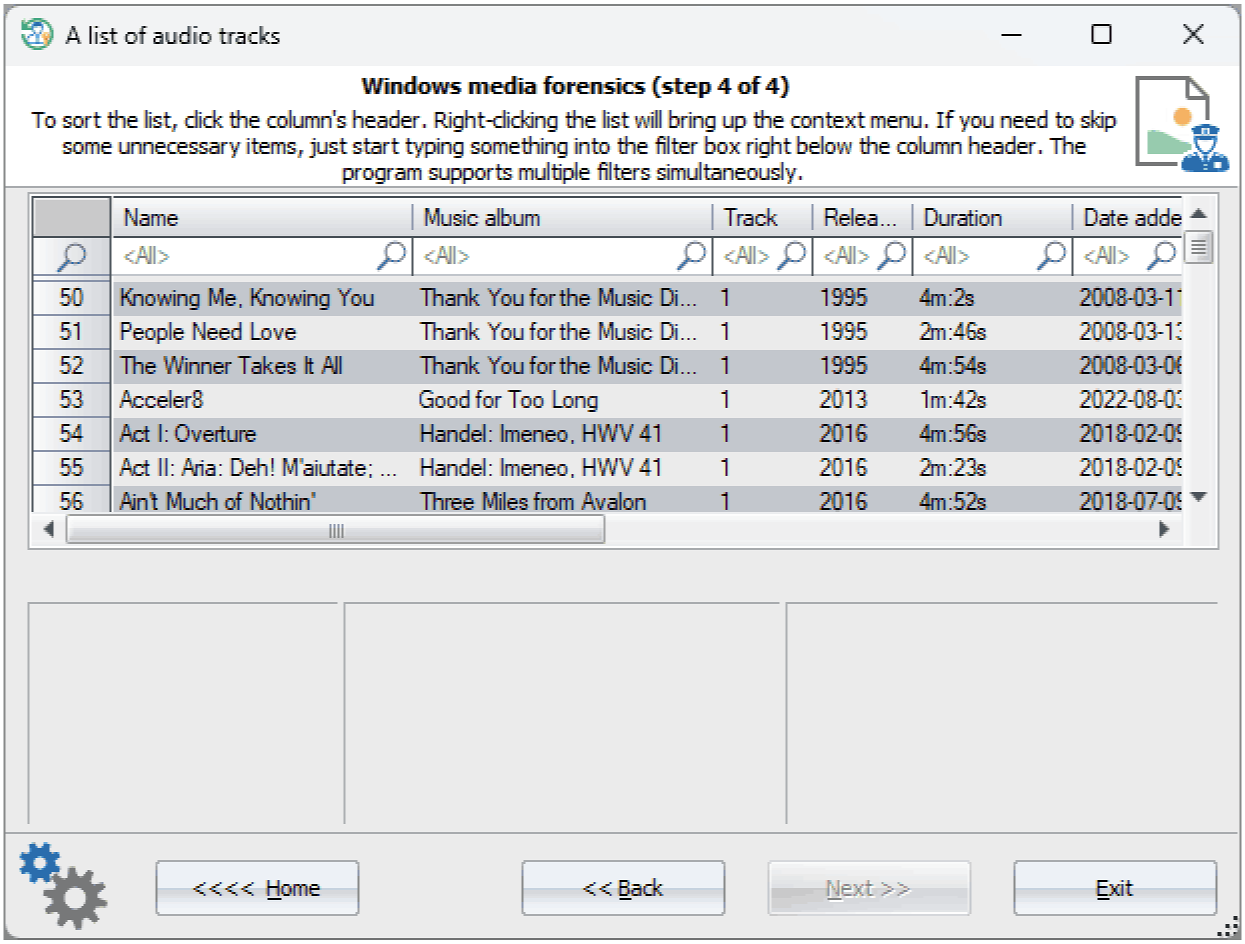
Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Name	Total i...	Modified	Uri
	<All>	<All>	<All>	<All>
36	artist - album	16	2003-03-11 08:01:18	E:\MyMusic\H
37	Brazzaville - 21st Century Girl (RU, ZAKCD 072)	14	2021-08-13 06:07:36	E:\MyMusic\E
38	Brazzaville - 2002 (RU, ZAKCD008)	11	2021-08-13 06:06:38	E:\MyMusic\E
39	Brazzaville - Brazzaville in Istanbul (RU, ZAKCD 078)	11	2021-08-13 06:07:50	E:\MyMusic\E
40	Brazzaville - Dream-Sea (RU, SCS-011)	11	2021-08-13 06:14:18	E:\MyMusic\E
41	Brazzaville - East L.A. Breeze (ltd. edition) (RU, ZAKC...	14	2021-08-13 06:07:26	E:\MyMusic\E
42	Brazzaville - Hastings Street (RU, ZAKCD 036)	15	2021-08-13 06:07:04	E:\MyMusic\E

A list of all playlists stored in the **Media Player**.

3.7.3.6.4 Audio tracks



Windows media forensics (step 4 of 4)

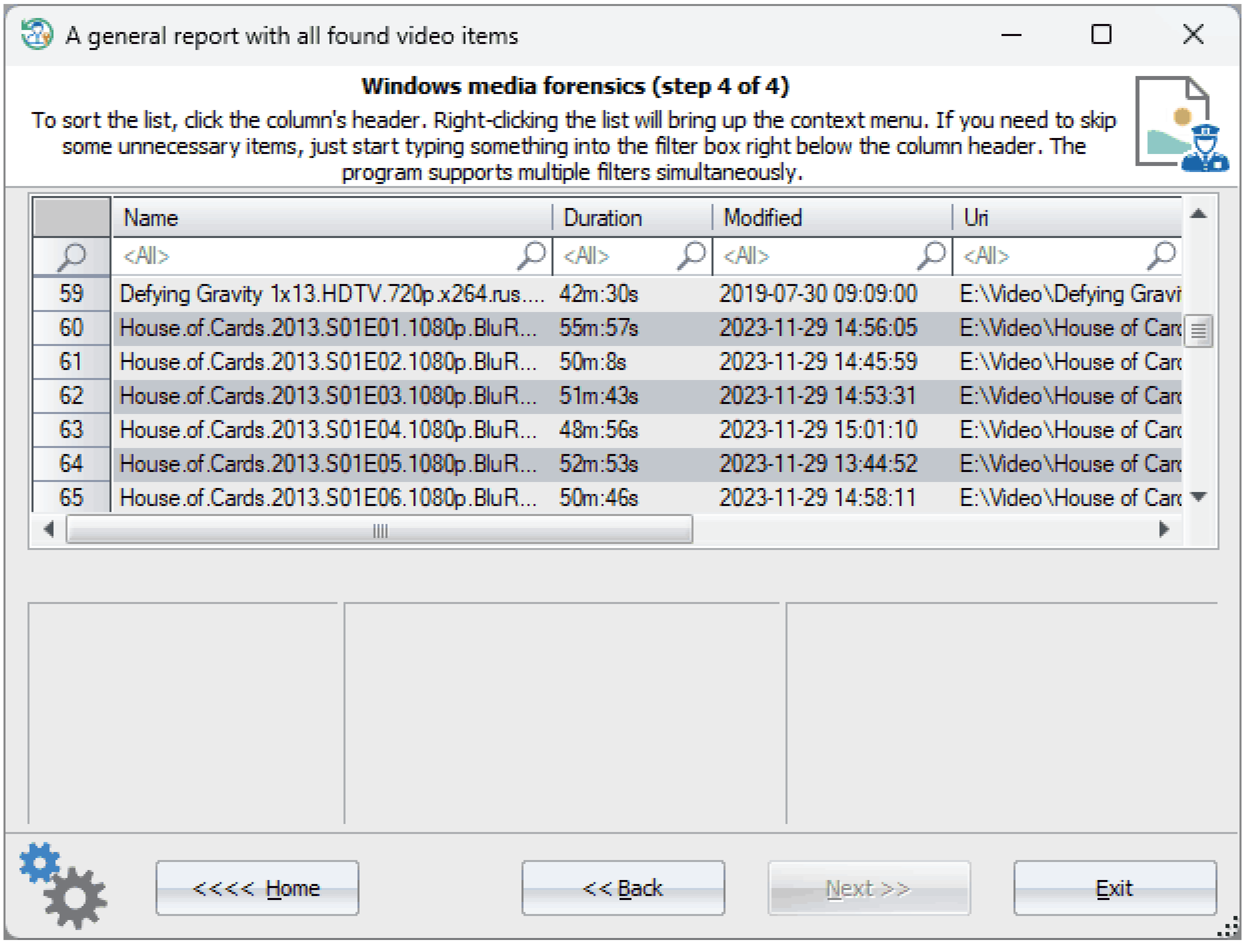
To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Name	Music album	Track	Relea...	Duration	Date adde
	<All>	<All>	<All>	<All>	<All>	<All>
50	Knowing Me, Knowing You	Thank You for the Music Di...	1	1995	4m:2s	2008-03-11
51	People Need Love	Thank You for the Music Di...	1	1995	2m:46s	2008-03-13
52	The Winner Takes It All	Thank You for the Music Di...	1	1995	4m:54s	2008-03-06
53	Acceler8	Good for Too Long	1	2013	1m:42s	2022-08-03
54	Act I: Overture	Handel: Imeneo, HWV 41	1	2016	4m:56s	2018-02-09
55	Act II: Aria: Deh! M'aiutate; ...	Handel: Imeneo, HWV 41	1	2016	2m:23s	2018-02-09
56	Ain't Much of Nothin'	Three Miles from Avalon	1	2016	4m:52s	2018-07-09

The **Audio tracks** report Includes the following information:

- Track name
- Album
- Track position in the album
- Album released date
- Track duration
- Date added to the computer
- Audio format
- Full path to the track

3.7.3.6.5 Video items



A general report with all found video items

Windows media forensics (step 4 of 4)

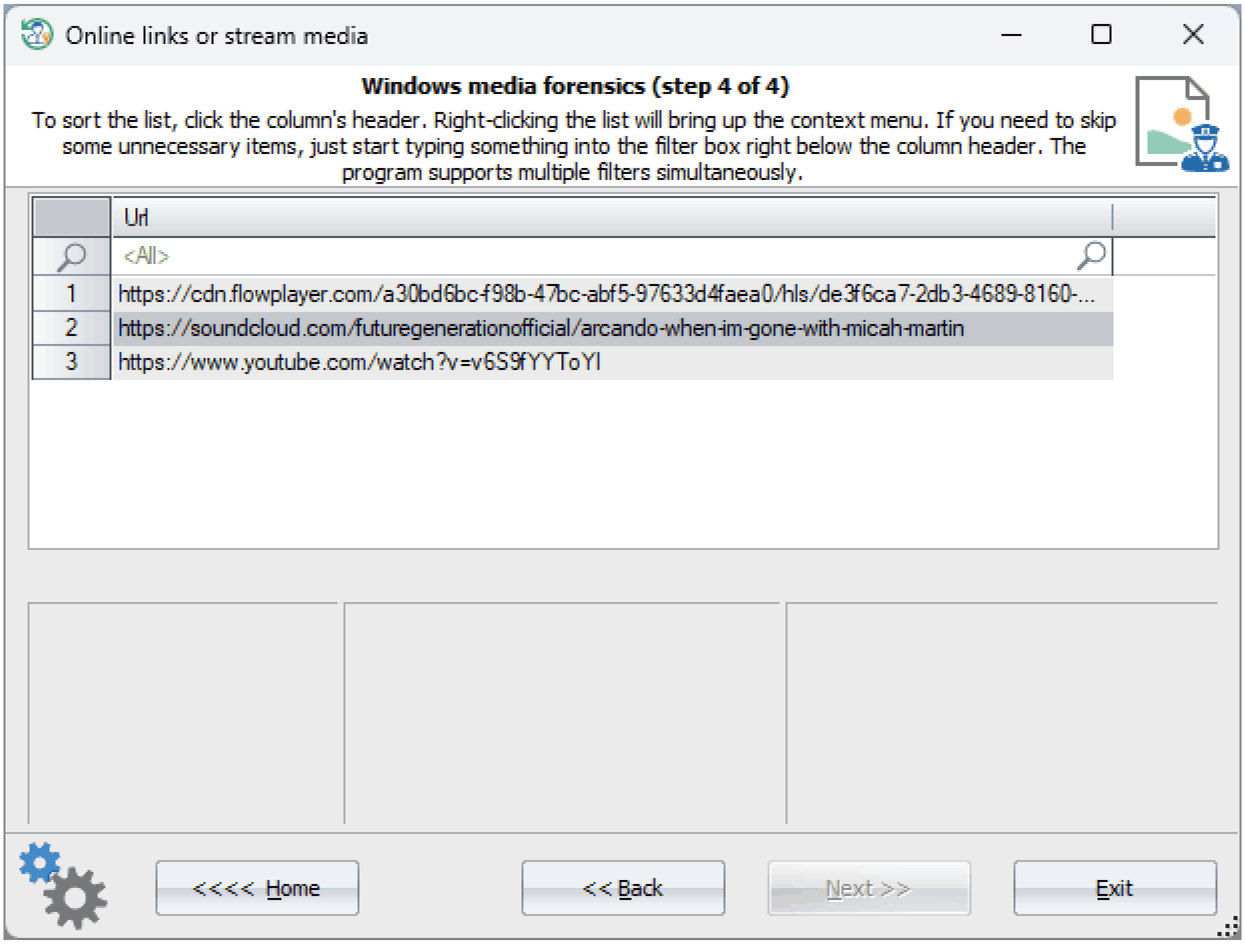
To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Name	Duration	Modified	Uri
	<All>	<All>	<All>	<All>
59	Defying Gravity 1x13.HDTV.720p.x264.rus....	42m:30s	2019-07-30 09:09:00	E:\Video\Defying Gravi
60	House.of.Cards.2013.S01E01.1080p.BluR...	55m:57s	2023-11-29 14:56:05	E:\Video\House of Carc
61	House.of.Cards.2013.S01E02.1080p.BluR...	50m:8s	2023-11-29 14:45:59	E:\Video\House of Carc
62	House.of.Cards.2013.S01E03.1080p.BluR...	51m:43s	2023-11-29 14:53:31	E:\Video\House of Carc
63	House.of.Cards.2013.S01E04.1080p.BluR...	48m:56s	2023-11-29 15:01:10	E:\Video\House of Carc
64	House.of.Cards.2013.S01E05.1080p.BluR...	52m:53s	2023-11-29 13:44:52	E:\Video\House of Carc
65	House.of.Cards.2013.S01E06.1080p.BluR...	50m:46s	2023-11-29 14:58:11	E:\Video\House of Carc

This report contains information about video elements stored by the **Media Player** application. Namely:

- Video name
- Duration
- Date of the last modification
- Full path to the file

3.7.3.6.6 URLs



Windows media forensics (step 4 of 4)

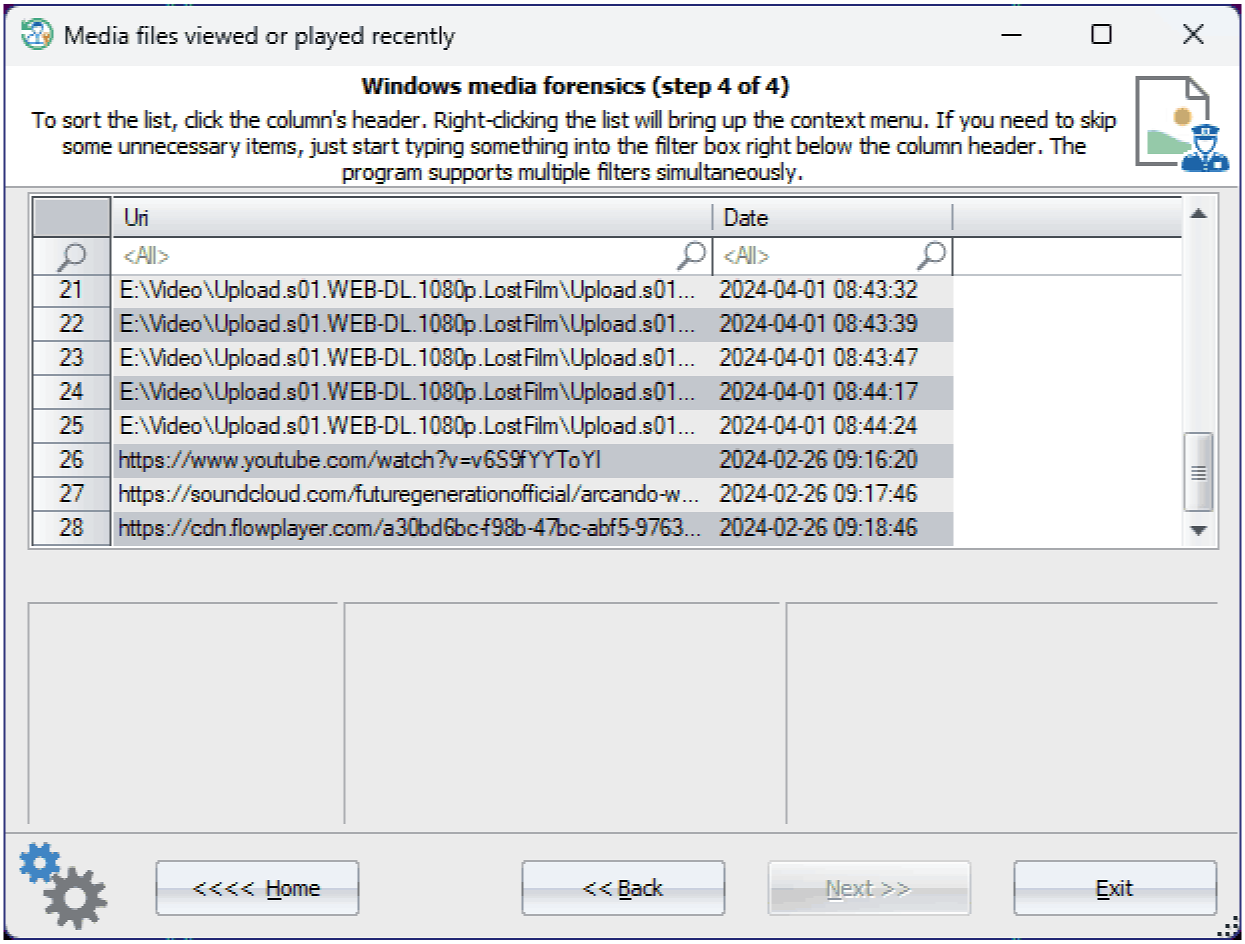
To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Url
	<All>
1	https://cdn.flowplayer.com/a30bd6bc-f98b-47bc-abf5-97633d4faea0/hls/de3f6ca7-2db3-4689-8160-...
2	https://soundcloud.com/futuregenerationofficial/arcando-when-im-gone-with-micah-martin
3	https://www.youtube.com/watch?v=v6S9fYYToYI

This report includes links to online or streaming videos stored in **Media Player**.

3.7.3.7 Media Player library actions

3.7.3.7.1 Played recently



Media files viewed or played recently

Windows media forensics (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Uri	Date
	<All>	<All>
21	E:\Video\Upload.s01.WEB-DL.1080p.LostFilm\Upload.s01...	2024-04-01 08:43:32
22	E:\Video\Upload.s01.WEB-DL.1080p.LostFilm\Upload.s01...	2024-04-01 08:43:39
23	E:\Video\Upload.s01.WEB-DL.1080p.LostFilm\Upload.s01...	2024-04-01 08:43:47
24	E:\Video\Upload.s01.WEB-DL.1080p.LostFilm\Upload.s01...	2024-04-01 08:44:17
25	E:\Video\Upload.s01.WEB-DL.1080p.LostFilm\Upload.s01...	2024-04-01 08:44:24
26	https://www.youtube.com/watch?v=v6S9fYYToYI	2024-02-26 09:16:20
27	https://soundcloud.com/futuregenerationofficial/arcando-w...	2024-02-26 09:17:46
28	https://cdn.flowplayer.com/a30bd6bc-f98b-47bc-abf5-9763...	2024-02-26 09:18:46

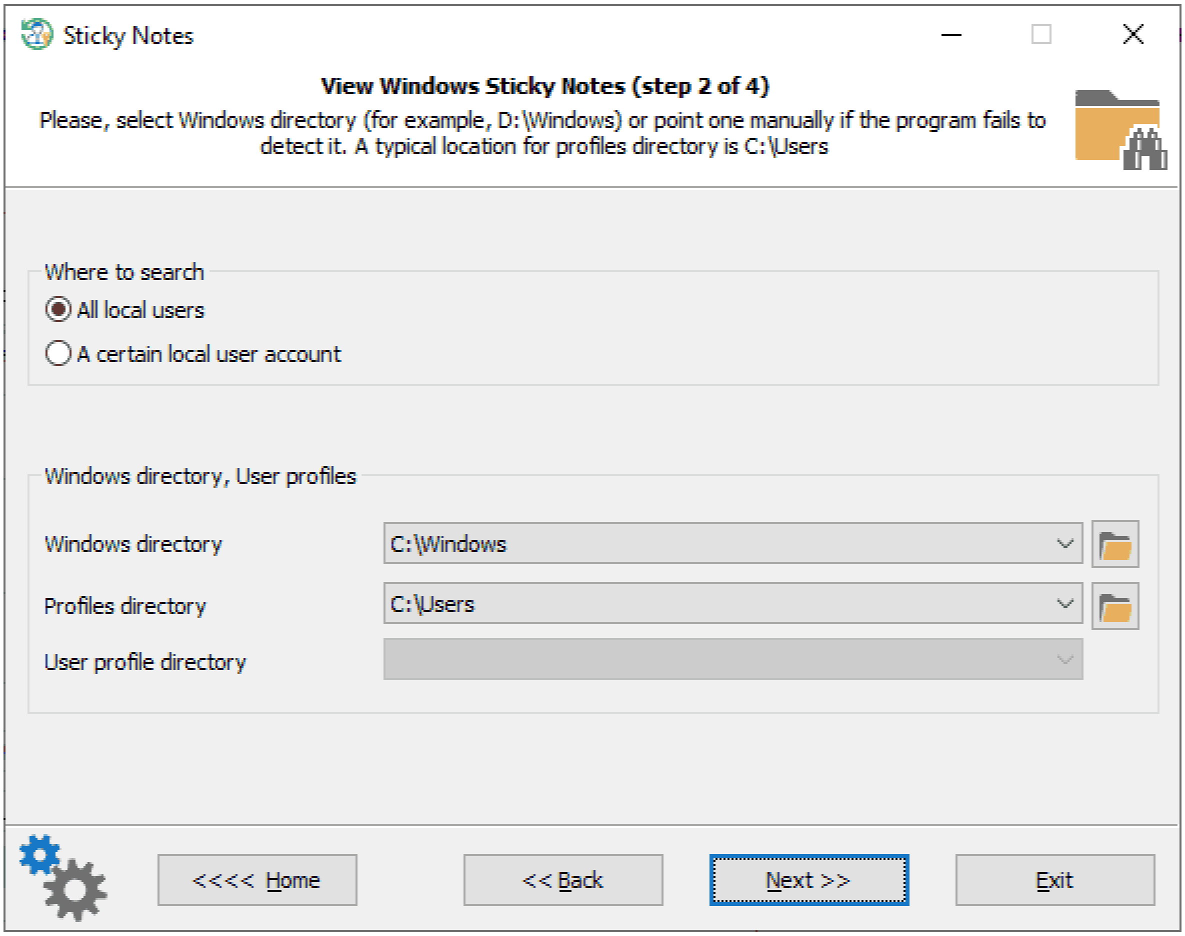
Media files viewed or played recently.

3.7.4 Sticky notes

Sticky Notes is a Microsoft application that became a part of Windows OS starting with Windows Vista. The application allows users to quickly take notes and stick them on their desktop.

The Reset Windows Password extracts and displays all stored as well as some deleted notes, including the text format, color and pictures. All local users are supported and all OSes (the notes are stored in different places depending on OS version).

Selecting user account



Sticky Notes

View Windows Sticky Notes (step 2 of 4)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it. A typical location for profiles directory is C:\Users

Where to search

● All local users

○ A certain local user account

Windows directory, User profiles

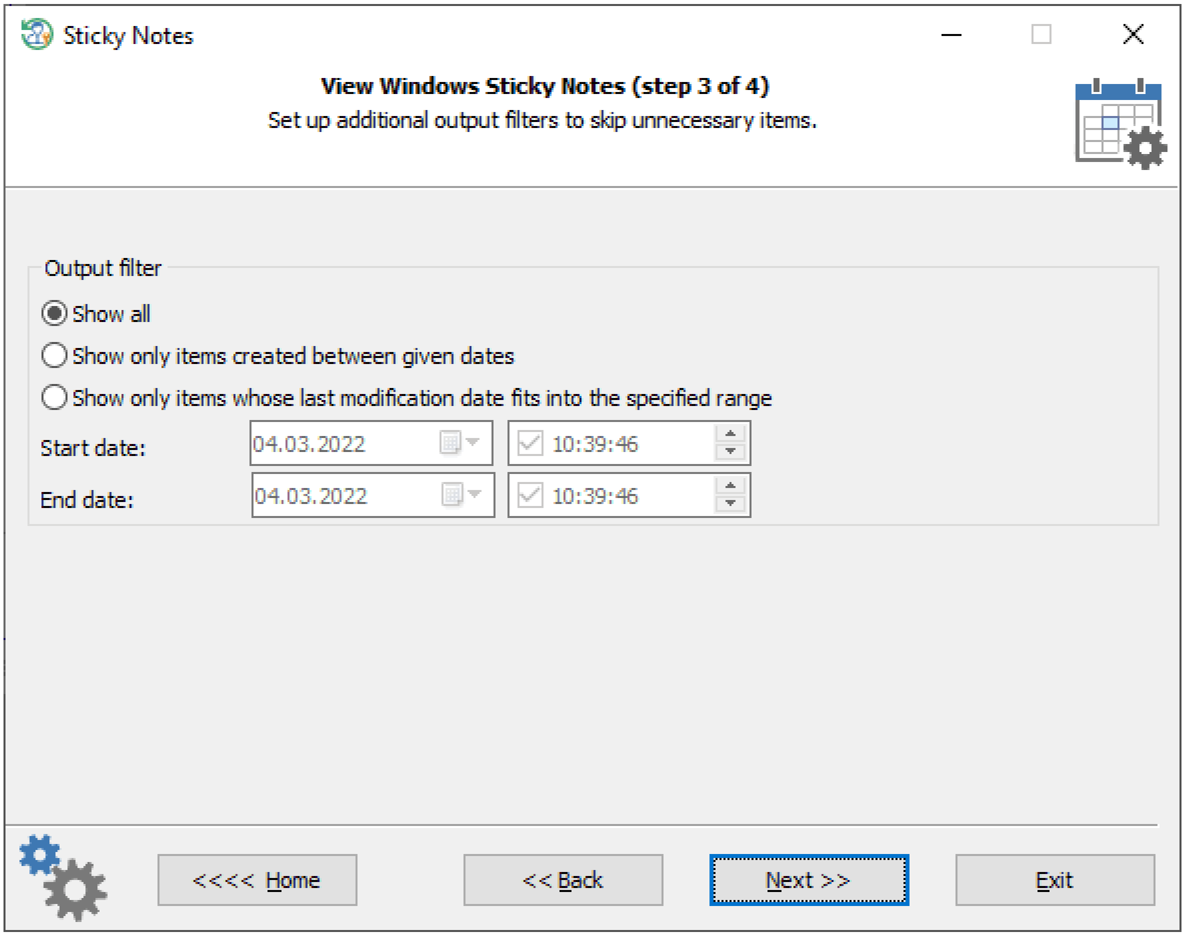
Windows directory: C:\Windows

Profiles directory: C:\Users

User profile directory:

On the first dialog, the program offers to choose the user account on which sticky notes you need to extract. By default, all local users are set.

Setting time filters



Sticky Notes

View Windows Sticky Notes (step 3 of 4)

Set up additional output filters to skip unnecessary items.

Output filter

● Show all

○ Show only items created between given dates

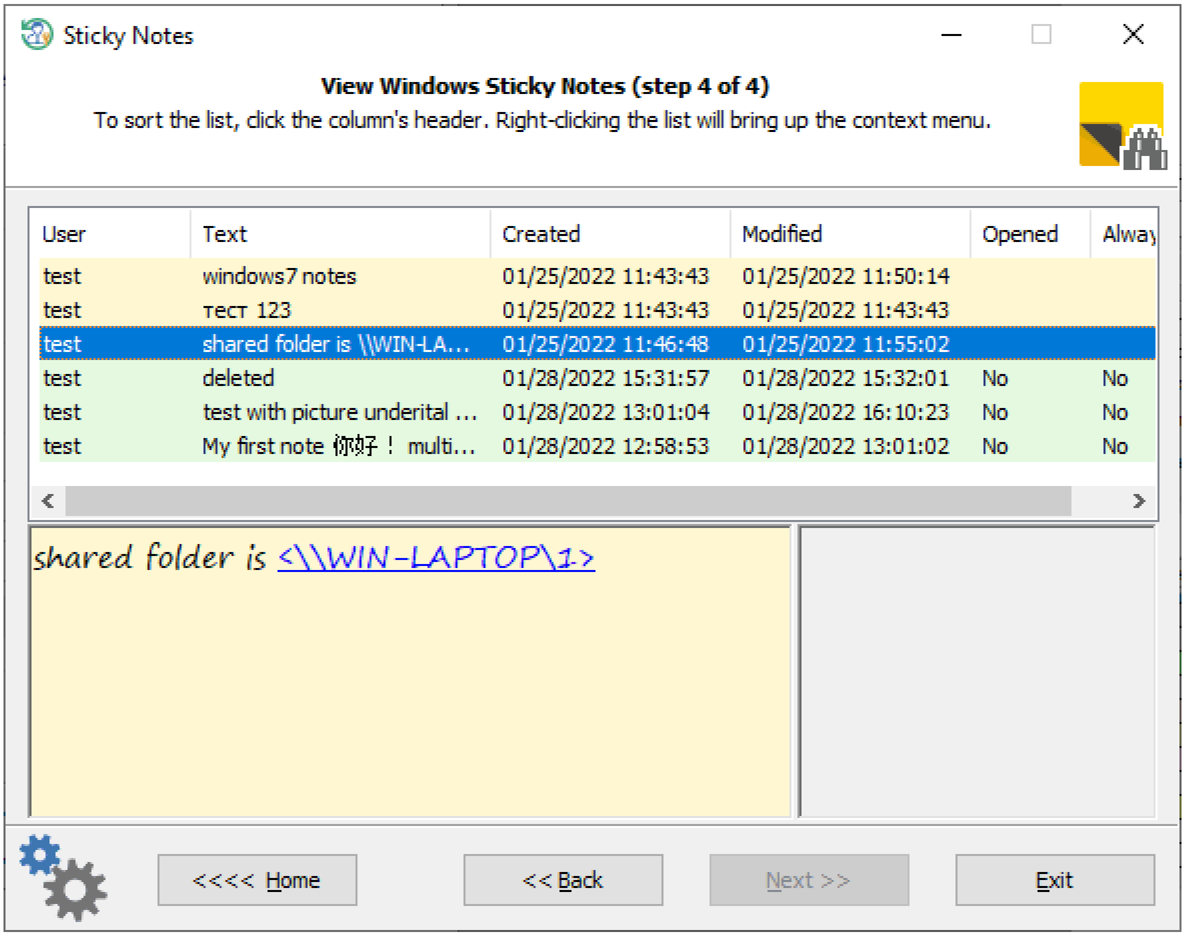
○ Show only items whose last modification date fits into the specified range

Start date: 04.03.2022 ☑ 10:39:46

End date: 04.03.2022 ☑ 10:39:46

Too many sticky notes can be ordered by setting up time filters and displaying notes sorted out by their creation or last modification dates.

Windows sticky notes



View Windows Sticky Notes (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu.

User	Text	Created	Modified	Opened	Alway
test	windows7 notes	01/25/2022 11:43:43	01/25/2022 11:50:14		
test	тест 123	01/25/2022 11:43:43	01/25/2022 11:43:43		
test	shared folder is \\WIN-LA...	01/25/2022 11:46:48	01/25/2022 11:55:02		
test	deleted	01/28/2022 15:31:57	01/28/2022 15:32:01	No	No
test	test with picture underital ...	01/28/2022 13:01:04	01/28/2022 16:10:23	No	No
test	My first note 你好！ multi...	01/28/2022 12:58:53	01/28/2022 13:01:02	No	No

shared folder is <\\WIN-LAPTOP\1>

The program sets the color of each sticky note as they were initially created. Windows 10 enhanced notes with pictures are supported as well. The pictures, if any, are displayed on the right part of the primary text box. All found notes can be copied to the clipboard or saved to a textual report.

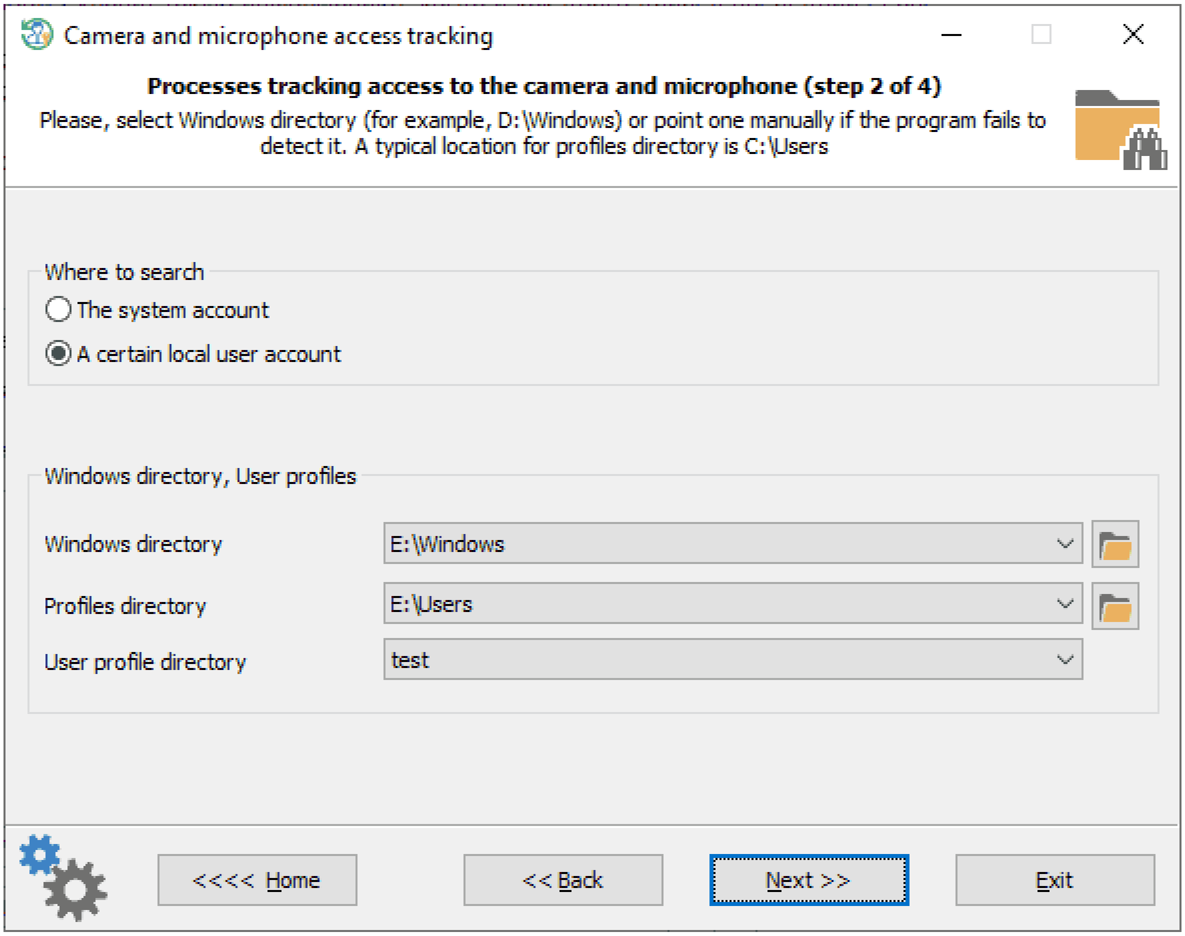
3.7.5 Camera and microphone access tracking

Using this forensic investigation feature you can figure out easily what program or process was using the microphone or camera (as well as some additional devices like location sensors, if Windows stores the history), when and how long was the last activity session.

Windows stores the tracking information in the following registry keys:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\microphone
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\webcam

This tool can also be used to detect a rat-like behavior of any malicious processes or programs accessing the hardware secretly.

Choosing user account



Camera and microphone access tracking

Processes tracking access to the camera and microphone (step 2 of 4)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it. A typical location for profiles directory is C:\Users

Where to search

○ The system account

● A certain local user account

Windows directory, User profiles

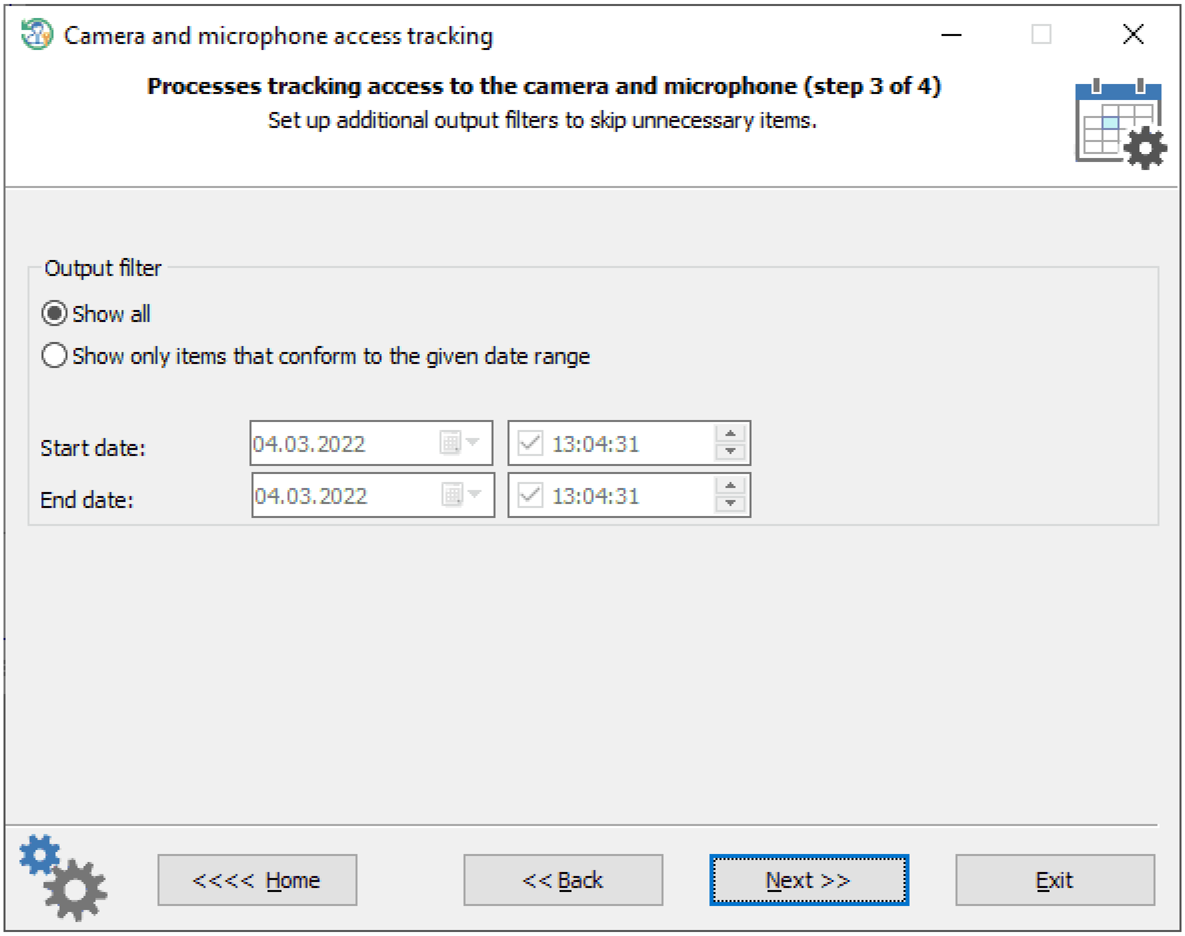
Windows directory: E:\Windows

Profiles directory: E:\Users

User profile directory: test

In order to extract the camera\microphone tracking information, you need to choose a user account first.

Time filters



Camera and microphone access tracking

Processes tracking access to the camera and microphone (step 3 of 4)

Set up additional output filters to skip unnecessary items.

Output filter

● Show all

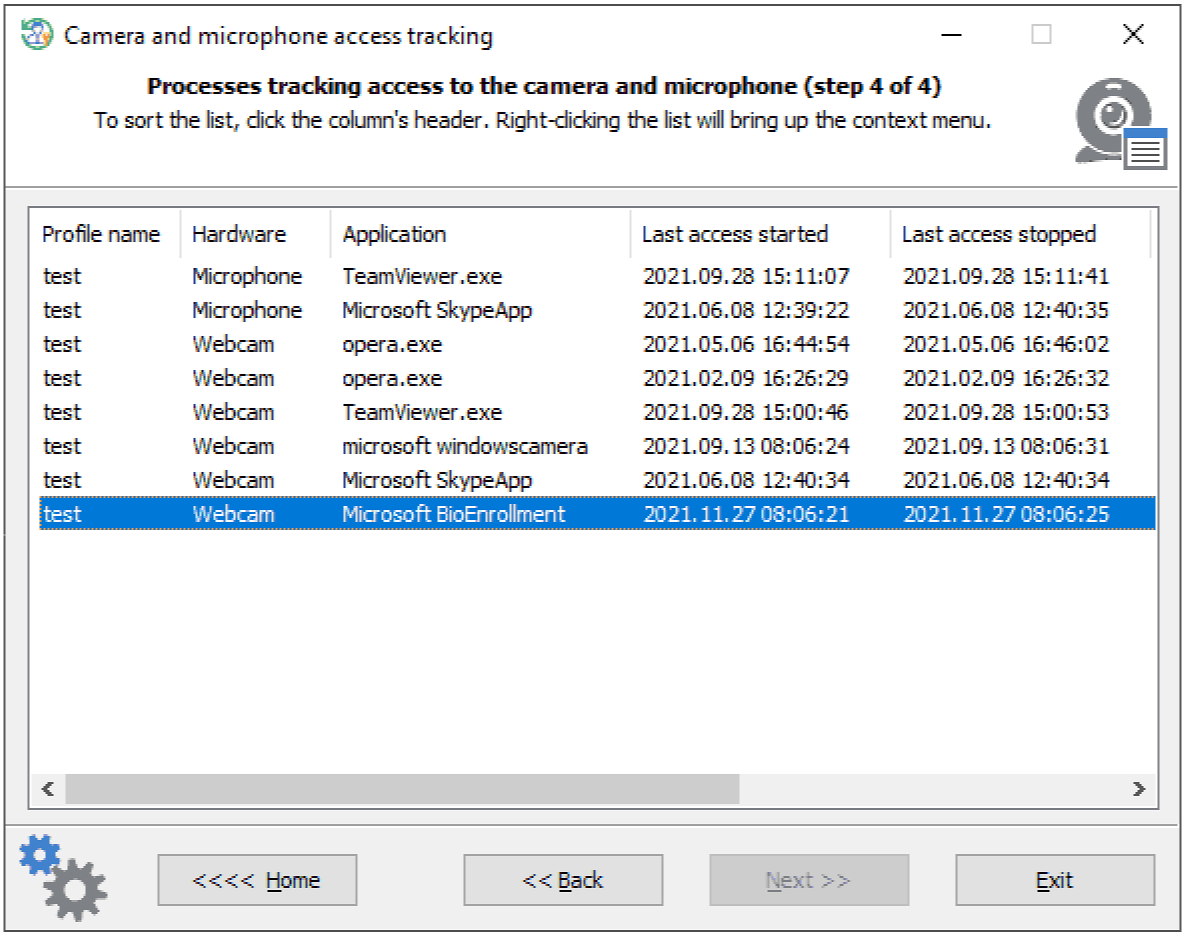
○ Show only items that conform to the given date range

Start date: 04.03.2022 ☑ 13:04:31

End date: 04.03.2022 ☑ 13:04:31

You use the time filters to display a certain date or period only.

Camera and microphone access tracking



Processes tracking access to the camera and microphone (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu.

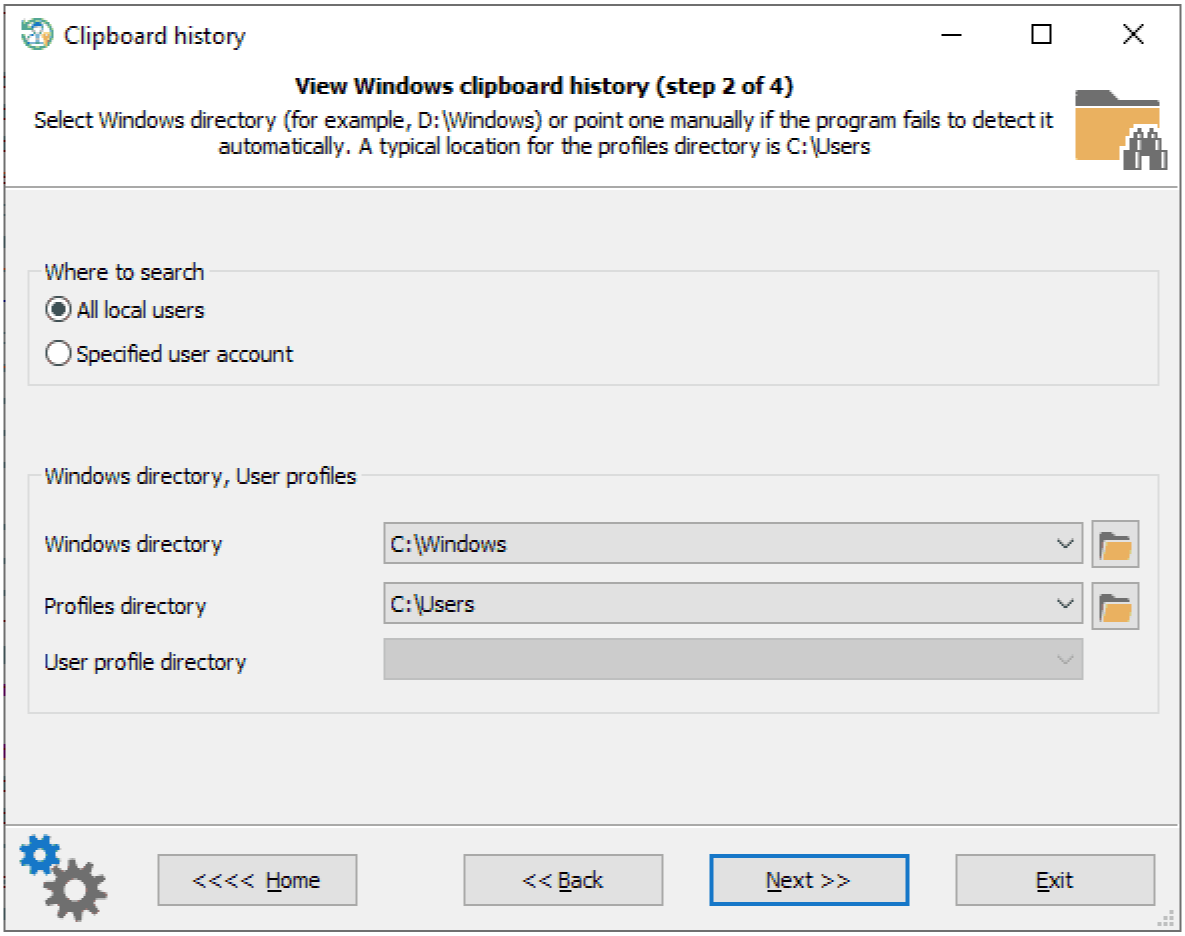
Profile name	Hardware	Application	Last access started	Last access stopped
test	Microphone	TeamViewer.exe	2021.09.28 15:11:07	2021.09.28 15:11:41
test	Microphone	Microsoft SkypeApp	2021.06.08 12:39:22	2021.06.08 12:40:35
test	Webcam	opera.exe	2021.05.06 16:44:54	2021.05.06 16:46:02
test	Webcam	opera.exe	2021.02.09 16:26:29	2021.02.09 16:26:32
test	Webcam	TeamViewer.exe	2021.09.28 15:00:46	2021.09.28 15:00:53
test	Webcam	microsoft windowscamera	2021.09.13 08:06:24	2021.09.13 08:06:31
test	Webcam	Microsoft SkypeApp	2021.06.08 12:40:34	2021.06.08 12:40:34
test	Webcam	Microsoft BioEnrollment	2021.11.27 08:06:21	2021.11.27 08:06:25

Where appropriate, the program retrieves access information for any available hardware, like Bluetooth devices, not just the microphone or camera.

3.7.6 Clipboard history

The clipboard history tool extracts and decrypts text, pictures, and other data stored by Windows clipboard. The Windows clipboard is cleared out every time the user logs off the system. However, if the clipboard history option is on, the system preserves and saves the clipboard information. Thus, the data can be easily extracted and decrypted even after the system shutdown. This is what this new tool is for.

Selecting Windows clipboard user



Clipboard history

View Windows clipboard history (step 2 of 4)

Select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it automatically. A typical location for the profiles directory is C:\Users

Where to search

● All local users

○ Specified user account

Windows directory, User profiles

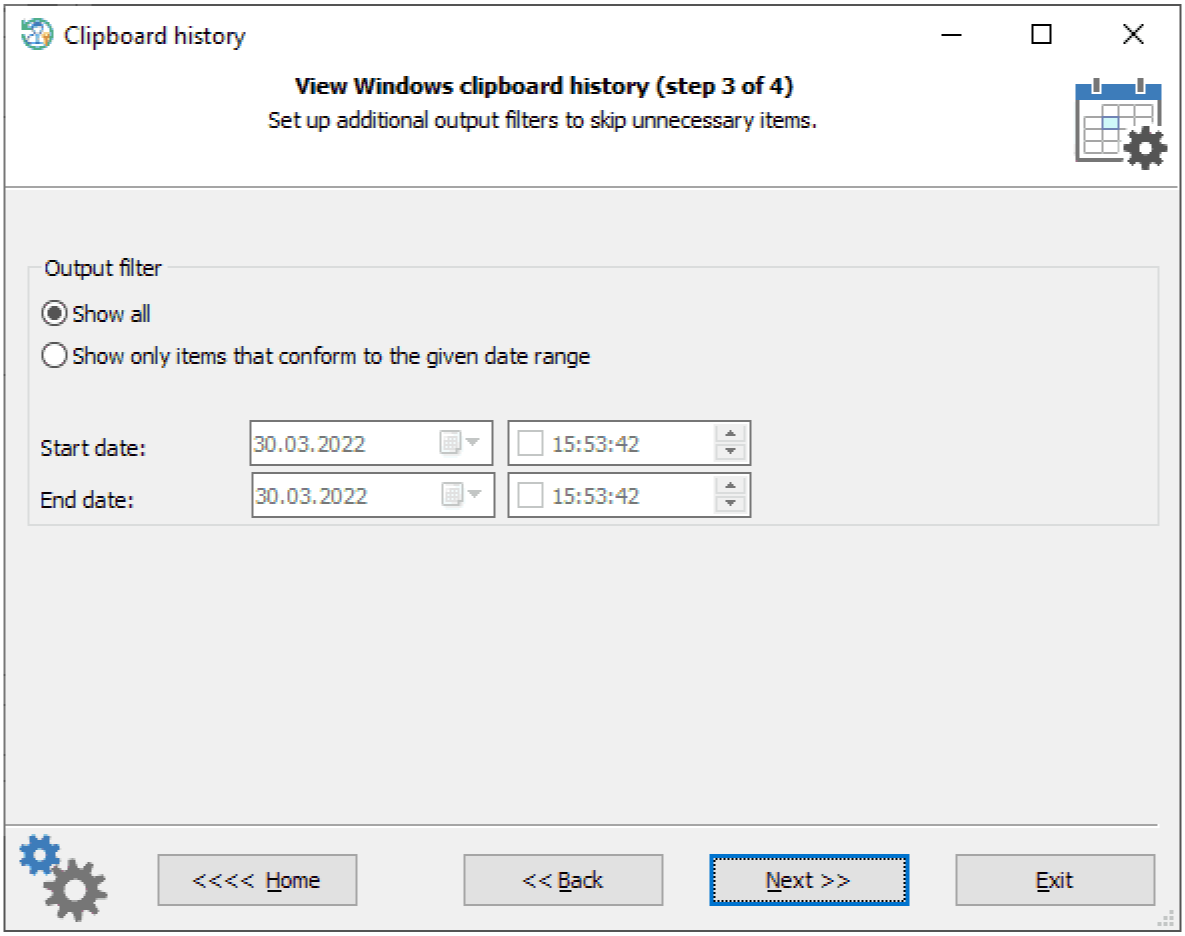
Windows directory: C:\Windows

Profiles directory: C:\Users

User profile directory:

Select the user account on which clipboard history you need to pull out. By default, all local users are set.

Setting clipboard time filters



View Windows clipboard history (step 3 of 4)

Set up additional output filters to skip unnecessary items.

Output filter

● Show all

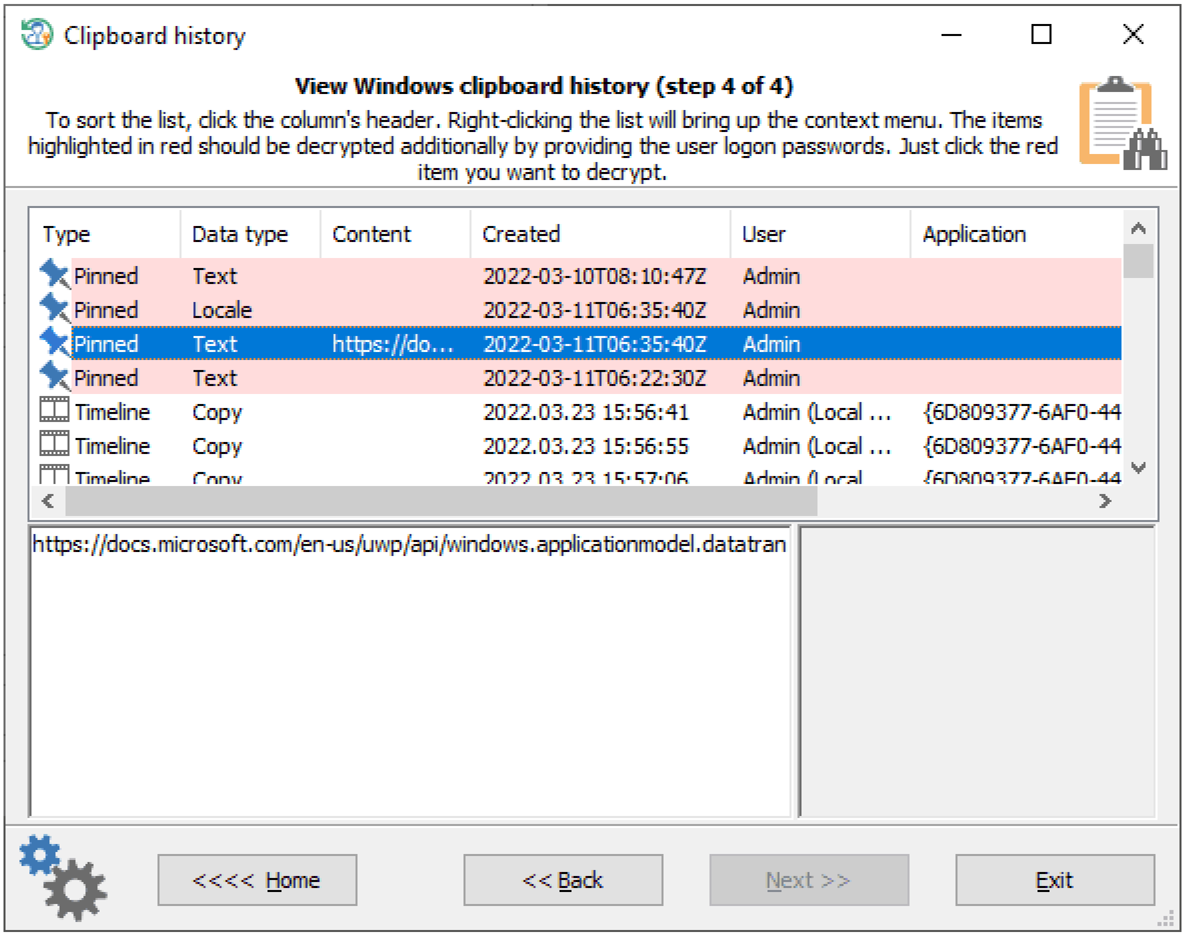
○ Show only items that conform to the given date range

Start date: 30.03.2022 □ 15:53:42

End date: 30.03.2022 □ 15:53:42

Set up time filters to skip showing unnecessary clipboard items.

Windows clipboard history



View Windows clipboard history (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. The items highlighted in red should be decrypted additionally by providing the user logon passwords. Just click the red item you want to decrypt.

Type	Data type	Content	Created	User	Application
Pinned	Text		2022-03-10T08:10:47Z	Admin	
Pinned	Locale		2022-03-11T06:35:40Z	Admin	
Pinned	Text	https://do...	2022-03-11T06:35:40Z	Admin	
Pinned	Text		2022-03-11T06:22:30Z	Admin	
Timeline	Copy		2022.03.23 15:56:41	Admin (Local ...	{6D809377-6AF0-44
Timeline	Copy		2022.03.23 15:56:55	Admin (Local ...	{6D809377-6AF0-44
Timeline	Copy		2022.03.23 15:57:06	Admin (Local	{6D809377-6AF0-44

https://docs.microsoft.com/en-us/uwp/api/windows.applicationmodel.datatran

The program supports 3 types of Windows clipboard location:

1. Clipboard items stored in Windows timeline database
2. Pinned clipboard history (requires additional decryption). To get an item pinned, invoke the clipboard history by pressing the Windows logo key + V and then selecting ‘Pin’ from the item’s context menu.
3. Clipboard sync data (may require additional decryption)

The **Copy/Paste** types in the ‘Data type’ column mean that there are no actual data exists (thus the **Content** column is always empty) but only a record on clipboard operation. The list of decrypted history contains some additional useful data, such as application and document name, where the clipboard operation took place, when this operation was completed and so on.

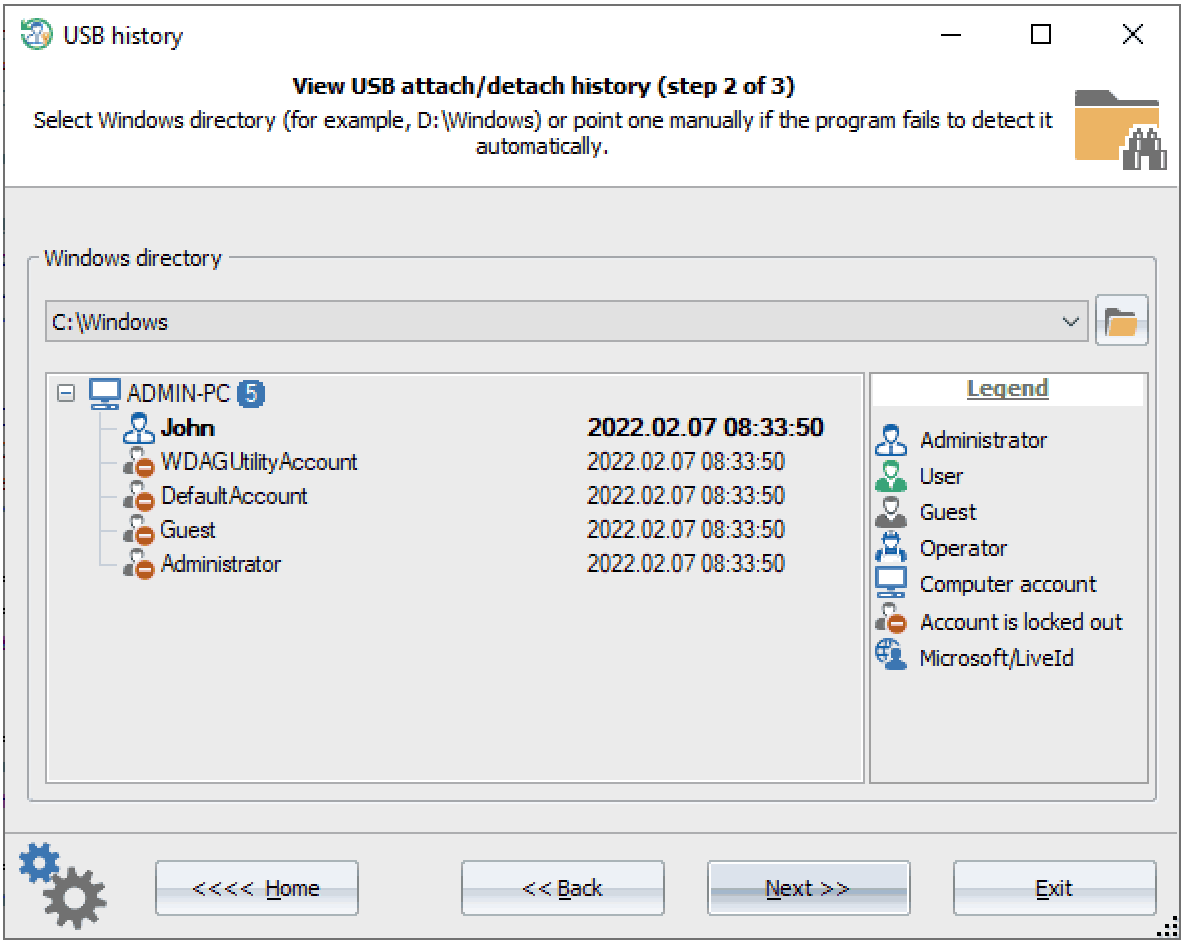
Decrypting some clipboard data may require the user logon password. Unnecessary though, if the user was the last person who had logged on to the system.

3.7.7 USB history

In forensics, it is often vital to find out what USB devices were connected to the computer and when. Since Windows stores traces of all connected or disconnected USB devices, it is quite simple to do this.

The USB history viewer allows you to extract the information on devices that were connected to the computer, their sizes, serial numbers, as well as other technical data, such as the partition table and the master boot record.

Selecting Operating System directory



USB history

View USB attach/detach history (step 2 of 3)

Select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it automatically.

Windows directory

C:\Windows

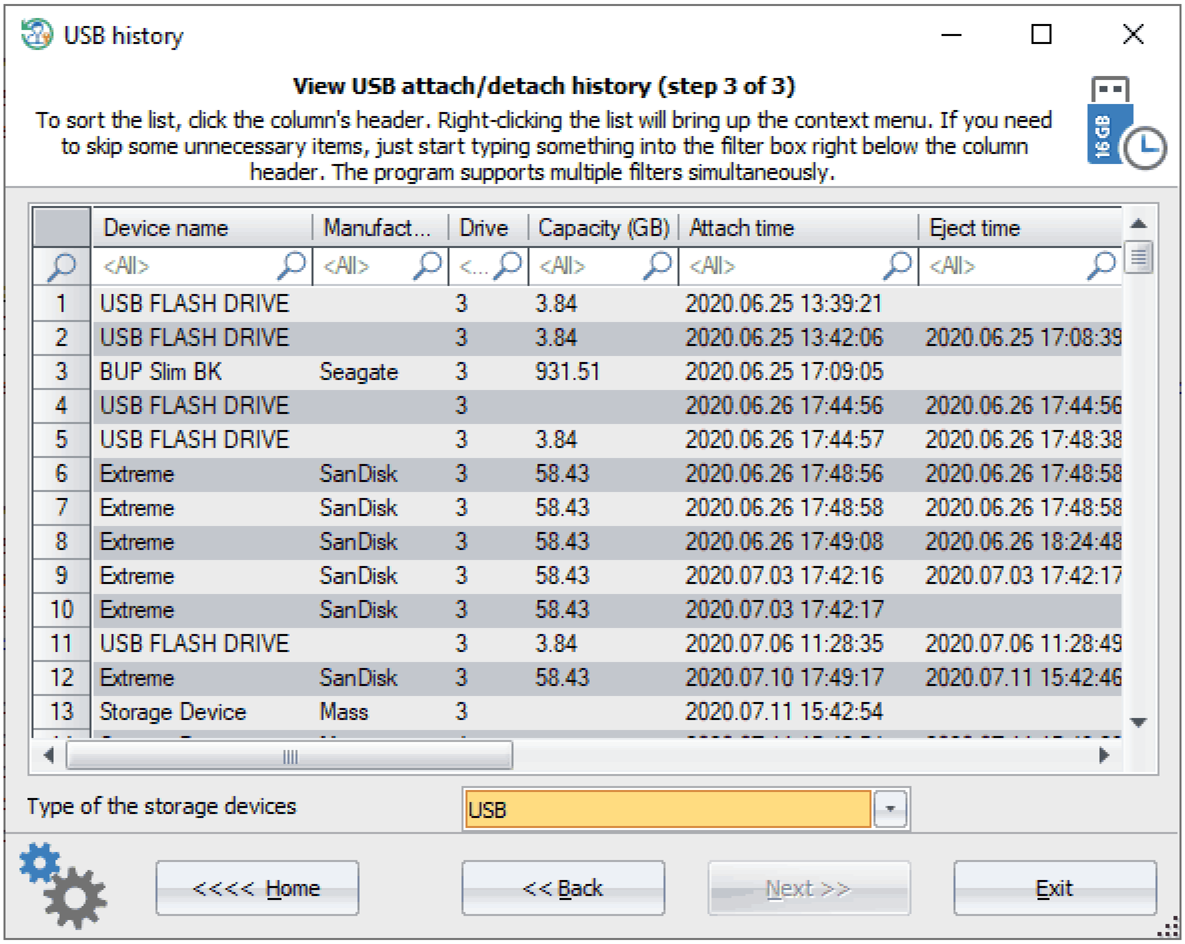
ADMIN-PC 5	
John	**2022.02.07 08:33:50**
WDAGUtilityAccount	2022.02.07 08:33:50
DefaultAccount	2022.02.07 08:33:50
Guest	2022.02.07 08:33:50
Administrator	2022.02.07 08:33:50

Legend

- Administrator
- User
- Guest
- Operator
- Computer account
- Account is locked out
- Microsoft/LiveId

To search for the storage history, select the Windows directory first.

USB history



View USB attach/detach history (step 3 of 3)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Device name	Manufact...	Drive	Capacity (GB)	Attach time	Eject time
	<All>	<All>	<...	<All>	<All>	<All>
1	USB FLASH DRIVE		3	3.84	2020.06.25 13:39:21	
2	USB FLASH DRIVE		3	3.84	2020.06.25 13:42:06	2020.06.25 17:08:39
3	BUP Slim BK	Seagate	3	931.51	2020.06.25 17:09:05	
4	USB FLASH DRIVE		3		2020.06.26 17:44:56	2020.06.26 17:44:56
5	USB FLASH DRIVE		3	3.84	2020.06.26 17:44:57	2020.06.26 17:48:38
6	Extreme	SanDisk	3	58.43	2020.06.26 17:48:56	2020.06.26 17:48:58
7	Extreme	SanDisk	3	58.43	2020.06.26 17:48:58	2020.06.26 17:48:58
8	Extreme	SanDisk	3	58.43	2020.06.26 17:49:08	2020.06.26 18:24:48
9	Extreme	SanDisk	3	58.43	2020.07.03 17:42:16	2020.07.03 17:42:17
10	Extreme	SanDisk	3	58.43	2020.07.03 17:42:17	
11	USB FLASH DRIVE		3	3.84	2020.07.06 11:28:35	2020.07.06 11:28:49
12	Extreme	SanDisk	3	58.43	2020.07.10 17:49:17	2020.07.11 15:42:46
13	Storage Device	Mass	3		2020.07.11 15:42:54	

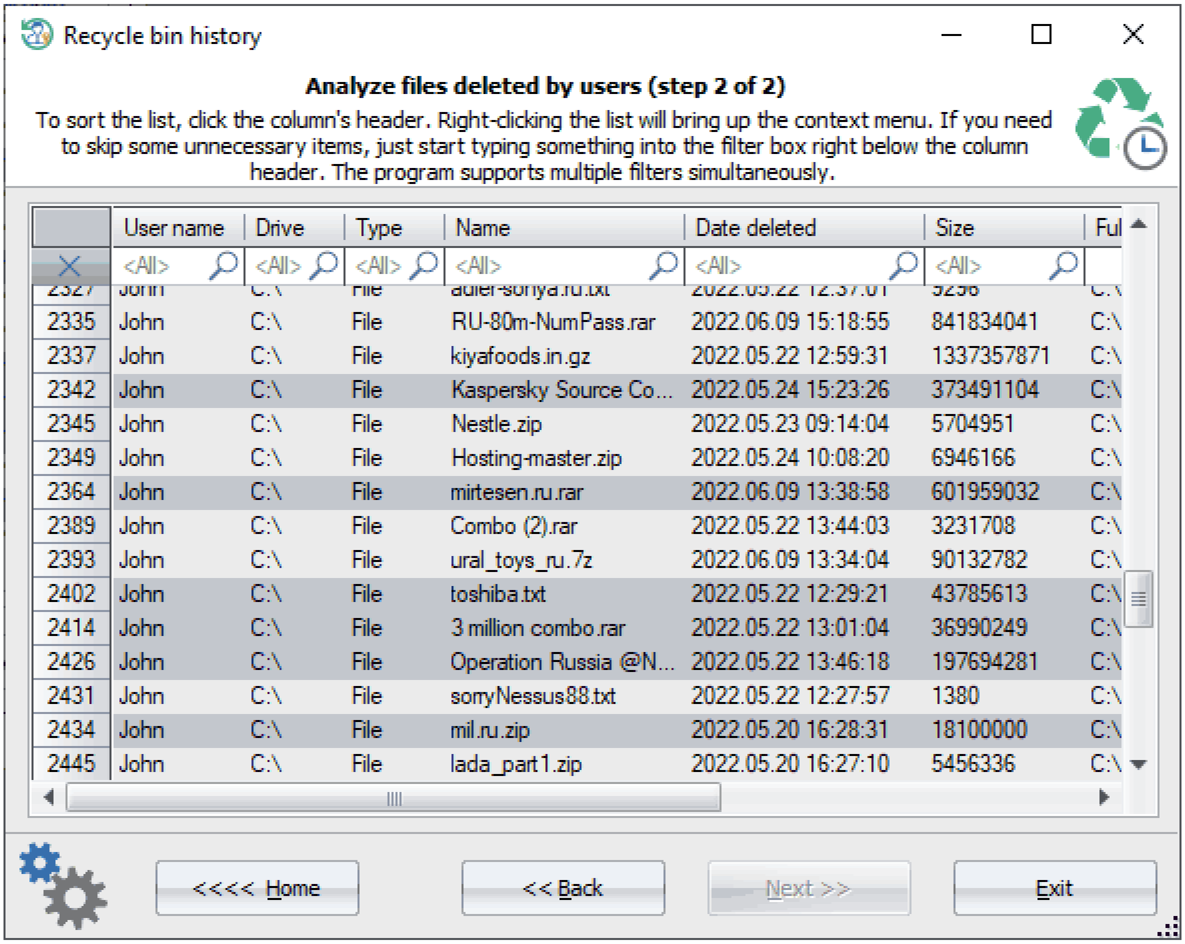
Type of the storage devices: USB

By default, the program displays the history of USB devices, however the program supports other storage types as well, such as 1394, ATA, ATAPI, FIBRE, Virtual File Backup Storages, ISCSI, MMC, RAID, SAS, SATA, SCSI, SD, SSA, Storage Spaces, Virtual Storages.

3.7.8 Recycle Bin history

The Windows Recycle Bin is a GUI element designed to delete shortcuts, files and folders easily, that everyone knows about, but forgets to clean it up time to time. In Windows, the files that have been moved to the Recycle Bin can be restored by owner.

Users often forget that an uncleaned Recycle Bin stores their evidences, passwords, history, source codes, etc. Therefore, for forensic experts, the Recycle Bin is the easiest way to dig around the user's recently deleted files.



Analyze files deleted by users (step 2 of 2)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	User name	Drive	Type	Name	Date deleted	Size	Ful
	<All>	<All>	<All>	<All>	<All>	<All>	
2327	John	C:\	File	adler-sonya.ru.txt	2022.05.22 12:37:01	5256	C:\
2335	John	C:\	File	RU-80m-NumPass.rar	2022.06.09 15:18:55	841834041	C:\
2337	John	C:\	File	kiyafoods.in.gz	2022.05.22 12:59:31	1337357871	C:\
2342	John	C:\	File	Kaspersky Source Co...	2022.05.24 15:23:26	373491104	C:\
2345	John	C:\	File	Nestle.zip	2022.05.23 09:14:04	5704951	C:\
2349	John	C:\	File	Hosting-master.zip	2022.05.24 10:08:20	6946166	C:\
2364	John	C:\	File	mirtesen.ru.rar	2022.06.09 13:38:58	601959032	C:\
2389	John	C:\	File	Combo (2).rar	2022.05.22 13:44:03	3231708	C:\
2393	John	C:\	File	ural_toys_ru.7z	2022.06.09 13:34:04	90132782	C:\
2402	John	C:\	File	toshiba.txt	2022.05.22 12:29:21	43785613	C:\
2414	John	C:\	File	3 million combo.rar	2022.05.22 13:01:04	36990249	C:\
2426	John	C:\	File	Operation Russia @N...	2022.05.22 13:46:18	197694281	C:\
2431	John	C:\	File	sorryNessus88.txt	2022.05.22 12:27:57	1380	C:\
2434	John	C:\	File	mil.ru.zip	2022.05.20 16:28:31	18100000	C:\
2445	John	C:\	File	lada_part1.zip	2022.05.20 16:27:10	5456336	C:\

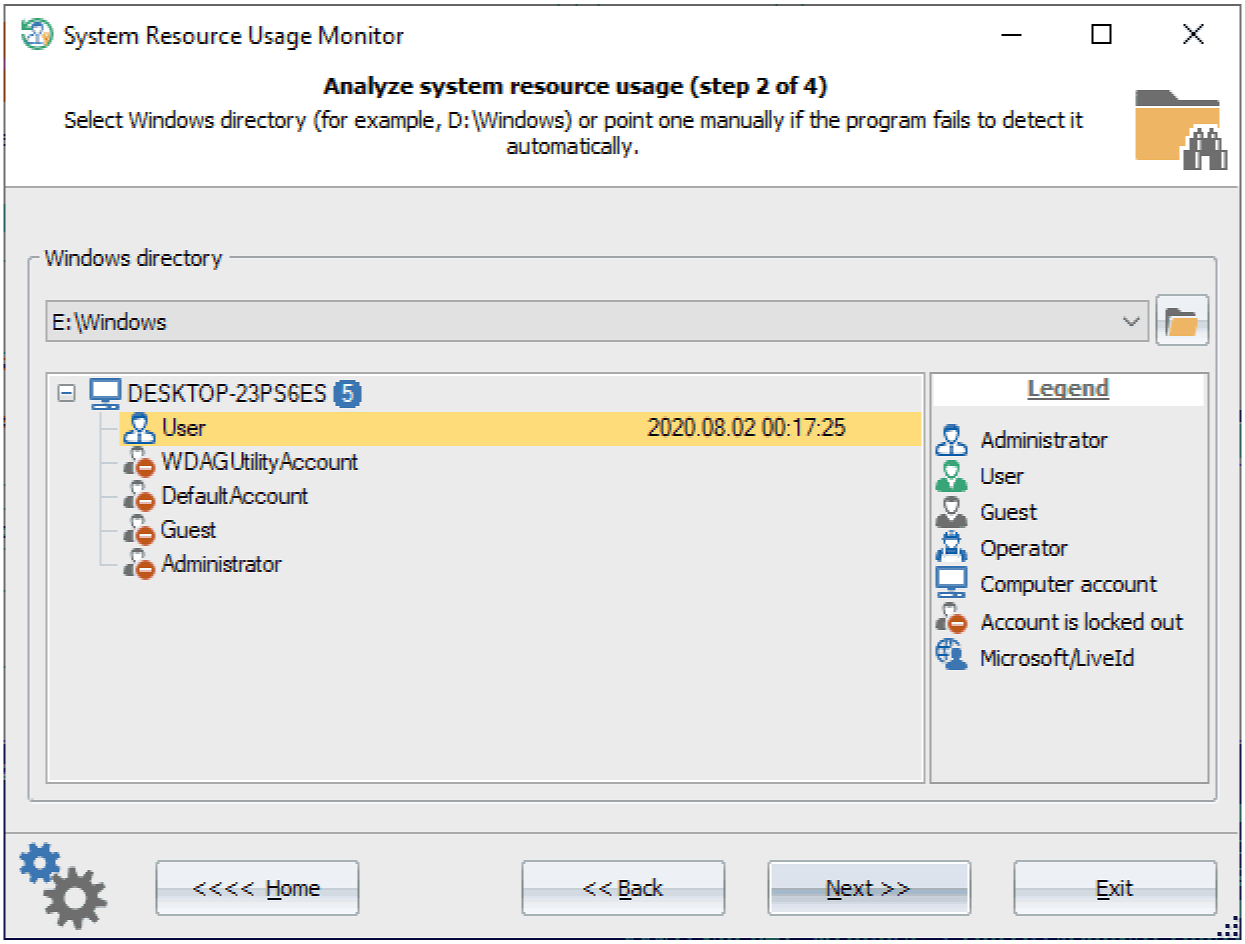
The **Recycle Bin History** tool scans every hard drive, extracts all deleted elements of every found Recycle Bin for every user account, and binds the data into a single table. You can use fast filters to search for the data you need. For example, to find all deleted shortcuts, just type in '*.lnk*' (without quotes) into the name filter. The selected items can be saved to a *.zip archive.

3.7.9 System resource usage monitor

The System Resource Usage Monitor (SRUM) is an underestimated, but important artifact of forensic investigation. It can tell what was happening on a computer at a certain point in time. SRUM stores (usually for the last couple of months) per-minute traces of user and process activity, statistics on sent and received data over network, some extended and exhaustive information on using processor time, mouse, keyboard, disk, and so on.

The system resource usage monitor appeared with Windows 8 as an integrated part of the Diagnostic Policy Service. Physically, all the data collected by SRUM is stored in the **SRUMDB.dat** file located at the **%WINDIR%\System32\sru** directory. This is an **E**xtensible **S**torage **E**ngine database, the same format Microsoft uses to store data in Active Directory, Windows Search, Windows Mail, etc.

Selecting OS directory



System Resource Usage Monitor

Analyze system resource usage (step 2 of 4)

Select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it automatically.

Windows directory

E:\Windows

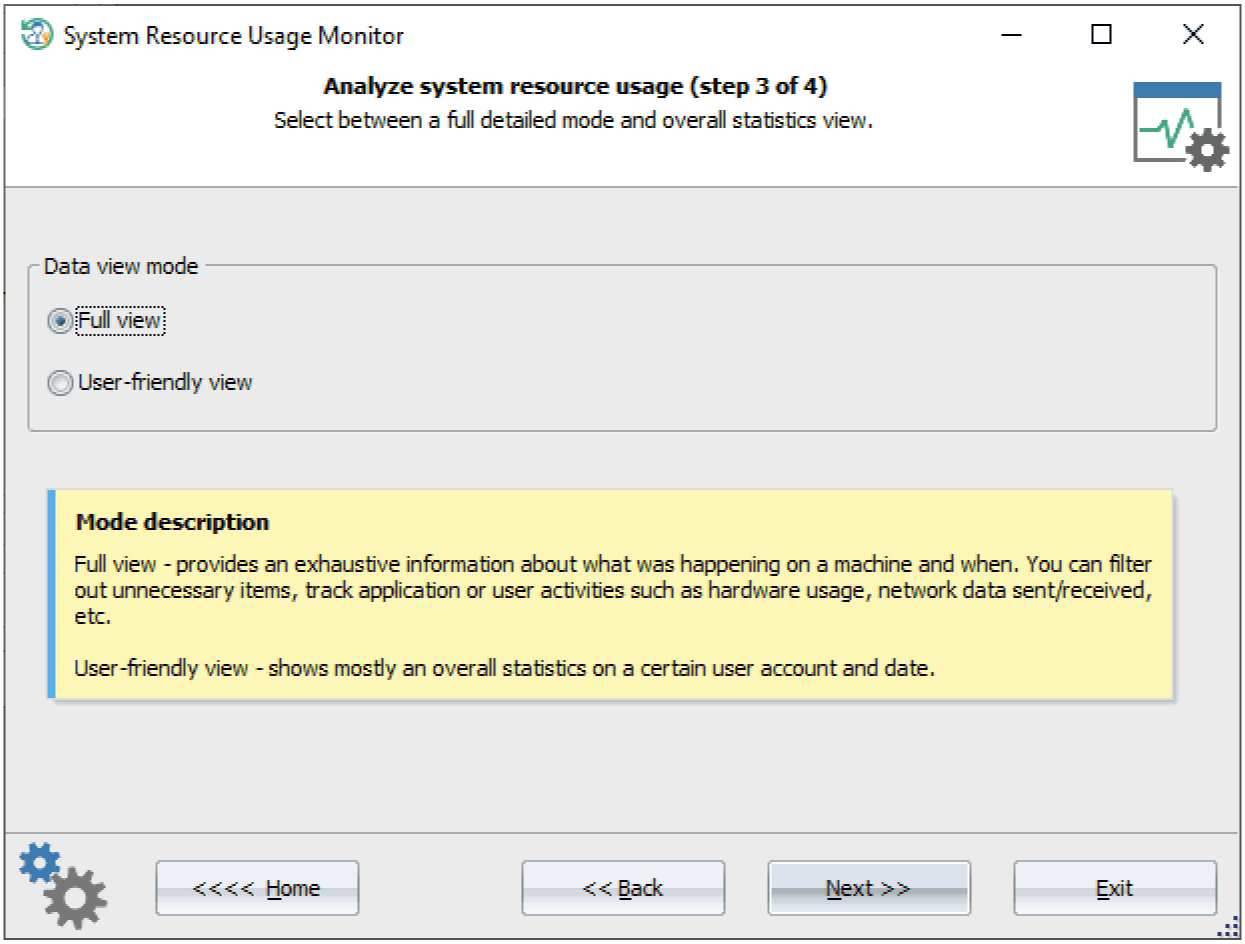
DESKTOP-23PS6ES 5	
User	2020.08.02 00:17:25
WDAGUtilityAccount	
DefaultAccount	
Guest	
Administrator	

Legend

- Administrator
- User
- Guest
- Operator
- Computer account
- Account is locked out
- Microsoft/LiveId

To parse and analyze the data from SRUM database, provide the path to the Windows directory first.

Selecting view mode



Analyze system resource usage (step 3 of 4)

Select between a full detailed mode and overall statistics view.

Data view mode

● Full view

○ User-friendly view

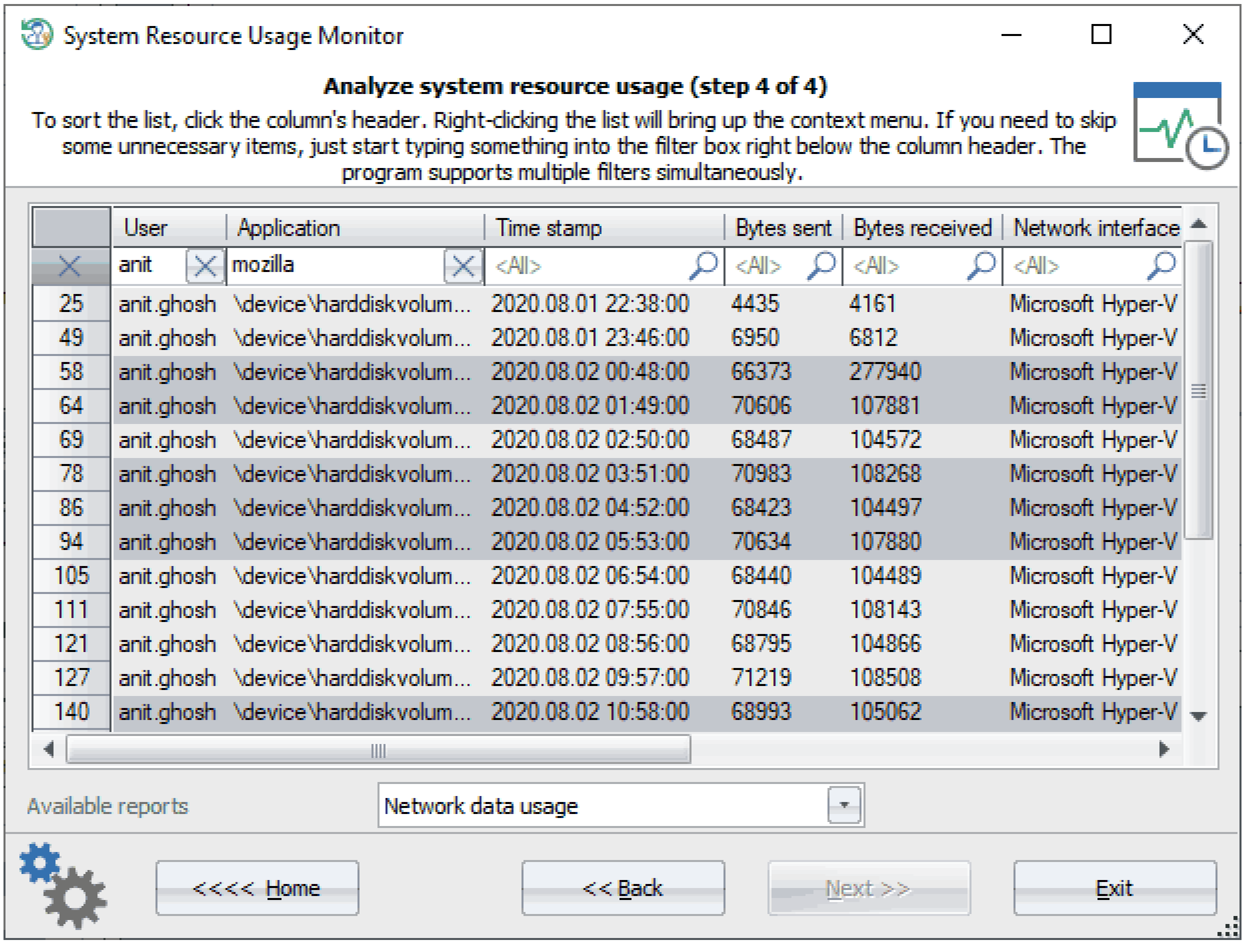
Mode description

Full view - provides an exhaustive information about what was happening on a machine and when. You can filter out unnecessary items, track application or user activities such as hardware usage, network data sent/received, etc.

User-friendly view - shows mostly an overall statistics on a certain user account and date.

You can switch between two modes for displaying the data. The full view mode displays all available information about system resource usage. You can filter out unnecessary items (f.e. user account or date), track application and user activities such as software and hardware usage, network data sent\received, CPU cycle utilization, metrics for I/O operations, etc. The short mode hides some redundant information and shows general statistics on users for a certain time period.

SRUM - full view



Analyze system resource usage (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	User	Application	Time stamp	Bytes sent	Bytes received	Network interface
	anit	mozilla	<All>	<All>	<All>	<All>
25	anit.ghosh	\device\harddiskvolum...	2020.08.01 22:38:00	4435	4161	Microsoft Hyper-V
49	anit.ghosh	\device\harddiskvolum...	2020.08.01 23:46:00	6950	6812	Microsoft Hyper-V
58	anit.ghosh	\device\harddiskvolum...	2020.08.02 00:48:00	66373	277940	Microsoft Hyper-V
64	anit.ghosh	\device\harddiskvolum...	2020.08.02 01:49:00	70606	107881	Microsoft Hyper-V
69	anit.ghosh	\device\harddiskvolum...	2020.08.02 02:50:00	68487	104572	Microsoft Hyper-V
78	anit.ghosh	\device\harddiskvolum...	2020.08.02 03:51:00	70983	108268	Microsoft Hyper-V
86	anit.ghosh	\device\harddiskvolum...	2020.08.02 04:52:00	68423	104497	Microsoft Hyper-V
94	anit.ghosh	\device\harddiskvolum...	2020.08.02 05:53:00	70634	107880	Microsoft Hyper-V
105	anit.ghosh	\device\harddiskvolum...	2020.08.02 06:54:00	68440	104489	Microsoft Hyper-V
111	anit.ghosh	\device\harddiskvolum...	2020.08.02 07:55:00	70846	108143	Microsoft Hyper-V
121	anit.ghosh	\device\harddiskvolum...	2020.08.02 08:56:00	68795	104866	Microsoft Hyper-V
127	anit.ghosh	\device\harddiskvolum...	2020.08.02 09:57:00	71219	108508	Microsoft Hyper-V
140	anit.ghosh	\device\harddiskvolum...	2020.08.02 10:58:00	68993	105062	Microsoft Hyper-V

Available reports: Network data usage

Most data lives in the following tables:
- Application timeline
- Resource usage
- Network connectivity
- Network data usage

Sample task. Find out when and how many bytes were received and sent from within the Firefox browser by anit.ghosh user account.
Sample solution. Let's type in into the username filter the following string 'annet.ghosh', and into the application filter - 'Mozilla' or 'Firefox'. So we should get the timeline statistics for our user, as shown in the picture above.

Data shared to all tables: user account, application name, the date and time the data was recorded into the database.

Data available in 'Application timeline' report: CPU timeline, CPU cycles, cycles breakdown, cycles attribute, cycles attribute breakdown, cycles WOB, cycles WOB breakdown, disk timeline, disk raw, network timeline, network tail raw, network bytes raw, metered network timeline, metered network tail raw, metered network bytes raw, rendered timeline, rendered, dirtied timeline, dirtied, propagated timeline, propagated, display required timeline, display required, in focus, user input timeline, user input, keyboard input timeline, keyboard input, mouse input, audio in timeline, audio in, audio out timeline, audio out, PSM foreground, flags, end time, timeline end, duration, span.

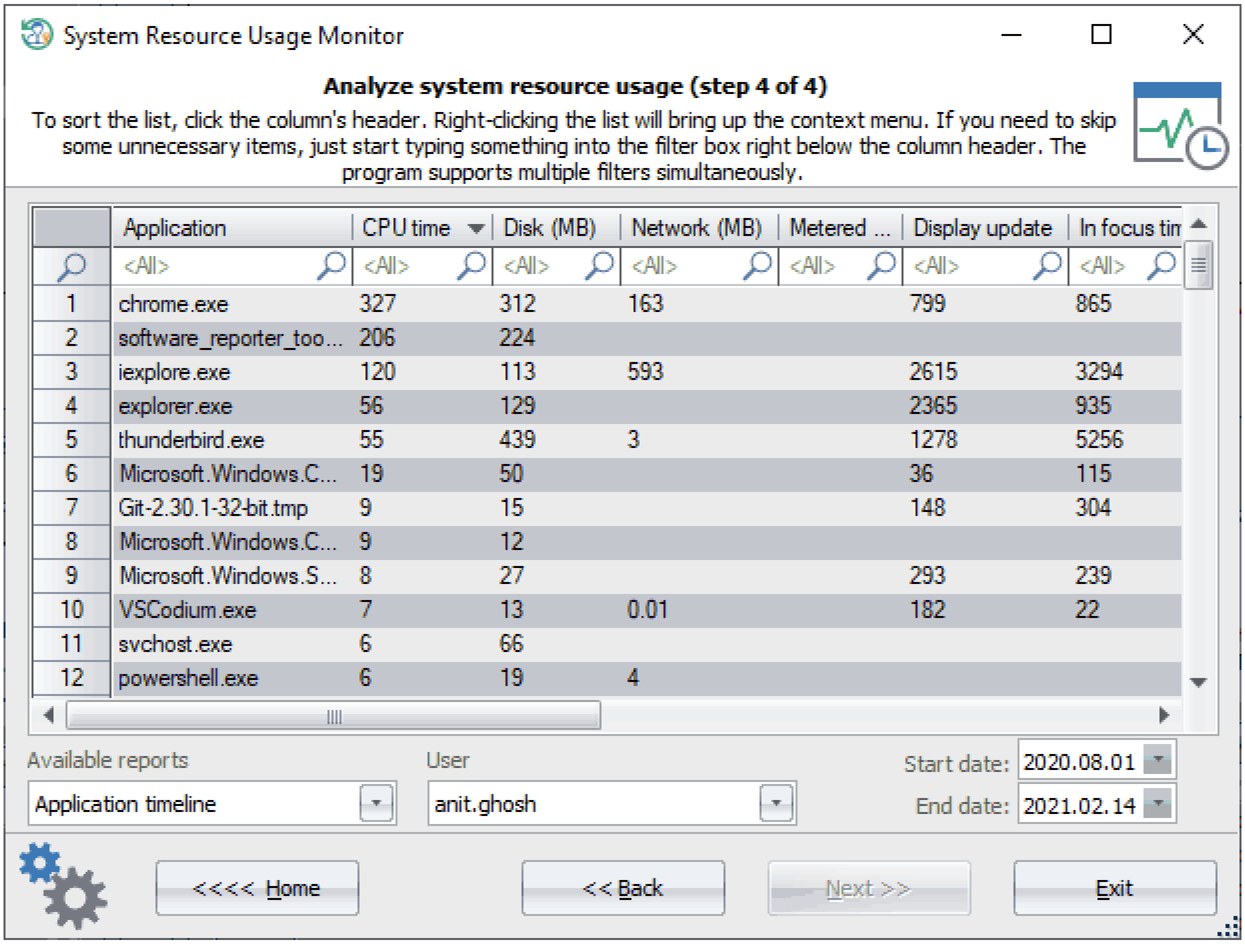
Data available in 'Resource usage' report: face time, foreground cycle time, foreground bytes read, foreground bytes write, foreground context switches, foreground number of flushes, foreground read operations, foreground write operations, background cycle time, background bytes read, background bytes write, background context switches, background number of flushes, background read operations, background write operations.

Data available in 'Windows push notifications' report: notification type, network type, payload size.

Data available in Network connectivity' report: connection started, connection time, network interface, interface type, profile ID, profile flags.

Data available in 'Network data usage' report: bytes sent, bytes received, network interface, interface type, profile ID, profile flags.

SRUM - user-friendly view



Analyze system resource usage (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu. If you need to skip some unnecessary items, just start typing something into the filter box right below the column header. The program supports multiple filters simultaneously.

	Application	CPU time	Disk (MB)	Network (MB)	Metered ...	Display update	In focus tim
	<All>	<All>	<All>	<All>	<All>	<All>	<All>
1	chrome.exe	327	312	163		799	865
2	software_reporter_too...	206	224				
3	iexplore.exe	120	113	593		2615	3294
4	explorer.exe	56	129			2365	935
5	thunderbird.exe	55	439	3		1278	5256
6	Microsoft.Windows.C...	19	50			36	115
7	Git-2.30.1-32-bit.tmp	9	15			148	304
8	Microsoft.Windows.C...	9	12				
9	Microsoft.Windows.S...	8	27			293	239
10	VSCodium.exe	7	13	0.01		182	22
11	svchost.exe	6	66				
12	powershell.exe	6	19	4			

Available reports: Application timeline

User: anit.ghosh

Start date: 2020.08.01

End date: 2021.02.14

General statistics for a specific user by a date frame.

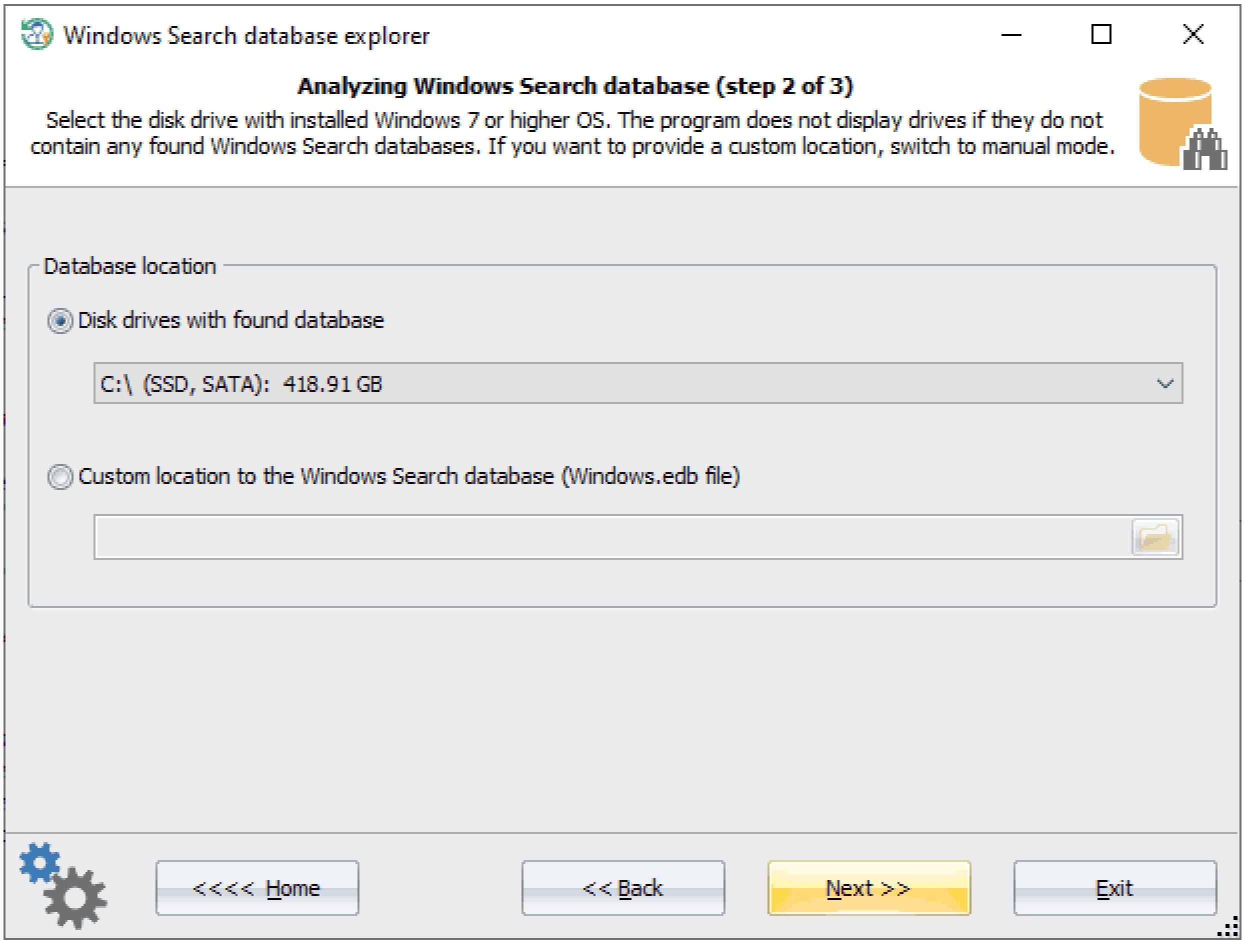
3.7.10 Windows Search database explorer

Windows Search is a content index desktop search platform developed by Microsoft. Windows Search creates an index of files, documents, emails, folders, programs, notes, photos, internet history, etc. as well as file contents. The purpose is to let users perform fast incremental search based on contents and details such as authors, dates, people, file names, file types, and sizes.

The Windows Search database provides a valuable source of information for a forensic investigator. The indexed data reside in a single **Extensible Storage Engine** file at the following directory:
%SYSTEMDRIVE%\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

The Windows 11 Search stores the data in the SQLite database named *Windows.db* but has a similar data structure.

The Windows Search explorer is a tool to parse the database and display collected information in a human-readable format.



Windows Search database explorer

Analyzing Windows Search database (step 2 of 3)

Select the disk drive with installed Windows 7 or higher OS. The program does not display drives if they do not contain any found Windows Search databases. If you want to provide a custom location, switch to manual mode.

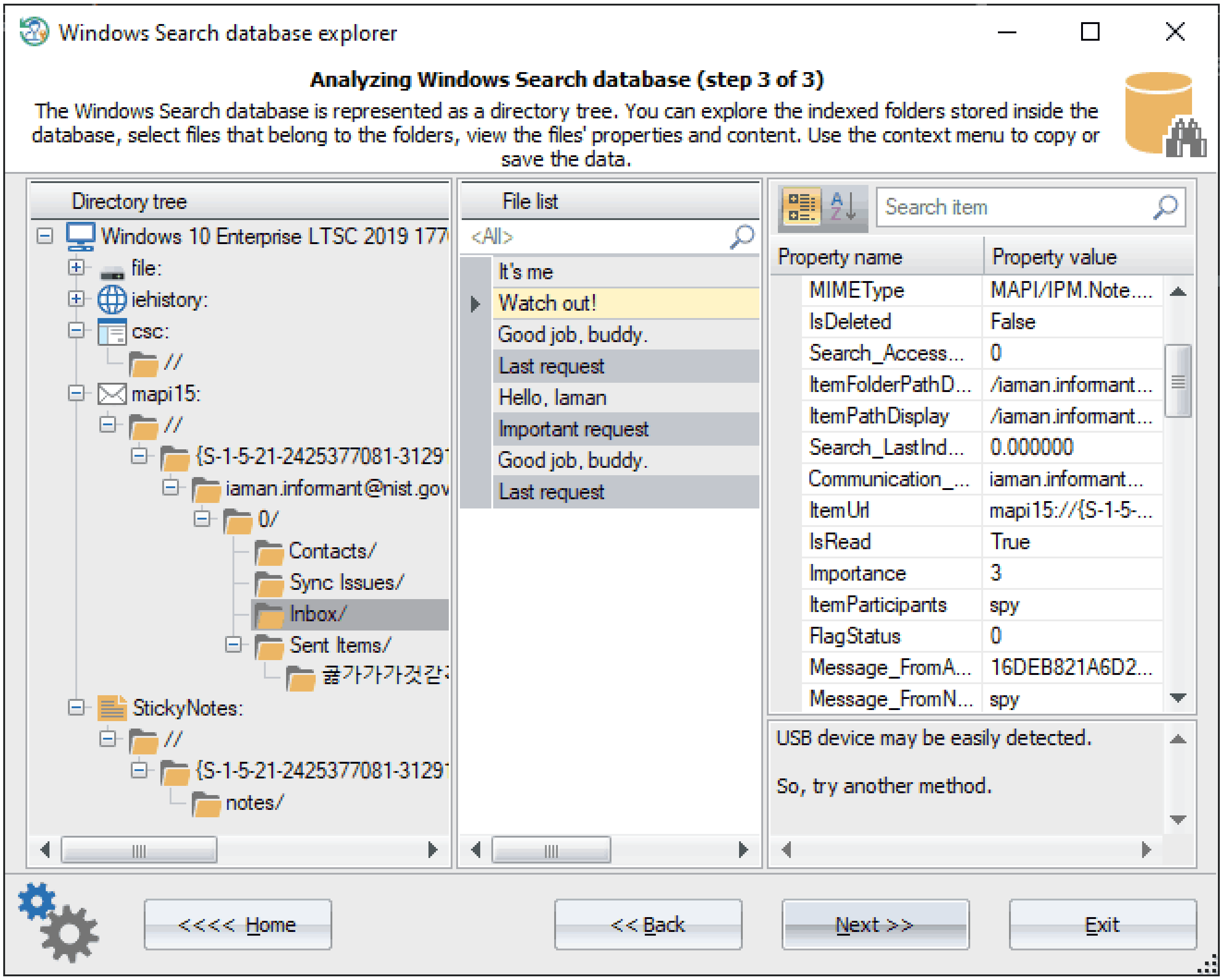
Database location

● Disk drives with found database

C:\ (SSD, SATA): 418.91 GB

○ Custom location to the Windows Search database (Windows.edb file)

First, you need to provide the path to the database. You can do it either selecting a disk (the program displays only those ones where it managed to fetch the database) or setting up a full path to the database manually.



Windows Search database explorer

Analyzing Windows Search database (step 3 of 3)

The Windows Search database is represented as a directory tree. You can explore the indexed folders stored inside the database, select files that belong to the folders, view the files' properties and content. Use the context menu to copy or save the data.

Directory tree

- Windows 10 Enterprise LTSC 2019 177
  - file:
  - iehistory:
  - csc:
    - //
  - mapi15:
    - //
      - {S-1-5-21-2425377081-3129
        - iaman.informant@nist.gov
          - 0/
            - Contacts/
            - Sync Issues/
            - Inbox/
            - Sent Items/
              - 굶가가가것갈
  - StickyNotes:
    - //
      - {S-1-5-21-2425377081-3129
        - notes/

File list

<All>

It's me
Watch out!
Good job, buddy.
Last request
Hello, Iaman
Important request
Good job, buddy.
Last request

Property name	Property value
MIMEType	MAPI/IPM.Note....
IsDeleted	False
Search_Access...	0
ItemFolderPathD...	/iaman.informant...
ItemPathDisplay	/iaman.informant...
Search_LastInd...	0.000000
Communication_...	iaman.informant...
ItemUrl	mapi15://{S-1-5-...
IsRead	True
Importance	3
ItemParticipants	spy
FlagStatus	0
Message_FromA...	16DEB821A6D2...
Message_FromN...	spy

USB device may be easily detected.

So, try another method.

The program builds a list of all found items and displays it in the left pane under the *directory tree*. So the *directory tree* is a parent for disk, email, internet history, user activity and other folders. Once a folder is selected under the *directory tree* pane, the program fills in the middle *file list* pane and displays items that belong to the selected folder there. To view all available properties (right pane), just select the item you need.

Here's the description of most used properties:

Name	Description
acquisitionid	A hash value that indicates the acquisition session.
applicationname	The name of the application that created this file or item. Do not use version numbers to identify the application's specific version.
appusermodel_excludefromshowinnewinstall	Prevents a Start menu entry for a newly installed application shortcut from receiving a highlight.
appusermodel_id	An explicit Application User Model ID (AppUserModelID) used to associate processes, files, and windows with a particular application.
appusermodel_isdestlistseparator	Inserts a separator in the Tasks section of a Jump List.

appusermodel_isdualmode	Indicates that an application supports dual desktop and immersive modes. In Windows 8, this property is only applicable for web browsers.
appusermodel_preventpinning	Disables the ability of a shortcut or window to be pinned to the taskbar or the Start menu. This property also makes the item ineligible for inclusion in the Start menu's Most Frequently Used (MFU) list.
appusermodel_relaunchcommand	Specifies a command that can be executed through ShellExecute to launch an application when it is pinned to the taskbar or when a new instance of the application is launched through the application's Jump List.
appusermodel_relaunchdisplaynameresource	Specifies the display name used for the shortcut created on the taskbar when the user chooses to pin an application to the taskbar or launch a new instance through its button's Jump List.
appusermodel_relaunchiconresource	Specifies the icon used for the shortcut created on the taskbar when the user chooses to pin an application to the taskbar or launch a new instance through its button's Jump List.
appusermodel_startpinoption	Set this property on a shortcut to (1) prevent an application from being automatically pinned to Start screen upon installation; or(2) indicate that an item is programmatically added to launcher via user action (which implies automatically pin to Start and delete on unpin).
appusermodel_toastactivatorclsid	Used to CoCreate an INotificationActivationCallback interface to notify about toast activations.
appzoneidentifier	Mark of the app container. The zone identifier as determined by the file's last writer.
audio_channelcount	Indicates the channel count for the audio file. Possible values are 1 for mono and 2 for stereo.
audio_compression	Indicates the audio compression used on the audio file.
audio_encodingbitrate	Indicates the average data rate in Hertz (Hz) for the audio file in bits per second.
audio_format	Indicates the format of the audio file.
audio_isvariablebitrate	Indicates whether the audio file had a variable or constant bit rate.
audio_samplerate	Indicates the sample rate for the audio file in samples per second.
audio_samplesize	Indicates the sample size for the audio file in bits per sample.
audio_streamname	Identifies the name of the stream for the audio file.
audio_streamnumber	Identifies the stream number of the audio file.
author	Represents the author or authors of the document.
calendar_duration	The calendar duration.
calendar_isonline	Indicates whether the event is an online event.
calendar_isrecurring	Indicates if the event will recur.
calendar_location	Indicates the location of the event.
calendar_optionalattendeeaddresses	Addresses of the all the optional attendees.
calendar_optionalattendeenames	Names of the all the optional attendees.
calendar_organizeraddress	The address of the event organizer. This is a mailing or street address.
calendar_organizername	The name of the event organizer.
calendar_remindertime	Stores the time the user chooses to be reminded of the event.
calendar_requiredattendeeaddresses	Addresses of the all the required attendees.
calendar_requiredattendeenames	Names of all the required attendees.
calendar_resources	Indicates the resources used for this event.

calendar_responsestatus	Stores the status of a user's responses to meetings in the calendar.
calendar_showtimeas	Indicates the status of the attendee during the event. User can choose to set the status as free, busy, tentative or out of office.
calendar_showtimeastext	The user-friendly form of Calendar_ShowTimeAs. This value is not intended to be parsed programmatically.
capacity	The amount of total storage space, expressed in bytes.
category	Deprecated. The category that can be assigned to an item such as a document or file.
comment	The comment attached to a file, typically added by a user.
communication_accountname	The account name.
communication_dateitemexpires	The date the item expires due to the retention policy.
communication_direction	Indicates whether a communication was incoming or outgoing.
communication_followupiconindex	The icon index used on messages marked for followup.
communication_headeritem	This property is true if the item is a header item, which means that the item has not been fully downloaded.
communication_policytag	This property identifies the retention policy applied to the item.
communication_securityflags	Security flags associated with the item to indicate whether the item is encrypted, signed, or DRM enabled.
communication_taskstatus	Indicates the current status of the task.
communication_taskstatustext	The user-friendly form of Communication_TaskStatus. This value is not intended to be parsed programmatically.
company	The company or publisher.
computer_decoratedfreespace	The computer's free space and total space stated as '%s free of %s'.
computername	The name of the computer where the item or file is located.
contact_accountpicturedynamicvideo	This is a stream containing the data necessary to render a contact's dynamic video account picture.
contact_accountpicturelarge	This is a stream containing the data necessary to render a contact's large account picture.
contact_accountpicturesmall	This is a stream containing the data necessary to render a contact's small account picture.
contact_anniversary	Anniversary of the contact.
contact_assistantname	Contact's assistant name.
contact_assistanttelephone	Telephone number of the contact's assistant.
contact_birthday	Birthday of the contact.
contact_businessaddress	Business address of the contact.
contact_businessaddresscity	Business address city of the contact.
contact_businessaddresscountry	Business address country of the contact.
contact_businessaddresspostalcode	Business address postal code of contact.

contact_businessaddresspostofficebox	Business address post office box number of the contact.
contact_businessaddressstate	Business address state of the contact.
contact_businessaddressstreet	Business address street of the contact.
contact_businessfaxnumber	Business address fax number of the contact.
contact_businesshomepage	Business address home page of the contact.
contact_businesstelephone	Business telephone number of the contact.
contact_callbacktelephone	Call back number of the contact.
contact_cartelephone	Car telephone number of the contact.
contact_children	Indicates the number of children the contact has.
contact_companymaintelephone	Indicates the main telephone number of the contact's company.
contact_department	Department name of the contact.
contact_emailaddress	Email address of the contact.
contact_emailaddress2	Email address 2 of the contact.
contact_emailaddress3	Email address 3 of the contact.
contact_emailaddresses	Indicates all the email addresses of the contact.
contact_emailname	Email name of the contact.
contact_fileasname	Indicates the FileAs name of the contact.
contact_firstname	Indicates the first name of the contact.
contact_fullname	Indicates the full name of the contact.
contact_gender	The user-friendly form of Contact_GenderValue.
contact_gendervalue	Identifies the gender of the contact.
contact_hobbies	Indicates the hobbies of the contact.
contact_homeaddress	Home address of the contact.
contact_homeaddresscity	Home address city name of the contact.
contact_homeaddresscountry	Home address country name of the contact.
contact_homeaddresspostalcode	Home address postal code of the contact.
contact_homeaddresspostofficebox	Home address postal box number of the contact.
contact_homeaddressstate	Home address state name of the contact.
contact_homeaddressstreet	Home address street name of the contact.
contact_homefaxnumber	Home fax number of the contact.
contact_hometelephone	Home telephone number of the contact.
contact_imaddress	Instant messaging address of the contact.
contact_initials	Initials of the contact.

contact_ja_companynamephonetic	Pronunciation of the contact's company name.
contact_ja_firstnamephonetic	Pronunciation of the first name.
contact_ja_lastnamephonetic	Pronunciation of the last name.
contact_jobtitle	Job title of the contact.
contact_label	Contact's calendar event label.
contact_lastname	Last name of the contact.
contact_mailingaddress	Mailing address of the contact.
contact_middlename	Middle name of the contact.
contact_mobiletelephone	Mobile telephone number of the contact.
contact_nickname	Nickname of the contact.
contact_officelocation	Office location of the contact.
contact_otheraddress	Other address of the contact.
contact_otheraddresscity	Other address city name of the contact.
contact_otheraddresscountry	Other address country name of the contact.
contact_otheraddresspostalcode	Other address postal code of the contact.
contact_otheraddresspostofficebox	Other address post office box number of the contact.
contact_otheraddressstate	Other address state name of the contact.
contact_otheraddressstreet	Other address street of the contact.
contact_pagertelephone	Pager telephone number of the contact.
contact_personaltitle	Contact's personal title.
contact_primaryaddresscity	Primary address city name of the contact.
contact_primaryaddresscountry	Primary address country name of the contact.
contact_primaryaddresspostalcode	Primary address postal code of the contact.
contact_primaryaddressstate	Primary address state name of the contact.
contact_primaryaddressstreet	Primary address street of the contact.
contact_primaryemailaddress	Primary Email address of the contact.
contact_primarytelephone	Primary telephone number of the contact.
contact_profession	Profession of the contact.
contact_spousename	Name eof the contact's spouse.
contact_suffix	Suffix attached to the contact's name.
contact_telexnumber	Telex number of the contact.
contact_ttytddtelephone	Teletype or telecommunication device number of the contact.

contact_webpage	Webpage of the contact.
containeditems	A list of the type of content in the item.
copyright	The copyright information stored as a string.
creatorappid	The AppId of the application that created this file.
creatoropenwithuioptions	Provides options that influence the behavior of UI controls that launch the file with the app specified in CreatorAppId.
dataobjectformat	The data object format. A string value that is the clipboard format name.
dateaccessed	Indicates the last time the item was accessed. The Indexing Service friendly name is 'access'.
dateacquired	The acquisition date of the file or media.
datearchived	The date the file item was last archived.
datecreated	The date and time the item was created on the file system where it is currently located.
dateimported	The date and time the file was imported into a private application database.
datemodified	The date and time of the last modification to the item. The Indexing Service friendly name is 'write'.
defaultsavelocationdisplay	Helps display as an icon whether or not a location is the default save location for owner and/or non-owners of a library.
descriptionid	The contents of an SHDESCRIPTIONID structure, represented as a buffer of bytes.
device_printerurl	The URL for the printer.
deviceinterface_bluetooth_deviceaddress	Bluetooth device address.
deviceinterface_bluetooth_flags	Bluetooth device flags.
deviceinterface_bluetooth_lastconnectedtime	Bluetooth device last connected time.
deviceinterface_bluetooth_manufacturer	Bluetooth device manufacturer.
deviceinterface_bluetooth_modelnumber	Bluetooth device model number.
deviceinterface_bluetooth_productid	Bluetooth device product identifier.
deviceinterface_bluetooth_productversion	Bluetooth device product version.
deviceinterface_bluetooth_serviceguid	Learn about the Bluetooth service GUID. This reference page describes the DeviceInterface_Bluetooth_ServiceGuid property.
deviceinterface_bluetooth_vendorid	Bluetooth device vendor identifier.
deviceinterface_bluetooth_vendoridsource	Bluetooth device vendor identifier source.
deviceinterface_hid_isreadonly	Indicates if a HID device is a Read-Only device.
deviceinterface_hid_productid	HID device Product Id.
deviceinterface_hid_usageid	HID device Usage Id.
deviceinterface_hid_usagepage	HID device Usage Page.
deviceinterface_hid_vendorid	HID device Vendor Id.

deviceinterface_hid_versionnumber	HID device Version Number.
deviceinterface_printerdriverdirectory	The directory location for the printer driver.
deviceinterface_printerdrivername	The name of the printer driver file.
deviceinterface_printerenumerationflag	Printer information Printer Enumeration Flag.
deviceinterface_printername	The name of the printer.
deviceinterface_printerportname	The port where the printer is located.
deviceinterface_proximity_supportsnfc	Indicates whether the device supports NFC communications (NDEF).
deviceinterface_serial_portname	Serial device friendly name.
deviceinterface_serial_usbproductid	Serial device USB Product Id.
deviceinterface_serial_usbvendorid	Serial device USB Vendor Id.
deviceinterface_winusb_deviceinterfaceclasses	WinUSB device interface GUID(s) used to open a handle to the device.
deviceinterface_winusb_usbclass	Class value from the USB device's first USB Interface Descriptor.
deviceinterface_winusb_usbproductid	Product ID from the USB device's USB Device Descriptor.
deviceinterface_winusb_usbprotocol	Protocol value from the USB device's first USB Interface Descriptor.
deviceinterface_winusb_usbsubclass	SubClass value from the USB device's first USB Interface Descriptor.
deviceinterface_winusb_usbvendorid	Vendor ID from the USB device's USB Device Descriptor.
devices_aep_aepid	Identity of the Device Association Endpoint.
devices_aep_bluetooth_cod_major	Bluetooth class of device major code.
devices_aep_bluetooth_cod_minor	Bluetooth class of device minor code.
devices_aep_bluetooth_cod_services_audio	Bluetooth class of device service audio.
devices_aep_bluetooth_cod_services_capturing	Bluetooth class of device service capturing.
devices_aep_bluetooth_cod_services_information	Bluetooth class of device service information.
devices_aep_bluetooth_cod_services_limiteddiscovery	Bluetooth class of device service limited discovery.
devices_aep_bluetooth_cod_services_networking	Bluetooth class of device service networking.

devices_aep_bluetooth_cod_services_objectxfer	Bluetooth class of device service object transfer.
devices_aep_bluetooth_cod_services_positioning	Bluetooth class of device service positioning.
devices_aep_bluetooth_cod_services_rendering	Bluetooth class of device service rendering.
devices_aep_bluetooth_cod_services_telephony	Bluetooth class of device service telephony.
devices_aep_bluetooth_le_addresstype	Bluetooth LE device address type.
devices_aep_bluetooth_le_appearance_category	Learn about the Bluetooth LE device appearance. This reference page describes the Devices_Aep_Bluetooth_Le_Appearance_Category property.
devices_aep_bluetooth_le_appearance_subcategory	Learn about the Bluetooth LE device appearance. This reference page describes the Devices_Aep_Bluetooth_Le_Appearance_Subcategory property.
devices_aep_bluetooth_le_appearance	Learn about the Bluetooth LE device appearance. This reference page describes the Devices_Aep_Bluetooth_Le_Appearance property.
devices_aep_bluetooth_le_isconnectable	Whether the Bluetooth LE device is currently advertising a connectable advertisement.
devices_aep_canpair	Whether the Device Association Endpoint can be paired with the system or not.
devices_aep_category	The Devices_Aep_Category property indicates the categories the device is part of, such as Printer or Camera.
devices_aep_containerid	Device Association Endpoint's Parent Container Id.
devices_aep_deviceaddress	Address based on the protocol of the Device Association Endpoint. IP Address for an IP device, Bluetooth address for Bluetooth device, etc.
devices_aep_isconnected	Whether the device is currently connected to the system or or not.
devices_aep_ispaired	Whether the Device Association Endpoint is paired with the system or not.
devices_aep_ispresent	Whether the device is currently present or not.
devices_aep_manufacturer	Device Association Endpoint's Manufacturer.
devices_aep_modelid	Device Association Endpoint's Model Id.
devices_aep_modelname	Device Association Endpoint's Model Name.
devices_aep_pointofservice_connectiontypes	A bit mask that specifies which connection types should be included in the search.
devices_aep_protocolid	Identity of the protocol this Device Association Endpoint was discovered over.
devices_aep_signalstrength	Signal strength of the device. Only applicable for some protocols.
devices_aepcontainer_canpair	Whether one of the child Device Association Endpoints can be paired with the system or not.
devices_aepcontainer_categories	The Devices_AepContainer_Categories property indicates the categories the device is part of, such as Printer or Camera.
devices_aepcontainer_children	List of child Device Association Endpoint Identities that are part of this Device Association Endpoint Container.

devices_aepcontainer_containerid	Device Association Endpoint Container's Identity.
devices_aepcontainer_dialprotocol_installedapplications	List of applications supporting DIAL protocol on the Device Association End Point Container.
devices_aepcontainer_ispaired	Whether one of the child Device Association Endpoints is paired with the system or not.
devices_aepcontainer_ispresent	Whether one of the Device Association Endpoints is currently present or not.
devices_aepcontainer_manufacturer	Manufacturer of the device.
devices_aepcontainer_modelids	List of Model Ids for the device. Each Model Id is a Guid in string form.
devices_aepcontainer_modelname	Model Name of the device.
devices_aepcontainer_protocolids	List of Protocol Ids that have contributed to building the Device Association Endpoint Container.
devices_aepcontainer_supportedurischemes	List of Casting Uri Schemes Supported by the Device Association Endpoint Container.
devices_aepcontainer_supportsaudio	Indicates if the Device Association Endpoint Container Supports Audio Casting.
devices_aepcontainer_supportscapturing	Indicates if the Device Association Endpoint Container Supports Capturing.
devices_aepcontainer_supportsimages	Indicates if the Device Association Endpoint Container Supports Image Casting.
devices_aepcontainer_supportsinformation	Indicates if the Device Association Endpoint Container Supports Information.
devices_aepcontainer_supportslimiteddiscovery	Indicates if the Device Association Endpoint Container Supports Limited Discovery.
devices_aepcontainer_supportsnetworking	Indicates if the Device Association Endpoint Container Supports SupportsNetworking.
devices_aepcontainer_supportsobjecttransfer	Indicates if the Device Association Endpoint Container Supports Object Transfer.
devices_aepcontainer_supportspositioning	Indicates if the Device Association Endpoint Container Supports Positioning.
devices_aepcontainer_supportsrendering	Indicates if the Device Association Endpoint Container Supports Rendering.
devices_aepcontainer_supportstelephony	Indicates if the Device Association Endpoint Container Supports Telephony.
devices_aepcontainer_supportsvideo	Indicates if the Device Association Endpoint Container Supports Video Casting.
devices_aepservice_aepid	Device Association Endpoint Service's Parent AEP Id.
devices_aepservice_bluetooth_cachemode	Bluetooth caching mode for the query.
devices_aepservice_bluetooth_gattservice_cachemode	Sets the Bluetooth Gatt cache mode for the query.
devices_aepservice_bluetooth_gattservice_device	Learn how the Devices_AepService_Bluetooth_GattService_Device property sets the Bluetooth device address to query.

devices_aepservice_bluetooth_rfcommservice_cachemode	Sets the Bluetooth RFCOMM cache mode for the query.
devices_aepservice_bluetooth_rfcommservice_device	Learn how the Devices_AepService_Bluetooth_RfcommService_Device property sets the Bluetooth device address to query.
devices_aepservice_bluetooth_serviceguid	Learn about the Bluetooth service GUID. This reference page describes the Devices_AepService_Bluetooth_ServiceGuid property.
devices_aepservice_bluetooth_targetdevice	Bluetooth parent device for the query. Required for uncached queries.
devices_aepservice_containerid	Device Association Endpoint Service's Parent Container Id.
devices_aepservice_friendlyname	Device Association Endpoint Service Friendly Name.
devices_aepservice_iot_serviceinterfaces	List of interfaces that are available for this service.
devices_aepservice_parentaepispaired	Whether the parent Device Association Endpoint is paired with the system or not.
devices_aepservice_protocolid	Identity of the protocol this Device Association Endpoint Service was discovered over.
devices_aepservice_serviceclassid	Identity of the service this Device Association Endpoint Service represents.
devices_aepservice_serviceid	Device Association Endpoint Service's Id.
devices_apppackagefamilyname	The package family name registered as the app for this device.
devices_audiodevice_microphone_sensitivityindbfs	Sensitivity information in Dbfs for a microphone device.
devices_audiodevice_microphone_signaltonoiseratioindb	Signal to noise ratio information in Db for a microphone device.
devices_audiodevice_rawprocessingsupported	Raw processing mode support for the audio device. If VARIANT.TRUE the device supports raw processing mode.
devices_audiodevice_speechprocessingsupported	Speech mode support for the audio device. If VARIANT.TRUE the device supports speech mode.
devices_batterylife	Remaining battery life, as a percentage.
devices_batterypluscharging	Remaining battery life of the device and its charging state.
devices_batterypluschargingtext	The remaining battery life of the device, and the device's charging state as a string.
devices_category	Singular form of device category.
devices_categorygroup	Plural of device category.
devices_categoryids	Indicates the actual raw category.
devices_categoryplural	A property with multiple device categories.
devices_chargingstate	Device charging status.
devices_children	Device instance ids of children of this device.
devices_classguid	Device Class Guid.
devices_compatibleids	Compatible Ids.
devices_connected	Device connection state.

devices_containerid	Device container ID.
devices_defaulttooltip	Tooltip for the default state.
devices_devicecapabilities	Device Capabilities.
devices_devicecharacteristics	Device Characteristics.
devices_devicedescription1	First line of the device description.
devices_devicedescription2	Second line of the device description.
devices_devicehasproblem	Device has a problem.
devices_deviceinstanceid	Device instance Id.
devices_devicemanufacturer	Device manufacturer. Property on device object.
devices_devobjecttype	DevQuery Device Object Type.
devices_dialprotocol_installedapplications	List of applications supporting DIAL protocol on the Device Association End Point.
devices_discoverymethod	Indicates the transport or physical connection on which the device is discovered.
devices_dnssd_domain	Domain portion of DNS-SD service instance name. (e.g. '.local' in 'myservice_http_tcp_local').
devices_dnssd_fullname	Complete DNS-SD service instance name, including instance, service, and domain.
devices_dnssd_hostname	DNS name of device is hosting the service.
devices_dnssd_instancename	Instance portion of DNS-SD service instance name.(e.g. 'myservice' in 'myservice_http_tcp_local').
devices_dnssd_networkadapterid	GUID for the network adapter on which to search for a service.
devices_dnssd_portnumber	Port number on which the service is listening.
devices_dnssd_priority	SRV record priority field. Not usually used.
devices_dnssd_servicename	Service type portion of DNS-SD service instance name. (e.g. 'http_tcp' in 'myservice_http_tcp_local').
devices_dnssd_textattributes	Text data associated with the service instance. Each string is typically a key-value pair, separated by '='.
devices_dnssd_ttl	SRV record Time-To-Live field. Not usually used.
devices_dnssd_weight	SRV record weight field. Not usually used.
devices_friendlyname	Friendly name of the device.
devices_functionpaths	Available functions for this device.
devices_glyphicon	Glyph Icon Path.
devices_hardwareids	Hardware Ids.
devices_icon	Icon Path.
devices_inlocalmachinecontainer	Device is in the local machine container.
devices_interfaceclassguid	Interface Class Guid.

devices_interfaceenabled	Indicates if the interface is enabled or not.
devices_interfacepaths	Available interfaces for this device.
devices_ipaddress	IP address of the device.
devices_isdefault	If this property is true, the device is the default device.
devices_isnetworkconnected	If this property is true, the device is connected to a network.
devices_isshared	If this property is true, the device is a shared device.
devices_issoftwareinstalling	If VARIANT.TRUE, the device installer is currently installing software.
devices_launchdevicestagefromexplorer	Indicates whether to launch Device Stage.
devices_localmachine	If true, the device in question is the computer.
devices_locationpaths	Device LocationPaths.
devices_manufacturer	Device manufacturer.
devices_metadatapath	Path to metadata for the device.
devices_microphonearray_geometry	Geometry data for the microphone array.
devices_missedcalls	Number of missed calls on the device.
devices_modelid	Model Id.
devices_modelname	Model name of the device.
devices_modelnumber	Model number of the device.
devices_networkedtooltip	Tool tip for connection state.
devices_networkname	Name of the device's network.
devices_networktype	Represents the type of the device's network.
devices_newpictures	Number of new pictures on the device.
devices_notification	Device notification.
devices_notifications_lowbattery	Device low battery notification.
devices_notifications_missedcall	Device missed call notification.
devices_notifications_newmessage	Device new message notification.
devices_notifications_newvoicemail	Device voicemail notification.
devices_notifications_storagefull	Device storage-full notification.
devices_notifications_storagefulllinktext	Link text for the device storage-full notification.
devices_notificationstore	Device notification store.
devices_notworkingproperly	If VARIANT.TRUE, the device is not working properly.
devices_paired	Device paired state. If true, indicates that the device is not paired with the computer.
devices_parent	Parent device.
devices_physicaldevicelocation	ACPI_PLD data for the device.

devices_playbackpositionpercent	The playback position on the device, as a percentage.
devices_playbackstate	The playback state of the device.
devices_playbacktitle	The current playback title on the device.
devices_present	Device is present.
devices_presentationurl	URL of a human readable webpage on the device.
devices_primarycategory	Primary category group for this device.
devices_remainingduration	The remaining playing time on the device, in 100ns units.
devices_restrictedinterface	Indicates if the interface is restricted.
devices_roaming	Indicates whether the device is roaming.
devices_saferemovalrequired	Indicates whether a device requires safe removal.
devices_serviceaddress	Endpoint address of the device service.
devices_serviceid	Identifier of the device service.
devices_sharedtooltip	Tooltip for the sharing state.
devices_signalstrength	Device signal strength.
devices_smartcards_readerkind	Smart card reader kind.
devices_status	Array of device status strings.
devices_status1	First line of the device status.
devices_status2	Second line of the device status.
devices_storagecapacity	Total storage capacity of the device.
devices_storagefreespace	Total free space on the storage device.
devices_storagefreespacepercent	Total free storage space on the device, as a percentage.
devices_textmessages	Number of unread messages on the device.
devices_voicemail	Indicates whether the device supports voicemail.
devices_wiadevicetype	Windows Image Acquisition (WIA) device type.
devices_wifi_interfaceguid	Wi-Fi Interface Guid.
devices_wifidirect_deviceaddress	Wi-Fi Direct Device Address.
devices_wifidirect_groupid	Wi-Fi Direct Group Id.
devices_wifidirect_informationelements	Indicates full set of IEs provided by the Wi-Fi Direct Device.
devices_wifidirect_interfaceaddress	Wi-Fi Direct Interface Address.
devices_wifidirect_interfaceguid	Wi-Fi Direct Interface GUID.
devices_wifidirect_isconnected	Indicates Wi-Fi Direct Device's Connectivity State.
devices_wifidirect_islegacydevice	Indicates if Wi-Fi Direct Device is a legacy device.

devices_wifidirect_ismiracastlcpsupported	Indicates if link content protection is supported by the Wi-Fi Direct Device if it is Miracast capable.
devices_wifidirect_isvisible	Indicates Wi-Fi Direct Device's Current Visibility.
devices_wifidirect_miracastversion	Indicates version of Miracast protocol if Wi-Fi Direct Device is Miracast capable.
devices_wifidirect_services	Indicates services supported by the Wi-Fi Direct Device.
devices_wifidirect_supportedchannellist	Wi-Fi Direct device's channel list.
devices_wifidirectservices_advertisementid	Wi-Fi Direct Services Advertisement Id.
devices_wifidirectservices_requestserviceinformation	Wi-Fi Direct Services Request Service Information.
devices_wifidirectservices_serviceaddress	Wi-Fi Direct Services Service Address.
devices_wifidirectservices_serviceconfigmethods	Wi-Fi Direct Services Configuration Methods.
devices_wifidirectservices_serviceinformation	Wi-Fi Direct Services Service Information.
devices_wifidirectservices_servicename	Wi-Fi Direct Services Service Name.
devices_winphone8cameraflags	Flags for a WP8 camera device.
devices_wwan_interfaceguid	WWAN Interface Guid.
document_datecreated	Indicates the date and time that a document was created. This information is stored in the document, not obtained from the file system.
document_dateprinted	Indicates the date and time the document was last printed. The legacy name is 'DocLastPrinted'.
document_datesaved	Indicates the date and time the document was last saved. The legacy name is 'DocLastSavedTm'.
document_security	Access control information, from SummaryInfo propset.
document_totaleditingtime	This property represents the total time between each open and save, accumulated since the creation of the document. This is measured in 100ns units, not milliseconds. VT.FILETIME for IPropertySetStorage handlers (legacy).
drm_dateplayexpires	Indicates when play rights expire.
drm_dateplaystarts	Indicates when play rights begin.
drm_description	Displays the description for Digital Rights Management (DRM).
drm_isdisabled	Indicates whether the media file has been disabled by DRM.
drm_isprotected	Indicates whether the file is protected under Digital Rights Management (DRM).
drm_playcount	Indicates the number of times the file has been played.
edgegesture_disabletouchwhenfullscreen	Prevents edge gesture behaviors when an application window is active and in full-screen mode (or an owned window is active).
expandoproperties	Properties that are not stored in the item itself, where the properties are in the form of a stream containing a SERIALIZEDPROPSTORAGE.
fileattributes	The attributes of the item. These are equivalent to the values recognized in the dwFileAttributes member of the WIN32_FIND_DATA structure.

filedescription	A user-friendly description of the file.
fileextension	Identifies the file extension of the file-based item, including the leading period.
filefrn	The unique file ID, also known as the File Reference Number.
filename	The file name, including its extension.
fileofflineavailabilitystatus	Null indicates the normal case (file is available offline). The partial case is only for folders where some content may be available offline and some may not.
fileowner	The owner of the file, as known by the file system.
fileplaceholderstatus	Contains the placeholder file's status flags.
finddata	Contains the WIN32_FIND_DATA structure as a buffer of bytes. Do not use this property for any other purpose.
flagcolortext	The user-friendly form of FlagColor. This value is not intended to be parsed programmatically.
flagstatus	'The status of a flag. Values: (0=none 1=white 2=Red).'
flagstatustext	The user-friendly form of FlagStatus. This value is not intended to be parsed programmatically.
folderkind	This property represents the types of content stored in this folder specified by the storage provider.Each folder type must be one of the known value specified by Kind definition FolderKind is a readonly property, it should only be updated by the storage provider.
foldernamedisplay	This property is similar to ItemNameDisplay except it is only set for folders, for files it will be empty.
freespace	The amount of free space in a volume, in bytes.
fulltext	This property is used to specify search terms that should be applied as broadly as possible across all valid properties for the data source(s) being searched. It should not be emitted from a data source.
gps_altitude	Indicates altitude based on the reference in GPS_AltitudeRef.
gps_altitudedenominator	The denominator of GPS_Altitude.
gps_altitudenumerator	The numerator of GPS_Altitude.
gps_altituderef	Indicates the reference for the altitude property (for example, above sea level, below sea level, absolute value).
gps_areainformation	Represents the name of the GPS area.
gps_date	The date and time of the GPS record.
gps_destbearing	Indicates the bearing to the destination point. Calculated from GPS_DestBearingNumerator and GPS_DestBearingDenominator.
gps_destbearingdenominator	The denominator of GPS_DestBearing.
gps_destbearingnumerator	The numerator of GPS_DestBearing.
gps_destbearingref	Indicates the reference used for giving the bearing to the destination point (for example,true direction, magnetic direction).
gps_destdistance	Indicates the distance to the destination point.
gps_destdistancedenominator	The denominator of GPS_DestDistance.
gps_destdistancenumerator	The numerator of GPS_DestDistance.
gps_destdistanceref	Indicates the unit used to express the distance to the destination (for example, kilometers, miles, knots).
gps_destlatitude	Learn how the GPS_DestLatitude property indicates the latitude of the destination point.

gps_destlatitudedenominator	The denominator of GPS_DestLatitude.
gps_destlatitudenumerator	The numerator of GPS_DestLatitude.
gps_destlatituderef	Indicates whether the latitude destination point is north or south latitude.
gps_destlongitude	Learn how the GPS_DestLongitude property indicates the longitude of the destination point.
gps_destlongitudedenominator	The denominator of GPS_DestLongitude.
gps_destlongitudenumerator	The numerator of GPS_DestLongitude.
gps_destlongituderef	Indicates whether the longitude destination point is east or west longitude.
gps_differential	Indicates whether differential correction was applied to the GPS receiver.
gps_dop	Indicates the GPS DOP (data degree of precision). Calculated from GPS_DOPNumerator and GPS_DOPDenominator.
gps_dopdenominator	The denominator of GPS_DOP.
gps_dopnumerator	The numerator of GPS_DOP.
gps_imgdirection	Indicates the direction of the image when it was captured. Calculated from GPS_ImgDirectionNumerator and GPS_ImgDirectionDenominator.
gps_imgdirectiondenominator	The denominator of GPS_Img Direction.
gps_imgdirectionnumerator	The numerator of GPS_Img Direction.
gps_imgdirectionref	Indicates reference for giving the direction of the image when it was captured, (for example, true direction, magnetic direction).
gps_latitude	Indicates latitude.
gps_latitudedecimal	Indicates the latitude based on the reference in GPS_LatitudeRef. Calculated from GPS_LatitudeNumerator and GPS_LatitudeDenominator.
gps_latitudedenominator	The denominator of GPS_Latitude.
gps_latitudenumerator	The numerator of GPS_Latitude.
gps_latituderef	Indicates whether latitude is north or south.
gps_longitude	Indicates the longitude.
gps_longitudedecimal	Indicates the longitude based on the reference in GPS_LongitudeRef. Calculated from GPS_LongitudeNumerator and GPS_LongitudeDenominator.
gps_longitudedenominator	The denominator of GPS_Longitude.
gps_longitudenumerator	The numerator of GPS_Longitude.
gps_longituderef	Indicates whether longitude is east or west.
gps_mapdatum	Indicates the geodetic survey data used by the GPS receiver.
gps_measuremode	Indicates the GPS measurement mode (for example, two-dimensional, three-dimensional).
gps_processingmethod	Indicates the name of the method used for finding locations.
gps_satellites	Indicates the GPS satellites used for measurements.
gps_speed	Indicates the speed of the GPS receiver movement.
gps_speeddenominator	The denominator of GPS_Speed.
gps_speednumerator	The numerator of GPS_Speed.

gps_speedref	Indicates the unit used to express the speed of the GPS receiver movement, (for example,kilometers per hour, miles per hour, knots).
gps_status	Indicates the status of the GPS receiver when the image was recorded (for example, measurement in progress, measurement interoperability).
gps_track	Indicates the direction of the GPS receiver movement.
gps_trackdenominator	The denominator of GPS_Track.
gps_tracknumerator	The numerator of GPS_Track.
gps_trackref	Indicates reference for the direction of the GPS receiver movement (for example, true direction, magnetic direction).
gps_versionid	Indicates the version of the GPS information.
highkeywords	The high confidence keywords for the item.
history_selectioncount	The count of instances the user has selected the item.
history_targeturlhostname	Mark of the Web zone, as URLZONE enumeration value.
identity_blob	Blob used to import and export identities.
identity_internetsid	The internet SID of an identity.
identity_keyprovidercontext	Identity key provider context.
identity_keyprovidername	Identity key provider name.
identity_logonstatusstring	A string that indicates the user logon status of an identity.
identity_primaryemailaddress	Primary e-mail address.
identity_primarysid	The primary SID of an identity.
identity_providerdata	The provider's custom data for an identity.
identity_providerid	This property specifies the Provider ID.
identity_qualifiedusername	The qualified user name of an identity.
identity_uniqueid	A unique identifier for an identity.
identity_username	User name for an identity.
identityprovider_name	Identity provider name.
identityprovider_picture	Picture for the identity provider.
image_bitdepth	Indicates how many bits are used in each pixel of the image. (Usually 8, 16, 24, or 32).
image_colorspace	The colorspace embedded in the image. Taken from the Exchangeable Image File (EXIF) information.
image_compressedbitsperpixel	Indicates the image compression level.
image_compressedbitsperpixeldenominator	The denominator of Image_CompressedBitsPerPixel.
image_compressedbitsperpixelnumerator	The numerator of Image_CompressedBitsPerPixel.
image_compression	The algorithm used to compress the image.
image_compressiontext	The user-friendly form of Image_Compression. Not intended to be parsed programmatically.
image_dimensions	The image dimensions in string format as horizontal pixels x vertical pixels. For example, 3080x2100.
image_horizontalresolution	Indicates the number of pixels per resolution unit in the image width.

image_horizontalsize	The horizontal size of the image, in pixels.
image_resolutionunit	Indicates the resolution units. Used for images with a non-square aspect ratio, but without meaningful absolute dimensions. 1 = No absolute unit of measurement. 2 = Inches. 3 = Centimeters. The default value is 2 (Inches).
image_verticalresolution	Indicates the number of pixels per resolution unit in the image height.
image_verticalsize	The vertical size of the image, in pixels.
imageparsingname	Image parsing name.
importancetext	The user-friendly form of Importance. This value is not intended to be parsed programmatically.
infotiptext	The text (with formatted property values) to show in the infotip.
internalname	The name of a .exe or .dll file as stored in a resource section within that file.
isattachment	Identifies whether the item is an attachment.
isdefaultnonownersavelocation	Identifies the default save location for a library for non-owners of the library.
isdefaultsavelocation	Identifies the default save location for a library for the owner of the library.
isencrypted	Identifies whether the item is encrypted.
isincomplete	Identifies whether the message was completely received. This value is used with some error conditions.
islocationsupported	Identifies whether a location was indexed (locally or remotely) at the time it was added to the library.
ispinnedtonamespacetree	Identifies whether a shell folder is pinned to the navigation pane.
isread	Identifies whether the item has been read.
issearchonlyitem	Identifies whether a location or a library is search only.
issendtotarget	Indicates whether an item is a valid SendTo target. This information is provided by certain Shell folders.
isshared	Indicates whether the item is shared. This checks only the non-inherited ACLs.
itemauthors	Generic list of authors associated with an item. For example, the artist name for a music track is the item author.
itemclasstype	Class type of the item.
itemdate	The primary date of interest for an item. In the case of photos, for example, this property maps to Photo_DateTaken.
itemfoldernamedisplay	The user-friendly display name of an item's parent folder.
itemfolderpathdisplay	Read about the ItemFolderPathDisplay property, which represents the user-friendly display path of an item's parent folder.
itemfolderpathdisplaynarrow	Read about the ItemFolderPathDisplayNarrow property, which represents the user-friendly display path of an item's parent folder.
itemname	The base name of the ItemNameDisplay property.
itemnamedisplay	The display name in 'most complete' form.
itemnamedisplaywithoutextension	This is similar to ItemNameDisplay except that it never includes a file extension.
itemnameprefix	The prefix of an item, used for e-mail messages where the subject begins with the prefix 'Re:'.
itemnamesortoverride	This string should be set to the phonetic version of the display name as defined in ItemNameDisplay in CJK locales(CHS Pinyin, JPN Hiragana, KOR Hangul, etc.).
itemparticipants	The generic list of people associated with and contributing to an item.

itempathdisplay	Read about the ItemPathDisplay property, which represents the user-friendly display path to the item.
itempathdisplaynarrow	Read about the ItemPathDisplayNarrow property, which represents the user-friendly display path to the item.
itemsubtype	Describes the sub-type of an item.
itemtype	The canonical type of the item.
itemtypetext	The user-friendly type name of the item.
itemurl	Represents a well-formed URL that points to the item.
keywords	The set of keywords (also known as 'tags') assigned to the item.
kind	Maps extensions to various .Search folders.
kindtext	The user-friendly form of Kind. This value is not intended to be parsed programmatically.
language	The primary language of the file, particularly if that file is a document.
lastwriterpackagefamilyname	Mark of the app container. The package family name of the last app to edit the file's contents.
layoutpattern_contentviewmodeforbrowse	Identifies the layout pattern that the content view mode should apply for this item in the context of browsing.
layoutpattern_contentviewmodeforsearch	Identifies the layout pattern that the content view mode should apply for this item in the context of searching.
librarylocationscount	Indicates the number of library locations.
link_status	Specifies whether the link path in Link.TargetParsingPath is verified.
link_targetextension	The file extension of the link target. See FileExtension.
link_targetparsingpath	The Shell namespace path to the target of the link item.
link_targetsfgaoflags	The IShellFolder::GetAttributesOf flags for the target of a link, with SFGAO_PKEYSFGAOMASK attributes masked out.
link_targetsfgaoflagsstrings	Expresses the SFGAO flags of a link as string values, and is used as a query optimization.
lowkeywords	The low confidence keywords for the item.
media_dateencoded	Represents the date and time the file was encoded. The DateTime is in UTC (in the doc, not file system).
media_dlnaprofileid	The DLNA profile ID for media content, defined by DLNA standards.
media_duration	Represents the actual play time of a media file and is measured in 100ns units, not milliseconds.
media_episodenumber	A 1 based monotonically incremented number that corresponds to the episode of the show.
media_framecount	Indicates the frame count for the image.
media_protectiontype	Describes the type of media protection.
media_providerrating	The rating (0 - 99) supplied by metadata provider.
media_providerstyle	The style of music or video, supplied by metadata provider.
media_seasonnumber	A 1 based monotonically incremented number that corresponds to the season that the show was first presented.
media_seriesname	A name that represents a specific series, such as a podcast or recorded television series.
media_thumbnaillargepath	The Media_ThumbnailLargePath property contains the filesystem path to the large thumbnail representation of the media item.
media_thumbnaillargeuri	Understand the Media_ThumbnailLargeUri property, which represents the URI of the large thumbnail representation of the media item.
media_thumbnailsmallpath	The Media_ThumbnailSmallPath property contains the filesystem path to the small thumbnail representation of the media item.

media_thumbnailsmalluri	Understand the Media_ThumbnailSmallUri property, which represents the URI of the small thumbnail representation of the media item.
media_usernoautoinfo	If true, do not alter this file's metadata. Set by user.
mediumkeywords	The medium confidence keywords for the item.
message_attachmentnames	The names of the attachments in a message.
message_bccaddress	'The addresses in the Bcc: field.'
message_bccname	'The names of people in the Bcc: field.'
message_ccaddress	'The addresses in the Cc: field.'
message_ccname	'The names of people in the Cc: field.'
message_datereceived	The date and time a communication was received.
message_datesent	The date and time a communication was sent.
message_flags	Flags associated with e-mail messages (identifying that a read receipt is pending, for example). The values stored here by Outlook are defined for PR_MESSAGE_FLAGS.
message_fromname	'The names of people in the From: field.'
message_messageclass	The type of Microsoft Outlook message (meeting, task, mail, and so on).
message_participants	Participants in communication.
message_proofinprogress	Identifies whether the message junk e-mail proofing is still in progress.
message_store	The store (also known as the protocol handler) FILE, MAIL, OUTLOOKEXPRESS.
message_toaddress	'The addresses in the To: field.'
message_todoflags	Identifies whether a message is flagged as a to-do item.
message_toname	'The names of people in the To: field.'
mimetype	The MIME type.
music_albumartistsortoverride	This optional string value allows for overriding the standard sort order of Music_AlbumArtist.This is very important for proper sorting of music files in Japanese which cannot becorrectly sorted phonetically (the user-expected ordering) without this field.It can also be used for customizing sorting in non-East Asian scenarios,such as allowing the user to remove articles for sorting purposes.
music_albumid	This property differentiates albums with the same title from different artists. It is the concatenation of Music_AlbumArtist and Music_AlbumTitle.
music_albumtitlesortoverride	This optional string value allows for overriding the standard sort order of Music_Album.This is very important for proper sorting of music files in Japanese which cannot becorrectly sorted phonetically (the user-expected ordering) without this field.It can also be used for customizing sorting in non-East Asian scenarios,such as allowing the user to remove articles for sorting purposes.
music_artistsortoverride	This optional string value allows for overriding the standard sort order of Music_Artist.This is very important for proper sorting of music files in Japanese which cannot becorrectly sorted phonetically (the user-expected ordering) without this field.It can also be used for customizing sorting in non-East Asian scenarios,such as allowing the user to remove articles for sorting purposes.
music_composersortoverride	This optional string value allows for overriding the standard sort order of Music_Composer.This is very important for proper sorting of music files in Japanese which cannot becorrectly sorted phonetically (the user-expected ordering) without this field.It can also be used for customizing sorting in non-East Asian scenarios,such as allowing the user to remove articles for sorting purposes.
music_displayartist	This property returns the best representation of the album artist for a specific music file based upon Music_AlbumArtist, Music_Artist, and Music_IsCompilation information.

music_iscompilation	Indicates whether the music file is part of a compilation.
namespaceclsid	The CLSID of the name space extension for an item, the object that implements IShellFolder for this item.
note_colortext	The user-friendly form of Note_Color. Not intended to be parsed programmatically.
ownersid	SID of the user that owns the library.
parentalrating	The parental rating stored in a format typically determined by the organization named in ParentalRatingsOrganization.
parentalratingreason	Explains file ratings.
parentalratingsorganization	The name of the organization whose rating system is used for ParentalRating.
parsingbindcontext	Used to get the IBindCtx for an item to be parsed.
parsingname	The Shell namespace name of an item relative to a parent folder.
parsingpath	The Shell namespace path to the item.
perceivedtype	The perceived file type based on its canonical type.
percentfull	The amount of space filled, as a percentage.
photo_aperture	The aperture value of the image, in APEX units.
photo_aperturedenominator	The denominator of Photo_Aperture.
photo_aperturenumerator	The numerator of Photo_Aperture.
photo_brightness	The brightness value of the image, in APEX units, usually in the range of -99.99 to 99.99.
photo_brightnessdenominator	The denominator of Photo_Brightness.
photo_brightnessnumerator	The numerator of Photo_Brightness.
photo_cameramanufacturer	The manufacturer name of the camera that took the photo, in a string format.
photo_cameramodel	The model name of the camera that shot the photo, in string form.
photo_cameraserialnumber	The serial number of the camera that produced the photo.
photo_contrast	Indicates the direction of contrast processing applied by the camera when the image was taken. '0' indicates 'Normal'; '1' indicates 'Soft'; '2' indicates 'Hard'.
photo_contrasttext	The user-friendly form of Photo_Contrast. It is not intended to be parsed programmatically.
photo_datetaken	The date when the photo was taken, as read from the camera in the file's Exchangeable Image File (EXIF) tag.
photo_digitalzoom	The digital zoom ratio when the image was shot.
photo_digitalzoomdenominator	The denominator of Photo_DigitalZoom.
photo_digitalzoomnumerator	The numerator of Photo_DigitalZoom.
photo_event	The event where the photo was taken. The end-user provides this value.
photo_exifversion	The Exchangeable Image File (EXIF) version.
photo_exposurebias	The amount of exposure bias used in the photo, as read from the camera.
photo_exposurebiasdenominator	The denominator of Photo_ExposureBias.
photo_exposurebiasnumerator	The numerator of Photo_ExposureBias.
photo_exposureindex	Indicates the exposure index selected on the camera or input device at the time the photo was taken. Calculated from Photo_ExposureIndexNumerator and

	Photo_ExposureIndexDenominator.
photo_exposureindexdenominator	The denominator of Photo_ExposureIndex.
photo_exposureindexnumerator	The numerator of Photo_ExposureIndex.
photo_exposureprogram	The Exposure Program mode of the camera at the time the photo was taken, as read from the Exchangeable Image File (EXIF) information.
photo_exposureprogramtext	The user-friendly form of Photo_ExposureProgram. Not intended to be parsed programmatically.
photo_exposuretime	The exposure time for the photo, in seconds, as read from the Exchangeable Image File (EXIF) information.
photo_exposuretimedenominator	The denominator of Photo_ExposureTime.
photo_exposuretimenumerator	The numerator of Photo_ExposureTime.
photo_flash	An indicator of the flash status when the photo was taken, as read from the Exchangeable Image File (EXIF) info.
photo_flashenergy	Indicates the strobe energy at the time the image was captured, measured in Beam Candle Power Seconds. Calculated from Photo_FlashEnergyNumerator and Photo_FlashEnergyDenominator.
photo_flashenergydenominator	The denominator of Photo_FlashEnergy.
photo_flashenergynumerator	The numerator of Photo_FlashEnergy.
photo_flashmanufacturer	A string indicating the manufacturer of the flash used to take the picture. Can be blank or not present.
photo_flashmodel	String indicating the model of the flash used to take the picture. Can be blank or not present.
photo_flashtext	The user-friendly form of Photo_Flash. Not intended to be parsed programmatically.
photo_fnumber	The FNumber value when the photo was taken, as read from the Exchangeable Image File (EXIF) information.
photo_fnumberdenominator	The denominator of Photo_FNumber.
photo_fnumbernumerator	The numerator of Photo_FNumber.
photo_focallength	The focal length of the lens as recorded by the camera when the photo was taken, measured in millimeters.
photo_focallengthdenominator	The denominator of Photo_FocalLength.
photo_focallengthinfilm	The focal length of the lens when the photo was taken, as converted to a 35mm film measurement.
photo_focallengthnumerator	The numerator of Photo_FocalLength.
photo_focalplanexresolution	Indicates the number of pixels in the image width (X direction) per FocalPlaneResolutionUnit on the camera focal plane. Calculated from Photo_FocalPlaneXResolutionNumerator and Photo_FocalPlaneXResolutionDenominator.
photo_focalplanexresolutiondenominator	The denominator of Photo_FocalPlaneXResolution.
photo_focalplanexresolutionnumerator	The numerator of Photo_FocalPlaneXResolution.

photo_focalplaneyresolution	Indicates the number of pixels in the image height (Y direction) per FocalPlaneResolutionUnit on the camera focal plane. Calculated from Photo_FocalPlaneYResolutionNumerator and Photo_FocalPlaneYResolutionDenominator.
photo_focalplaneyresolutiondenominator	The denominator of Photo_FocalPlaneYResolution.
photo_focalplaneyresolutionnumerator	The numerator of Photo_FocalPlaneYResolution.
photo_gaincontrol	Indicates the degree of overall image gain adjustment. Calculated from Photo_GainControlNumerator and Photo_GainControlDenominator.
photo_gaincontroldenominator	The denominator of Photo_GainControl.
photo_gaincontrolnumerator	The numerator of Photo_GainControl.
photo_gaincontroltext	The user-friendly form of Photo_GainControl. Not intended to be parsed programmatically.
photo_isospeed	The International Standards Organization (ISO) speed as recorded by the camera when the photo was taken.
photo_lensmanufacturer	String indicating the manufacturer of the lens used to take the picture. Can be blank or not present.
photo_lensmodel	A string indicating the model of the lens used to take the picture. Can be blank or not present.
photo_lightsource	The light source when the photo was taken, as read from the Exchangeable Image File (EXIF) information.
photo_makernote	The Exchangeable Image File (EXIF) extensibility mechanism that allows camera manufacturers to provide custom information.
photo_makernoteoffset	The offset for the maker note specified in Photo_MakerNote.
photo_maxaperture	The maximum aperture of the lens as recorded by the camera, taken from the Exchangeable Image File (EXIF) information.
photo_maxaperturedenominator	The denominator of Photo_MaxAperture.
photo_maxaperturenumerator	The numerator of Photo_MaxAperture.
photo_meteringmode	The metering mode used by the camera, taken from the Exchangeable Image File (EXIF) information.
photo_meteringmodetext	The user-friendly form of Photo_MeteringMode. Not intended to be parsed programmatically.
photo_orientation	The orientation of the photo when it was taken, as specified in the Exchangeable Image File (EXIF) information and in terms of rows and columns.
photo_orientationtext	The user-friendly form of Photo_Orientation. Not intended to be parsed programmatically.
photo_peoplenames	The people tags on an image.
photo_photometricinterpretation	The pixel composition.
photo_photometricinterpretationtext	The user-friendly form of Photo_PhotometricInterpretation.
photo_programmode	The class of the program used by the camera to set exposure.
photo_programmodetext	The user-friendly form of Photo_ProgramMode. Not intended to be parsed programmatically.
photo_relatedsoundfile	The file name of a sound annotation file associated with the photo.
photo_saturation	Indicates the direction of saturation processing applied by the camera when the photo was taken.

photo_saturationtext	The user-friendly form of Photo_Saturation. Not intended to be parsed programmatically.
photo_sharpness	Indicates the direction of sharpness processing applied by the camera when the photo was taken.
photo_sharpnesstext	The user-friendly form of Photo_Sharpness. Not intended to be parsed programmatically.
photo_shutterspeed	The shutter speed of the camera when the photo was taken. This is given in APEX units.
photo_shutterspeeddenominator	The denominator of Photo_ShutterSpeed.
photo_shutterspeednumerator	The numerator of Photo_ShutterSpeed.
photo_subjectdistance	The distance to the subject in meters. Calculated from Photo_SubjectDistanceNumerator and Photo_SubjectDistanceDenominator.
photo_subjectdistancedenominator	The denominator of Photo_SubjectDistance.
photo_subjectdistancenumerator	The numerator of Photo_SubjectDistance.
photo_tagviewaggregate	A read-only aggregation of tag-like properties for use in building views.
photo_transcodedforsync	A VT.BOOL that indicates whether the image has been transcoded for synchronizing with an external device.
photo_whitebalance	The white balance mode at the time the photo was shot, as taken from the Exchangeable Image File (EXIF) information.
photo_whitebalancetext	The user-friendly form of Photo_WhiteBalance. Not intended to be parsed programmatically.
prioritytext	The user-friendly form of Priority. This value is not intended to be parsed programmatically.
propgroup_advanced	Read about the PropGroup_Advanced property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_audio	Read about the PropGroup.Audio property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_calendar	Read about the PropGroup_Calendar property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_camera	Read about the PropGroup_Camera property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_contact	The property group separator used in property lists to separate contacts from other types. Do not use this property for getting or setting values. This property is intended only as a marker.
propgroup_content	Read about the PropGroup_Content property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_description	The property group separator used in property lists to separate descriptions from other types. Do not use this property for getting or setting values. This property is intended only as a marker.
propgroup_filesystem	Read about the PropGroup_FileSystem property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_general	Read about the PropGroup_General property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_gps	Read about the PropGroup_GPS property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_image	The property group separator used in property lists to separate image files from other types. Do not use this property for getting or setting values. It is intended only as a marker.

propgroup_media	Read about the PropGroup_Media property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_mediaadvanced	Read about the PropGroup_MediaAdvanced property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_message	Read about the PropGroup_Message property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_music	The property group separator used in property lists to separate music files from other types. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_origin	Read about the PropGroup_Origin property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_photoadvanced	Read about the PropGroup_PhotoAdvanced property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_recordedtv	Read about the PropGroup_RecordedTV property. Do not use this property for getting or setting values. It is intended only as a marker.
propgroup_video	The property group separator used in property lists to separate video files from other types. Do not use this property for getting or setting values. It is intended only as a marker.
proplist_conflictprompt	The list of properties to show in the file operation conflict resolution dialog. Properties with empty values will not be displayed.
proplist_contentviewmodeforbrowse	The list of properties to show in the content view mode of an item in the context of browsing.
proplist_contentviewmodeforsearch	Identifies the list of properties to show in the content view mode of an item in the context of searching.
proplist_extendedtileinfo	The list of properties to show in the listview on extended tiles. Register under the regvalue of 'ExtendedTileInfo'.
proplist_fileoperationprompt	The list of properties to show in the file operation confirmation dialog.
proplist_fulldetails	The list of all the properties to show in the details page.
proplist_infotip	The list of properties to show in the infotip. Properties with empty values will not be displayed.
proplist_nonpersonal	The list of properties considered 'non-personal'. The system will leave these properties untouched when directed to remove all non-personal properties from a given file. Register under the regvalue of 'NonPersonal'.
proplist_previewdetails	The list of properties to display in the preview pane. Register under the regvalue of 'PreviewDetails'.
proplist_previewtitle	The one or two properties to display in the preview pane title section.
proplist_quicktip	The list of properties to show in the infotip when the item is on a slow network.
proplist_tileinfo	The list of properties to show in the listview on tiles. Register under the regvalue of 'TileInfo'.
proplist_xpdetailspanel	Obsolete. The list of properties to display in the XP webview details panel.
rating	A rating system that uses integer values between 1 and 99. This is the rating system used by the Windows Vista Shell.
ratingtext	The user-friendly form of Rating. This value is not intended to be parsed programmatically.
recordedtv_channelnumber	The recorded TV channels. For example, 42, 5, 53.
recordedtv_credits	Indicates the credits for the program, in the following format. 'Actor1/Actor2/Actor3...;Director1/Director2/Director3...;Host1/Host2/Host3...;GuestStar'.

recordedtv_episodename	The names of recorded TV episodes. For example, 'Nowhere to Hyde'.
recordedtv_stationcallsign	Any recorded station call signs. For example, 'TOONP'.
search_autosummary	An automated search system summary of the full text contents of a document, displayed in the search results view in Search Explorer. Use this property only when consuming the values in an application, not when providing values to a property handler.
search_containerhash	The hash code used to identify attachments to be deleted based on a common container url.
search_contents	The contents of the item.
search_entryid	The entry ID for an item within a given catalog in the Windows Search Index.
search_gathertime	The Datetime value representing the time when the Windows Search Gatherer process last pushed properties of this document to the Windows Search Gatherer Plugins.
search_hitcount	When using CONTAINS over the Windows Search Index, this is the number of matches of the term. If there are multiple CONTAINS, an AND computes the minimal number of hits, and an OR computes the maximal number of hits.
search_iscloseddirectory	Emitted as TRUE by a container item to indicate that its child items do not need to be enumerated by an indexer if the container item has not changed since the last incremental index verification crawl.
search_isfullycontained	Emitted as TRUE by all child items of a container (such as an e-mail or a compressed file with a .zip name extension) that emits Search_IsClosedDirectory as TRUE. This ensures that the child items are included in the search index.
search_queryfocusedsummary	The query-focused summary of the document.
search_queryfocusedsummarywithfallback	The query-focused summary of the document. If none is available, the AutoSummary is returned.
search_querypropertyhits	Contains the list of matched properties from a query.
search_rank	Relevance rank of row, with a range from 0-1000.
search_store	The identifier for the protocol handler that produced the item. For example, MAPI, CSC, FILE, and so on.
search_urltoindex	Emitted by a container IFilter for each child URL within the container. The children are eventually crawled by the indexer if they are within scope.
search_urltoindexwithmodificationtime	This property is the same as Search_UrlToIndex except that it includes the time that the URL was last modified.
security_allowedenterprisedataprotectionidentities	Encryption options.
security_encryptionowners	Learn about the Security_EncryptionOwners property, which supports file ownership for different versions of Windows.
security_encryptionownersdisplay	Learn about the Security_EncryptionOwnersDisplay property, which supports file ownership for different versions of Windows.
sensitivitytext	The user-friendly form of Sensitivity. This value is not intended to be parsed programmatically.
sfgaoflags	SFGAO values as used in IShellFolder::GetAttributesOf.
sharedwith	Indicates who the item is shared with.
sharingstatus	'Indicates the sharing status of an item: Not Shared, Shared, Everyone (homegroup or everyone), or Private.'
shell_omitfromview	Omits an item from Shell views.

shell_sfgaoflagsstrings	Expresses the SFGAO flags as string values, and is used as a query optimization.
simplerating	A rating system that uses a range of integer values between 0 and 5.
size	The system-provided file system size of the item, in bytes.
sourcepackagefamilyname	Package family name of the app which the storage item instance originated.
status	Generic status information applicable to the item.
statusbarselecteditemcount	The count of selected items in the view and the estimated total size.
statusbarviewitemcount	The count of items in the view and the estimated total size.
storage_portable	Indicates if the drive for the storage is portable.
storage_removablemedia	Indicates if the storage media is removable.
storage_systemcritical	Indicates if the storage media is system critical.
storageprovidercallerversioninformation	The storage provider caller protocol version information.The format of this property is provider specific, refer to the storage provider documentation for more information.
storageproviderfilechecksum	The checksum computed by the storage provider for the file. Files with the same checksum value will have the same contents.
storageproviderfileidentifier	The storage provider identifier for this file.
storageproviderfileremoteuri	The storage provider's remote Uri for this file.
storageproviderfileversion	The storage provider file version for this file.
storageproviderfileversionwaterline	The storage provider computed file version waterline for this file. This value is used to detect if a file has changed.
storageproviderid	This property represents the \[Storage Provider ID\] part of the fully-qualified provider identifier'\Storage Provider ID\Windows SID\Account ID\'.
storageprovidersharestatuses	This property represents a list of share statuses for the file/folder specified by the storage provider.Each share status must be one of the known value specified by the enumerations belowStorageProviderShareStatuses is a readonly property, it should only be updated by the storage provider.
storageprovidersharingstatus	This property represents a the most permissive share status for the file/folder specified by the storage provider.The share statuses from most to least permissive are Owned > Co-owned > Public > Shared > Private.StorageProviderSharingStatus is a readonly property.
subject	The subject of a document. This property maps to the OLE document property Subject.
supplemental_albumid	Contains the identifiers of the albums that the item is a member of. Can be used in conjunction with the Album item in the Content Indexer APIs to notify other apps about picture albums either the user created or apps have already created.
supplemental_resourceid	Contains the identifier for the item on the remote sync service. Used for comparing a file on the system to ones that are available in the cloud.
sync_progresspercentage	An integer value between 0 and 100 that represents the percentage completed.
sync_state	State of the system synch.
sync_status	Status of the system synch.
thumbnail	Represents the thumbnail in VT.CF format.
thumbnailcacheid	A unique value used as a key to cache thumbnails.
thumbnailstream	Data that represents the thumbnail in VT.STREAM format, supported by Windows GDI+ and Windows codecs such as .jpg and .png.
title	The title of the item.

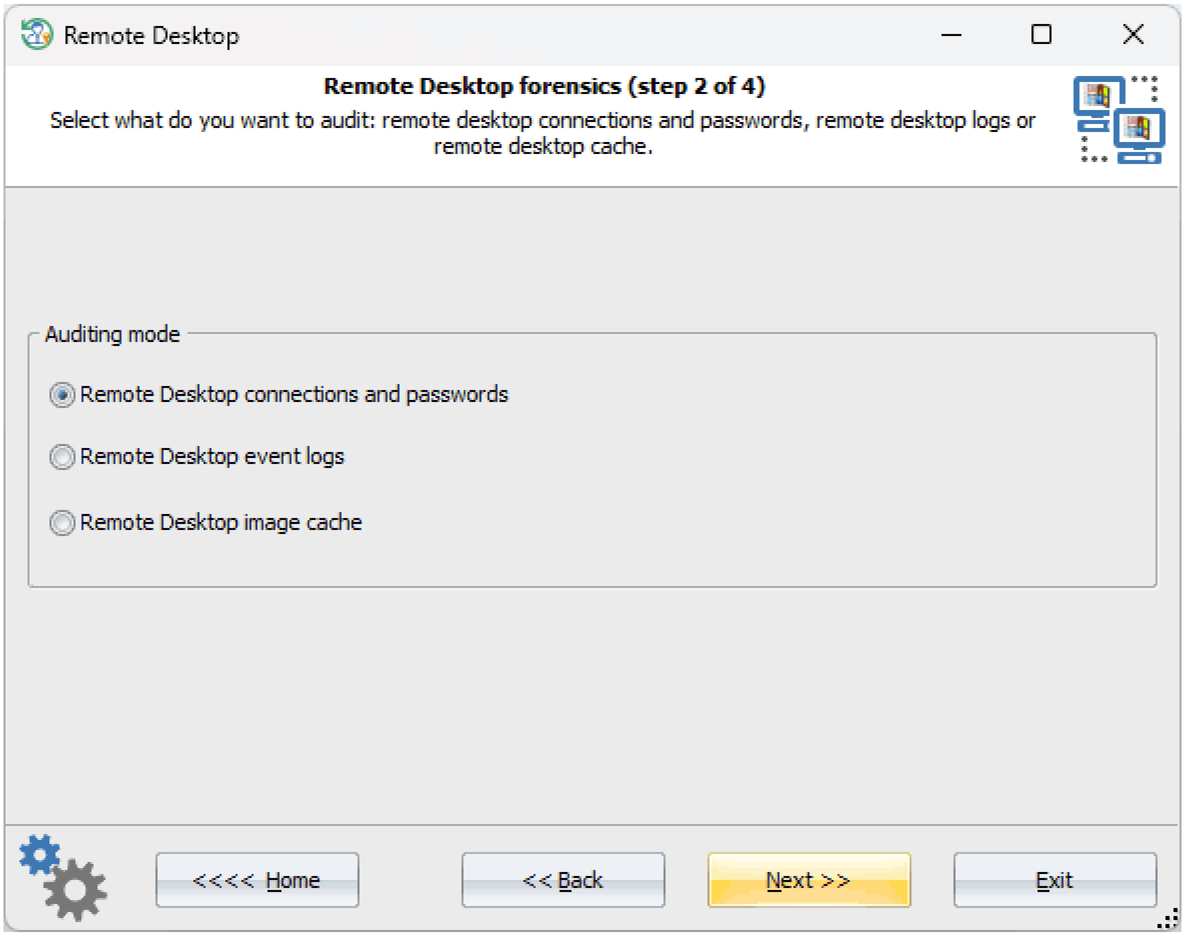
titlesortoverride	This optional string value allows for overriding the standard sort order of Title.This is very important for proper sorting of music files in Japanese which cannot be correctly sorted phonetically (the user-expected ordering) without this field.It can also be used for customizing sorting in non-East Asian scenarios,such as allowing the user to remove articles for sorting purposes.
trademarks	The trademark associated with the item, in a string format.
video_compression	Specifies the video compression format.
video_director	Indicates the person who directed the video.
video_encodingbitrate	Indicates the data rate in 'bits per second' for the video stream. 'DataRate'.
video_fourcc	Specifies the FOURCC code for the video stream.
video_frameheight	Indicates the frame height for the video stream.
video_framerate	Indicates the frame rate for the video stream, in frames per 1000 seconds.
video_framewidth	Indicates the frame width for the video stream.
video_horizontalaspectratio	Indicates the horizontal portion of the pixel aspect ratio. The X portion of XX:YY. For example, 10 is the X portion of 10:11.
video_isspherical	Indicates whether the media file has a spherical video stream.
video_orientation	This is the video orientation in degrees.
video_samplesize	Indicates the sample size in bits for the video stream. 'SampleSize'.
video_streamname	Indicates the name for the video stream. 'StreamName'.
video_streamnumber	Indicates the ordinal number of the stream being played.
video_totalbitrate	Indicates the total data rate in 'bits per second' for all video and audio streams.
video_transcodedforsync	Indicates the vertical portion of the aspect ratio.
video_verticalaspectratio	Indicates the horizontal portion of the pixel aspect ratio. The Y portion of XX:YY. For example, 11 is the Y portion of 10:11 .
volume_filesystem	The name of a volume's file system. This is valid for Shell items that describe a volume.
volume_isroot	A Boolean value stating whether a volume is a root volume.
volumeid	The GUID of the NTFS Volume.
zoneidentifier	Learn about the ZoneIdentifier property, which is the mark of the web zone, as a URLZONE enumeration value.

Experienced users can take advantage of an additional option for creating wordlists containing all indexed words from the search database. These dictionaries can be used later for further analysis or in any password recovery software.

3.7.11 Remote Desktop

This feature of the program provides a forensic information on remote connections via Remote Desktop Protocol in Windows.

The Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft. It allows users to remotely connect to a Windows-based computer over a network connection and access the remote PC's desktop, applications, and files. Once connected, the user can interact with the remote desktop, run applications, and transfer files between the local and remote computers. RDP supports a variety of features, including audio and video redirection, printer and clipboard sharing, and remote assistance.



Remote Desktop forensics (step 2 of 4)

Select what do you want to audit: remote desktop connections and passwords, remote desktop logs or remote desktop cache.

Auditing mode

● Remote Desktop connections and passwords

○ Remote Desktop event logs

○ Remote Desktop image cache

In forensic investigations, it is crucial to gather every possible piece of evidence related to remote connections, including saved login information, activity records, and any images of the remote desktop that may have been cached. This particular section of the program is designed to do just that.

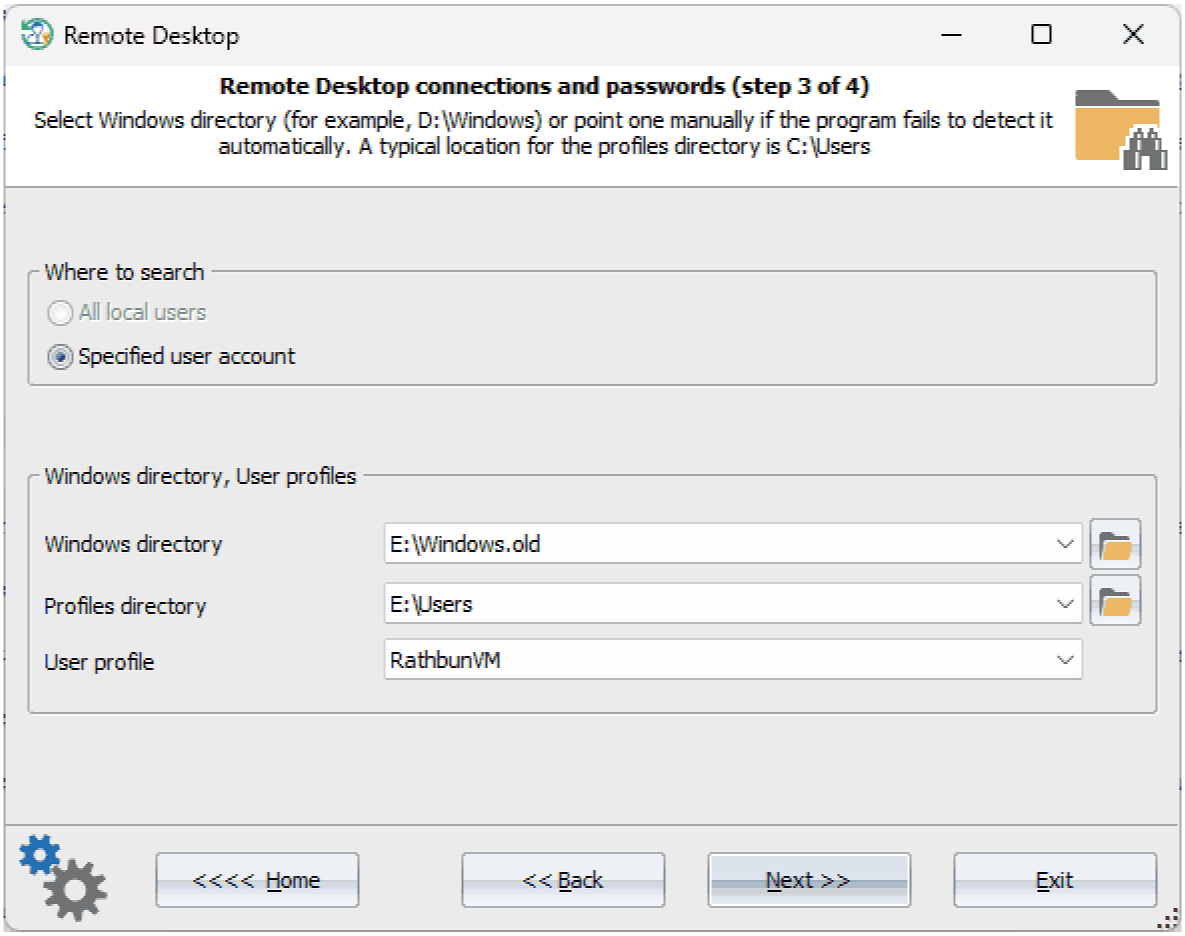
3.7.11.1 Remote Desktop connections and passwords

When a user connects to a remote computer via Remote Desktop Protocol, the credentials of the remote computer are cached locally (assuming the user has selected the appropriate option) to allow for automatic authentication during subsequent connections.

The cached credentials are stored in the Windows Credential Manager, which is a secure storage area for usernames, passwords, and other authentication information, enabling the user to connect to the remote computer later without having to enter their username and password.

The program can enumerate, extract, and decrypt the RDP credentials stored in the Windows Credential Manager in just two simple steps.

Selecting user account



Remote Desktop

Remote Desktop connections and passwords (step 3 of 4)

Select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it automatically. A typical location for the profiles directory is C:\Users

Where to search

○ All local users

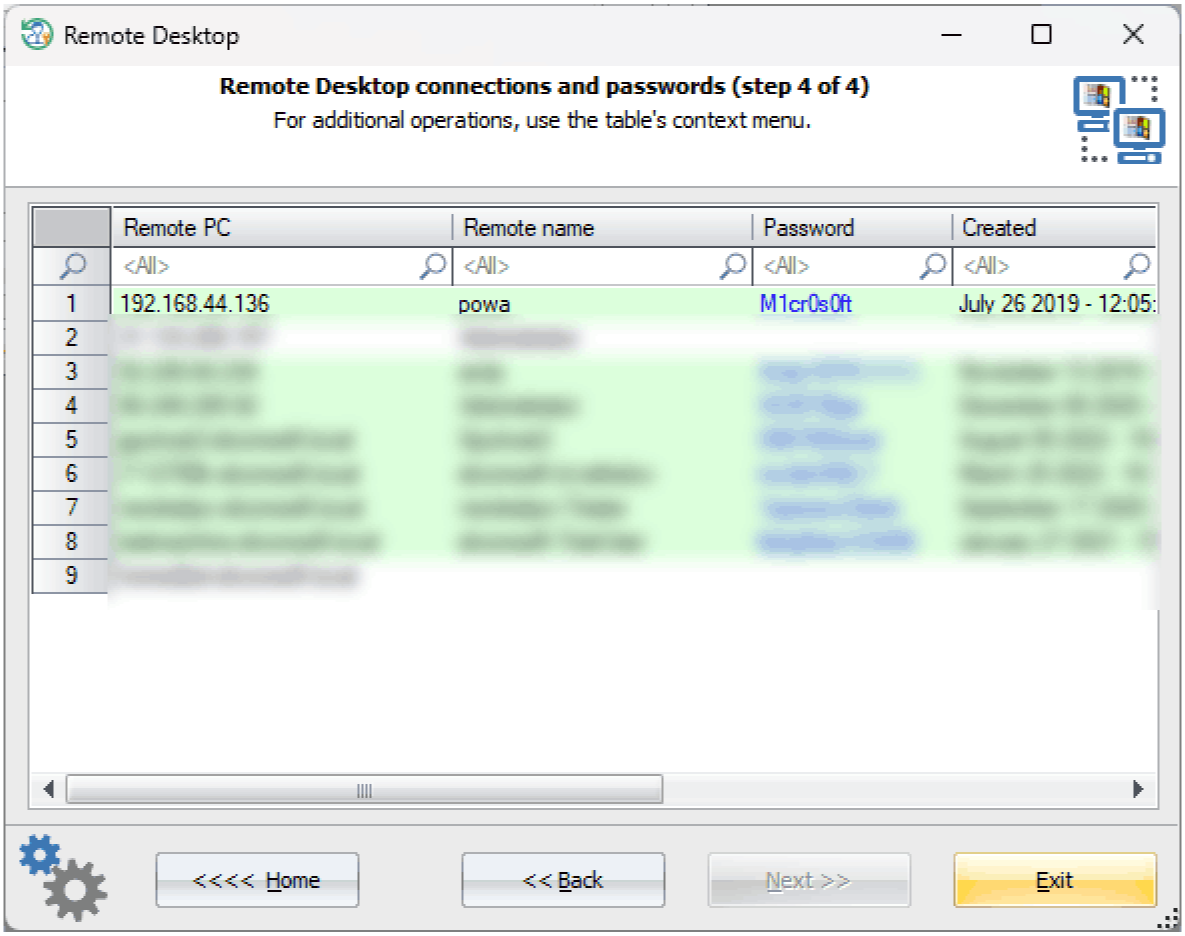
● Specified user account

Windows directory, User profiles

Windows directory	E:\Windows.old
Profiles directory	E:\Users
User profile	RathbunVM

Firstly, input the Windows directory and the user account to be scanned for saved RDP credentials.

Remote desktop connections and passwords



Remote Desktop connections and passwords (step 4 of 4)

For additional operations, use the table's context menu.

	Remote PC	Remote name	Password	Created
	<All>	<All>	<All>	<All>
1	192.168.44.136	powa	M1cr0s0ft	July 26 2019 - 12:05:
2	[redacted]	[redacted]		
3	[redacted]	[redacted]	[redacted]	[redacted]
4	[redacted]	[redacted]	[redacted]	[redacted]
5	[redacted]	[redacted]	[redacted]	[redacted]
6	[redacted]	[redacted]	[redacted]	[redacted]
7	[redacted]	[redacted]	[redacted]	[redacted]
8	[redacted]	[redacted]	[redacted]	[redacted]
9	[redacted]			

If required, provide the account logon password. The program will output all decrypted RDP credentials, along with the address of the remote computer, date connected, and other relevant information.

If you need to decrypt other passwords stored in the Windows Credential Manager, switch to the network password recovery tool.

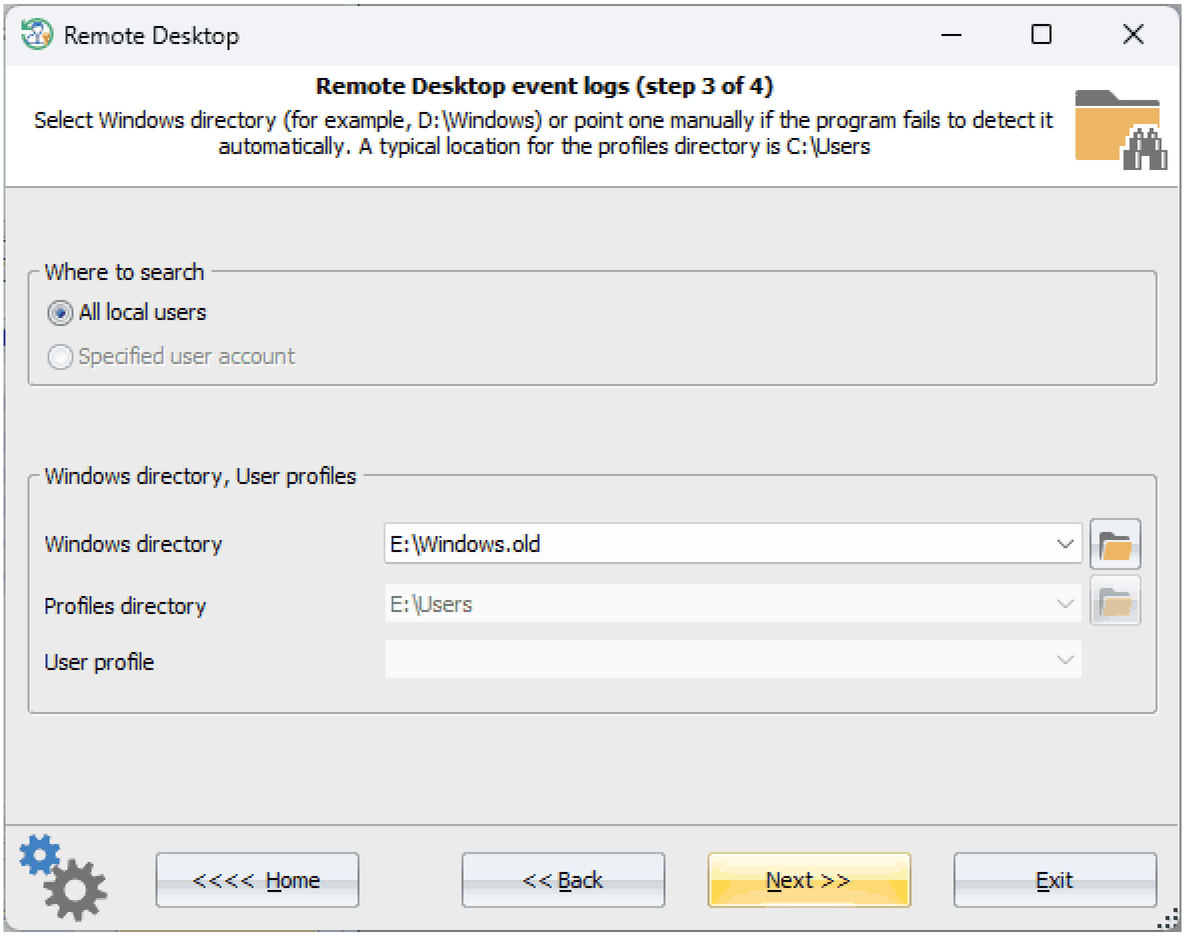
3.7.11.2 Remote Desktop event viewer

When using the Terminal Server Client (also known as Remote Desktop Connection) in Windows, various events related to the client are saved and can be viewed later using the Event Viewer. To view events related to the Terminal Server Client, open the Event Viewer, navigate to the "Applications and Services Logs" section, expand the "Microsoft" folder and select the "TerminalServices-ClientActiveXCore" log.

The Event Viewer is a tool in Windows that allows users to view and manage system and application logs. However, it can only be accessed after logging in to the account. Another issue is that events related to Remote Desktop are scattered across different logs and not restricted to the "TerminalServices-ClientActiveXCore" log.

This program feature overcomes both problems by gathering as many events related to RDP connections as possible, extracting additional data from the "TerminalServices-RemoteConnectionManager," "RemoteDesktopServices-RdpCoreTS," "TerminalServices-LocalSessionManager," "System," and "Security" logs.

Selecting Windows directory



Remote Desktop

Remote Desktop event logs (step 3 of 4)

Select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it automatically. A typical location for the profiles directory is C:\Users

Where to search

● All local users

○ Specified user account

Windows directory, User profiles

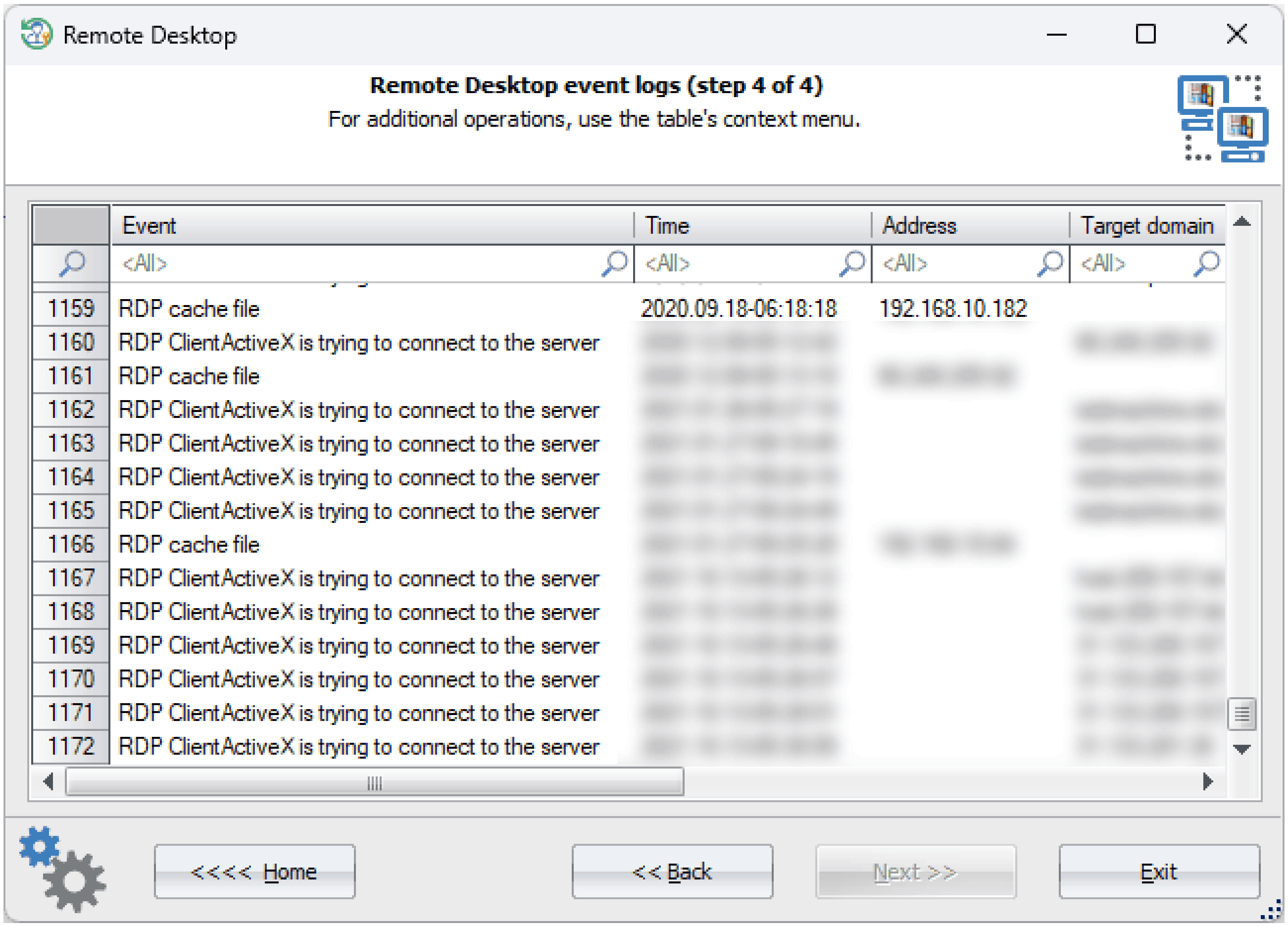
Windows directory: E:\Windows.old

Profiles directory: E:\Users

User profile:

To do this, specify the directory where Windows is located.

Remote desktop events viewer



Remote Desktop event logs (step 4 of 4)

For additional operations, use the table's context menu.

	Event	Time	Address	Target domain
	<All>	<All>	<All>	<All>
1159	RDP cache file	2020.09.18-06:18:18	192.168.10.182	
1160	RDP ClientActiveX is trying to connect to the server	[redacted]		[redacted]
1161	RDP cache file	[redacted]	[redacted]	
1162	RDP ClientActiveX is trying to connect to the server	[redacted]		[redacted]
1163	RDP ClientActiveX is trying to connect to the server	[redacted]		[redacted]
1164	RDP ClientActiveX is trying to connect to the server	[redacted]		[redacted]
1165	RDP ClientActiveX is trying to connect to the server	[redacted]		[redacted]
1166	RDP cache file	[redacted]	[redacted]	
1167	RDP ClientActiveX is trying to connect to the server	[redacted]		[redacted]
1168	RDP ClientActiveX is trying to connect to the server	[redacted]		[redacted]
1169	RDP ClientActiveX is trying to connect to the server	[redacted]		[redacted]
1170	RDP ClientActiveX is trying to connect to the server	[redacted]		[redacted]
1171	RDP ClientActiveX is trying to connect to the server	[redacted]		[redacted]
1172	RDP ClientActiveX is trying to connect to the server	[redacted]		[redacted]

Viewing the found RDP logs. You can use the context menu to save the list as HTML report.

Please note that it may take some time to enumerate and analyze all log items.

3.7.11.3 Remote Desktop image cache

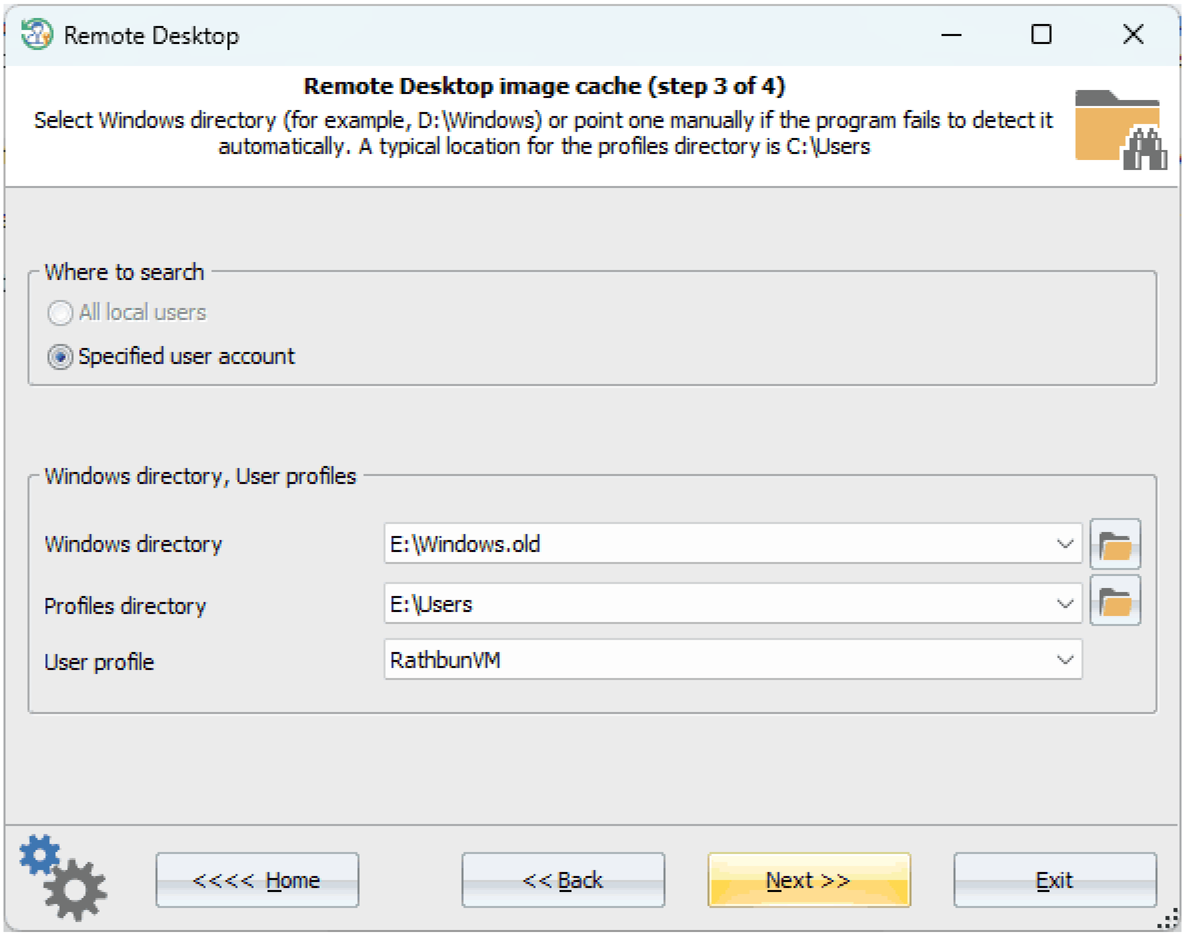
Image caching of the Remote Desktop Protocol in Windows allows to improve the performance of remote connections by storing a copy of the remote desktop screen on the client device. This enables the RDP client to quickly redraw the screen without having to transfer each pixel over the network every time the remote screen updates.
When a remote session is established, the RDP client receives an initial full-screen update from the server and saves it in its cache in memory. It then receives subsequent updates from the remote desktop as delta updates, which describe the changes made to the screen since the last update. This technique drastically improves the responsiveness and speed of remote desktop connections, especially in cases where the network connection has limited bandwidth or high latency.

The contents of the memory cache is then saved to ".bmc" and ".bin" files in the "c:\Users\<user>\AppData\Local\Microsoft\Terminal Server Client\Cache" folder. The binary structure of the ".bmc" and ".bin" files is not publicly documented by Microsoft.

The bitmap cache files consist of tiles, usually 64x64 pixels, with each tile representing a portion of the remote screen. Some tiles of the cache are saved from memory to the ".bin" files, so they are available even after the remote session has ended.

To reconstruct the original image of the remote screen or at least a portion of it, you can use the drag-and-drop operations in the program to swap the tiles. However, it may need a bit of elbow grease.

Selecting remote desktop user



Remote Desktop

Remote Desktop image cache (step 3 of 4)

Select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it automatically. A typical location for the profiles directory is C:\Users

Where to search

○ All local users

● Specified user account

Windows directory, User profiles

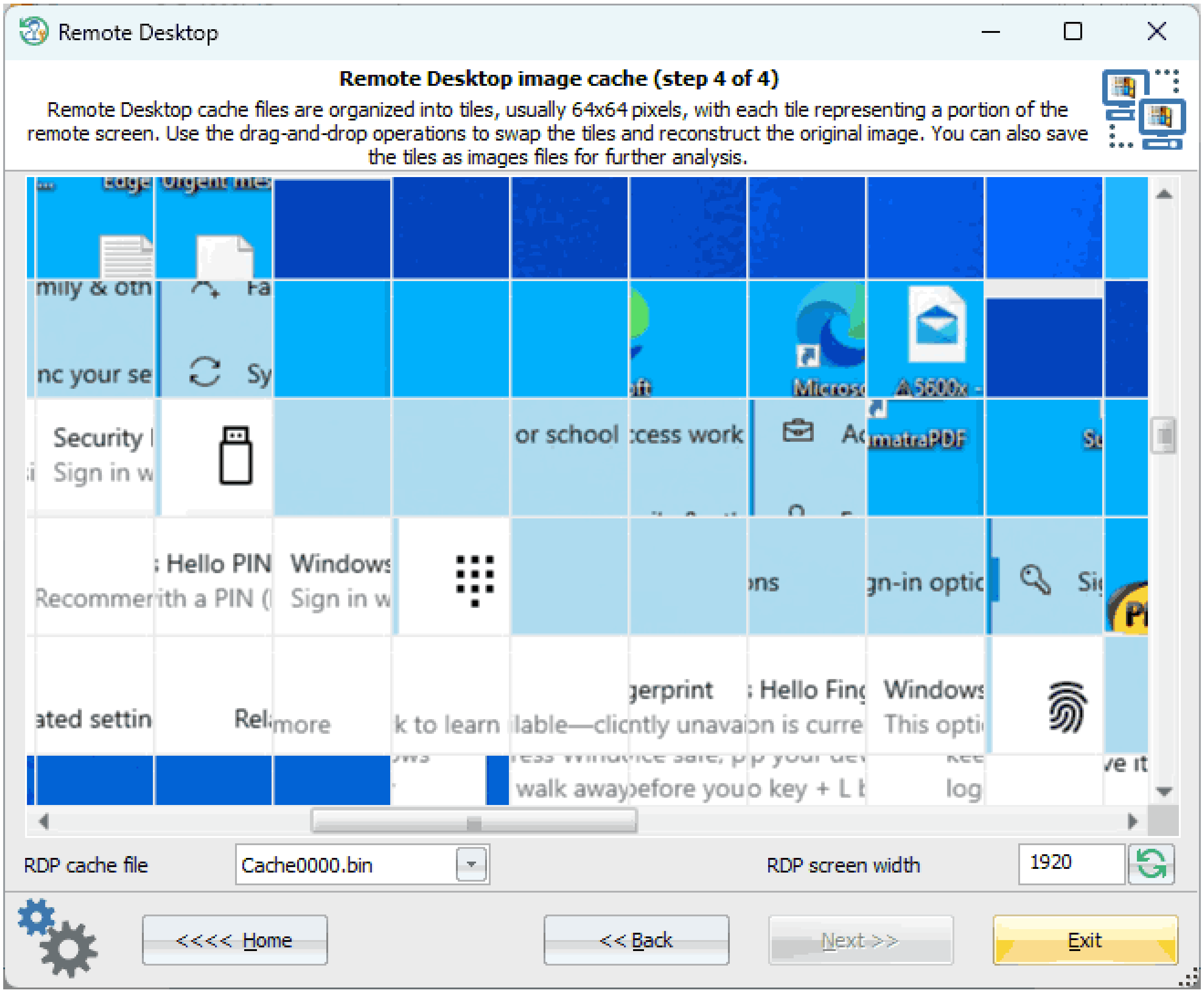
Windows directory: E:\Windows.old

Profiles directory: E:\Users

User profile: RathbunVM

Select the user account to search for the remote desktop cached.

View remote desktop image cache



Remote Desktop image cache (step 4 of 4)

Remote Desktop cache files are organized into tiles, usually 64x64 pixels, with each tile representing a portion of the remote screen. Use the drag-and-drop operations to swap the tiles and reconstruct the original image. You can also save the tiles as images files for further analysis.

RDP cache file: Cache0000.bin

RDP screen width: 1920

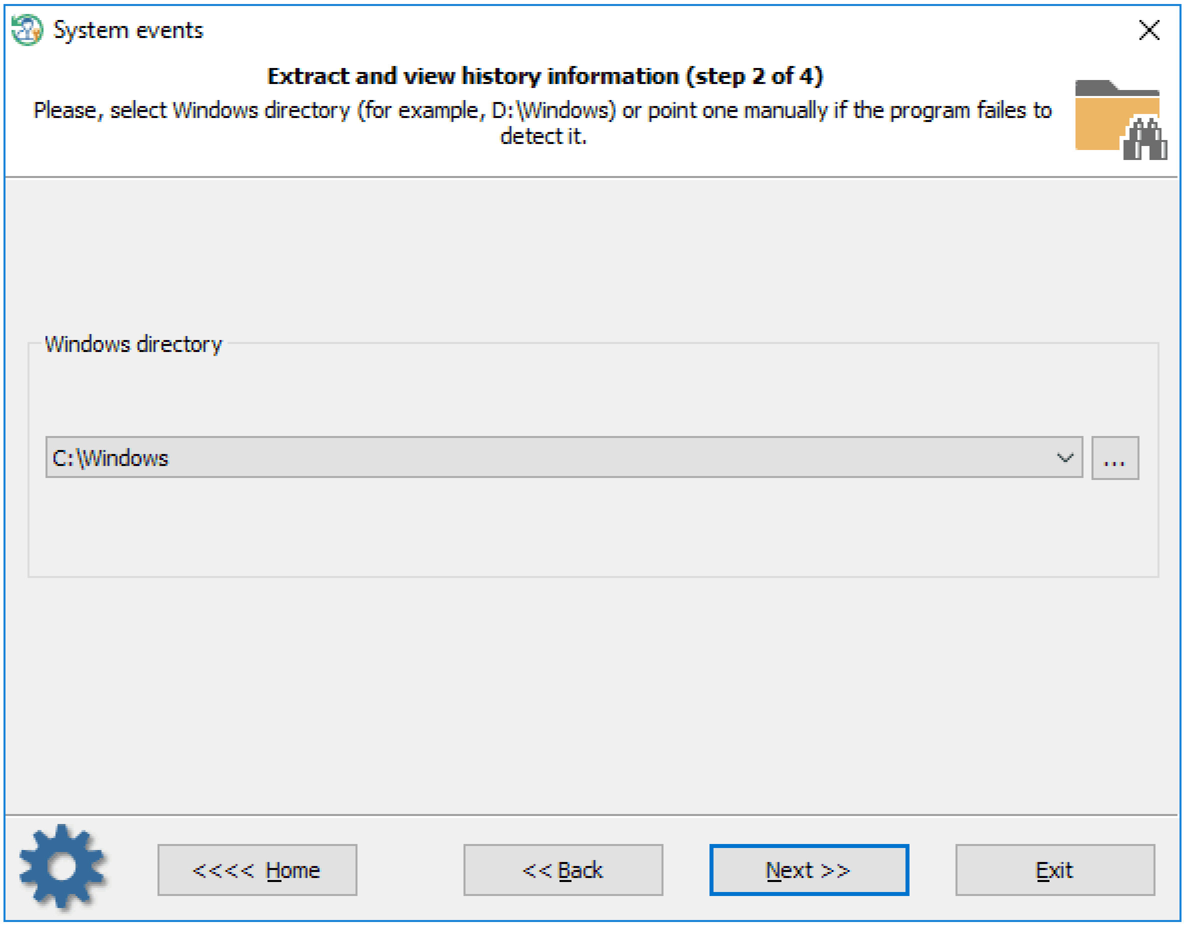
Viewing and editing the RDP cache. Use the drag-and-drop to swap any two tiles. if you want to save the entire bitmap, a separate tile, or all tiles, select the appropriate item from the context menu.

3.7.12 View system events

All Windows OSes log various types of events that occur in the system time to time: errors in device or driver installations, application failures, security notifications, etc. Events help users and administrators to eliminate errors, perform diagnostics and monitoring the system, maintain its security. Events are stored in *.evtx files and are recorded in chronological order. Every evtx file corresponds to a specific event source or to an operating system component. For example, system.evtx keeps tracking of common system notifications. Security.evtx holds all security events. And so on.

The system event viewer is a simple tool allowing to display major events that occur in Windows Vista and later OSes. For example, starting or shutting down the system, logging on/off user accounts, drivers installation, etc.

Selecting Windows directory



System events

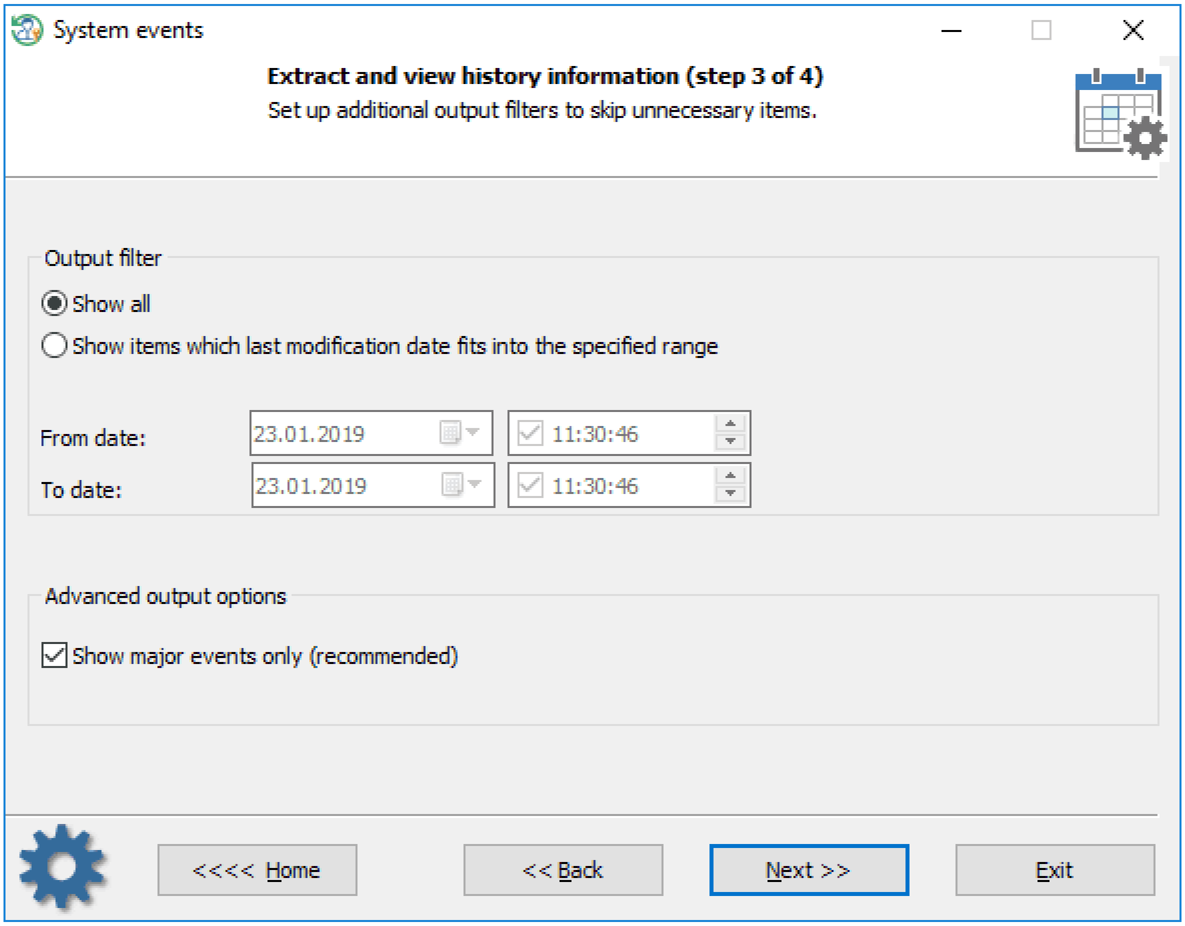
Extract and view history information (step 2 of 4)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program failes to detect it.

Windows directory: C:\Windows

First, you must select the Windows directory that holds the event logs. Typically, C:\Windows or D:\Windows.

Setting output filters



System events

Extract and view history information (step 3 of 4)

Set up additional output filters to skip unnecessary items.

Output filter

● Show all

○ Show items which last modification date fits into the specified range

From date: 23.01.2019 ☑ 11:30:46

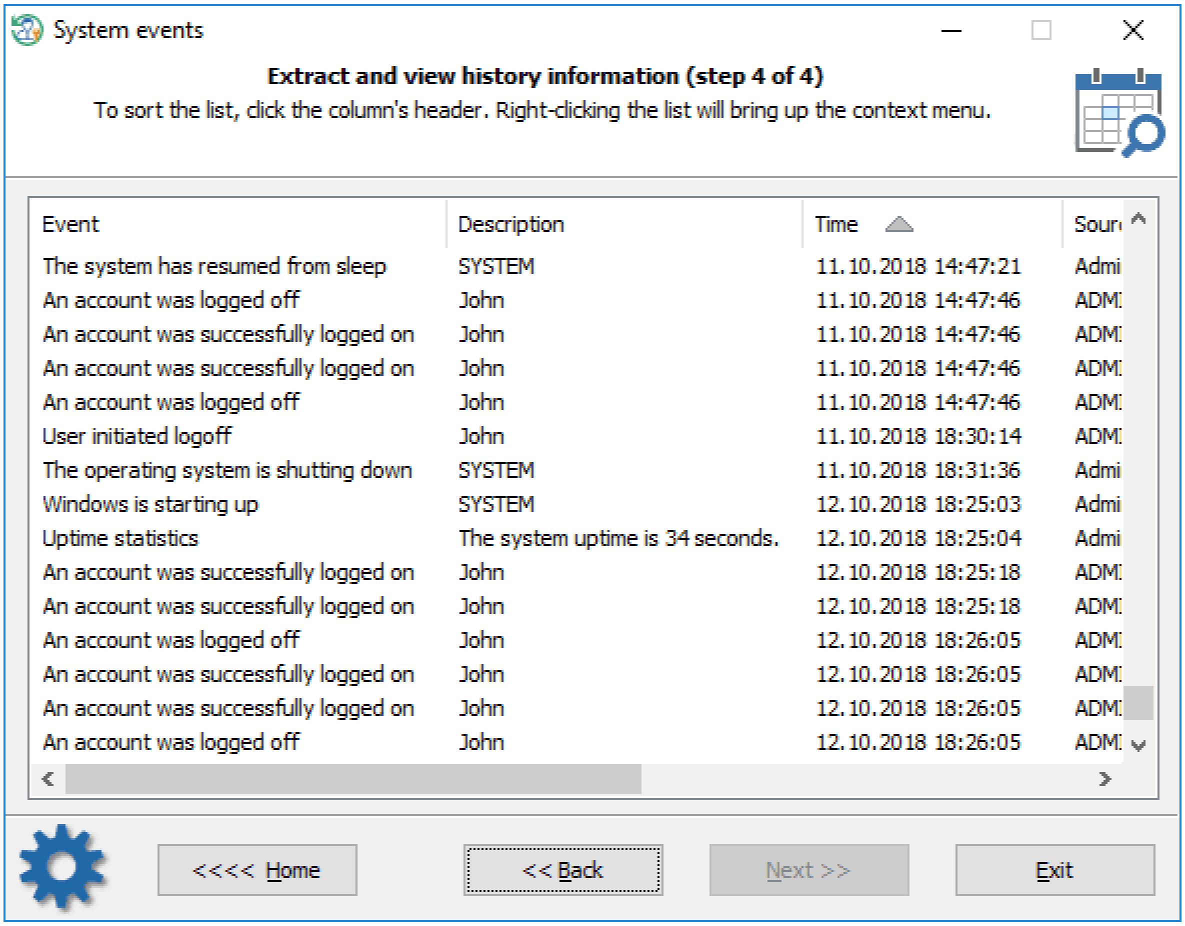
To date: 23.01.2019 ☑ 11:30:46

Advanced output options

☑ Show major events only (recommended)

On the next step, you can additionally configure output filters to display events that occurred in specific time. There's also an option for displaying all events (even unknown to the program). If the option is set, the program outputs known/major events only, all events otherwise.

Viewing Windows events



Extract and view history information (step 4 of 4)

To sort the list, click the column's header. Right-clicking the list will bring up the context menu.

Event	Description	Time	Sour
The system has resumed from sleep	SYSTEM	11.10.2018 14:47:21	Admi
An account was logged off	John	11.10.2018 14:47:46	ADMI
An account was successfully logged on	John	11.10.2018 14:47:46	ADMI
An account was successfully logged on	John	11.10.2018 14:47:46	ADMI
An account was logged off	John	11.10.2018 14:47:46	ADMI
User initiated logoff	John	11.10.2018 18:30:14	ADMI
The operating system is shutting down	SYSTEM	11.10.2018 18:31:36	Admi
Windows is starting up	SYSTEM	12.10.2018 18:25:03	Admi
Uptime statistics	The system uptime is 34 seconds.	12.10.2018 18:25:04	Admi
An account was successfully logged on	John	12.10.2018 18:25:18	ADMI
An account was successfully logged on	John	12.10.2018 18:25:18	ADMI
An account was logged off	John	12.10.2018 18:26:05	ADMI
An account was successfully logged on	John	12.10.2018 18:26:05	ADMI
An account was successfully logged on	John	12.10.2018 18:26:05	ADMI
An account was logged off	John	12.10.2018 18:26:05	ADMI

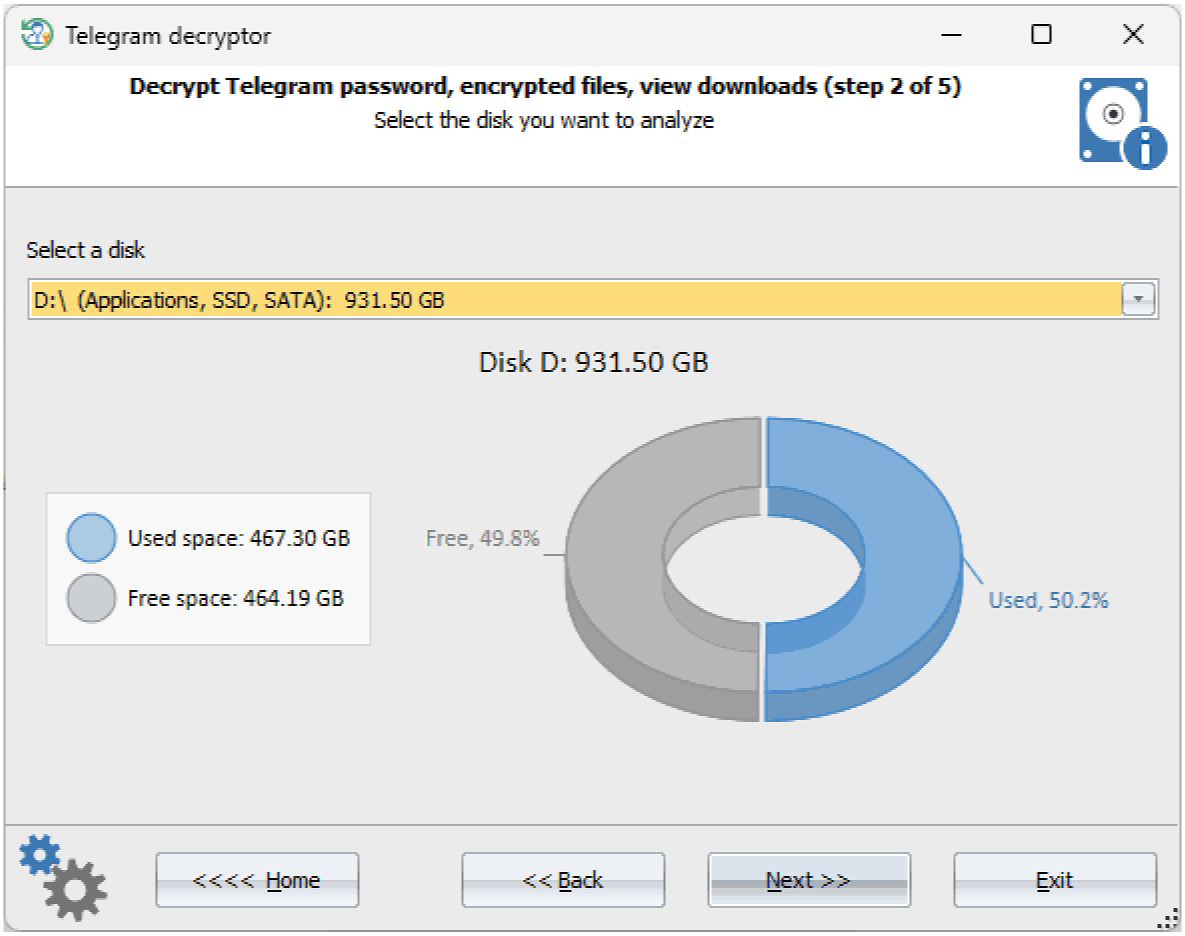
Collecting and processing the information may take considerable time, depending on the size of *.evtx files of the target system. In order to hide some certain records that are of no interest to you, right-click on the list of events and select one of the corresponding menu items. To sort the list, click one of its headers.

3.7.13 Telegram decryptor

As you may know, the popular cross-platform messenger **Telegram** is one of the most widely-used applications for instant message exchanging. The application is available for download and installation on the Windows operating system and is known as **Telegram Desktop**. Telegram provides reliable built-in security. All local data used by the application, such as settings, cache, images, and so on, are securely encrypted.

This feature of the Reset Windows Password is aimed to search for the Telegram passcode, decrypt locally encrypted files, and analyze downloads of the Telegram Desktop application.

Selecting source disk to scan



Telegram decryptor

Decrypt Telegram password, encrypted files, view downloads (step 2 of 5)

Select the disk you want to analyze

Select a disk: D:\ (Applications, SSD, SATA): 931.50 GB

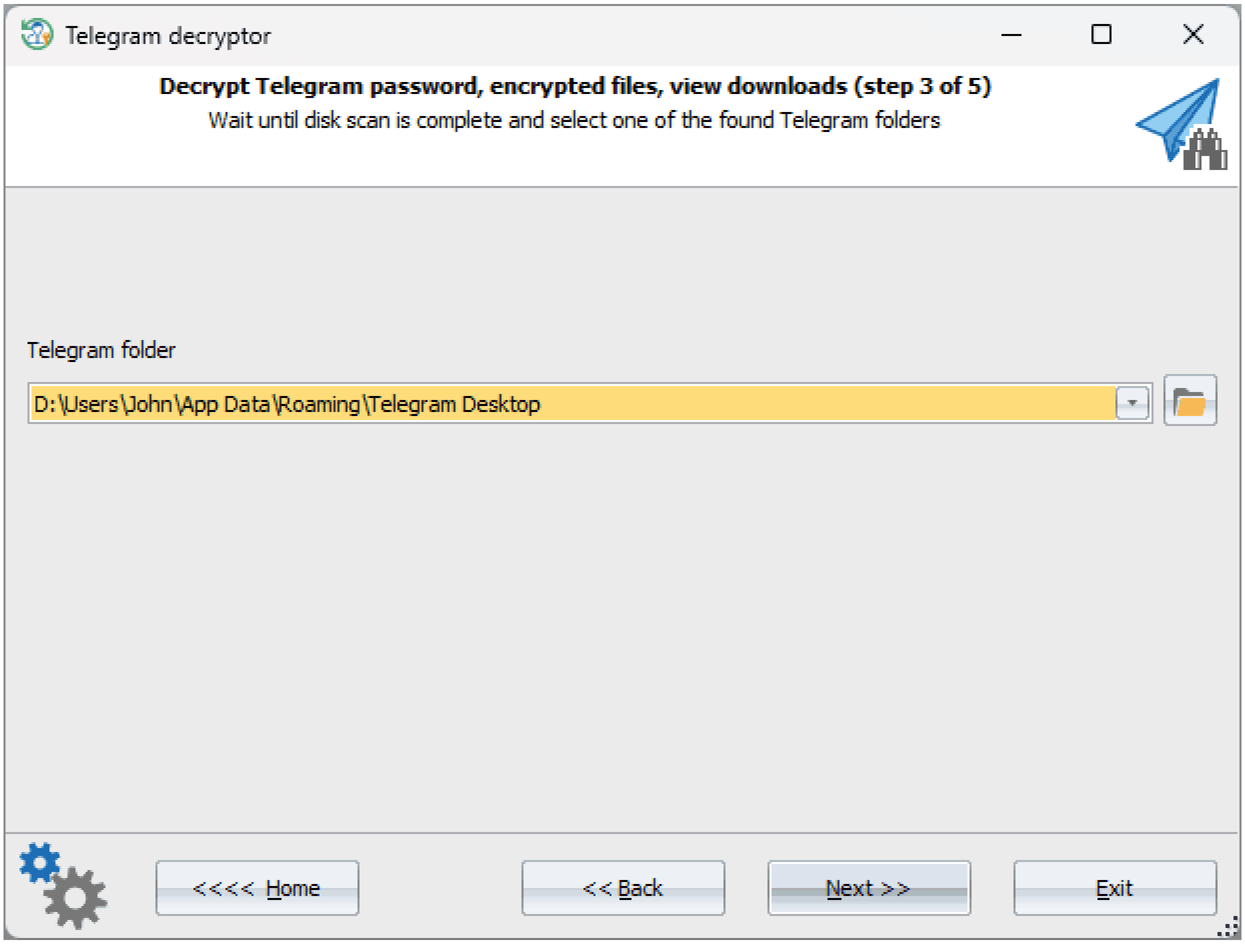
Disk D: 931.50 GB

Used space: 467.30 GB

Free space: 464.19 GB

Choose the disk on which you need to search for the Telegram Desktop directories or files.

Choosing Telegram folder



Telegram decryptor

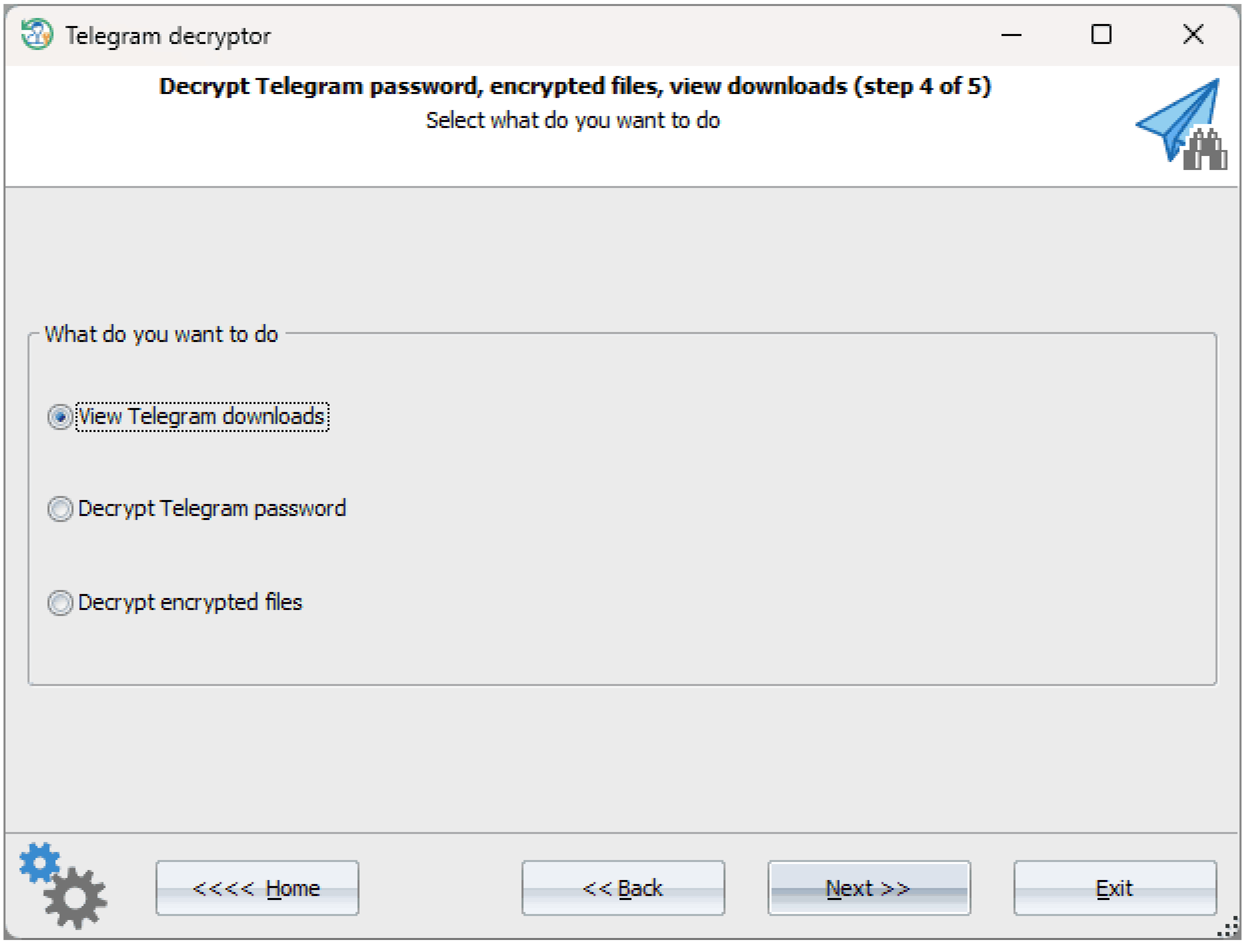
Decrypt Telegram password, encrypted files, view downloads (step 3 of 5)

Wait until disk scan is complete and select one of the found Telegram folders

Telegram folder: D:\Users\John\App Data\Roaming\Telegram Desktop

After the disk is selected, the program will start an immediate search of Telegram directories on the disk. Please note, the initial scan may take a few minutes if this disk has not been cached yet. Subsequent searches typically takes seconds. The program guarantees successful detection of all Telegram Desktop directories on the selected disk, wherever they may be located.
Found Telegram Desktop folders can be selected from the dropdown list. Choose the directory you need, if there are multiple ones, in order to proceed.

Choosing what do you need to recover



Decrypt Telegram password, encrypted files, view downloads (step 4 of 5)

Select what do you want to do

What do you want to do

● View Telegram downloads

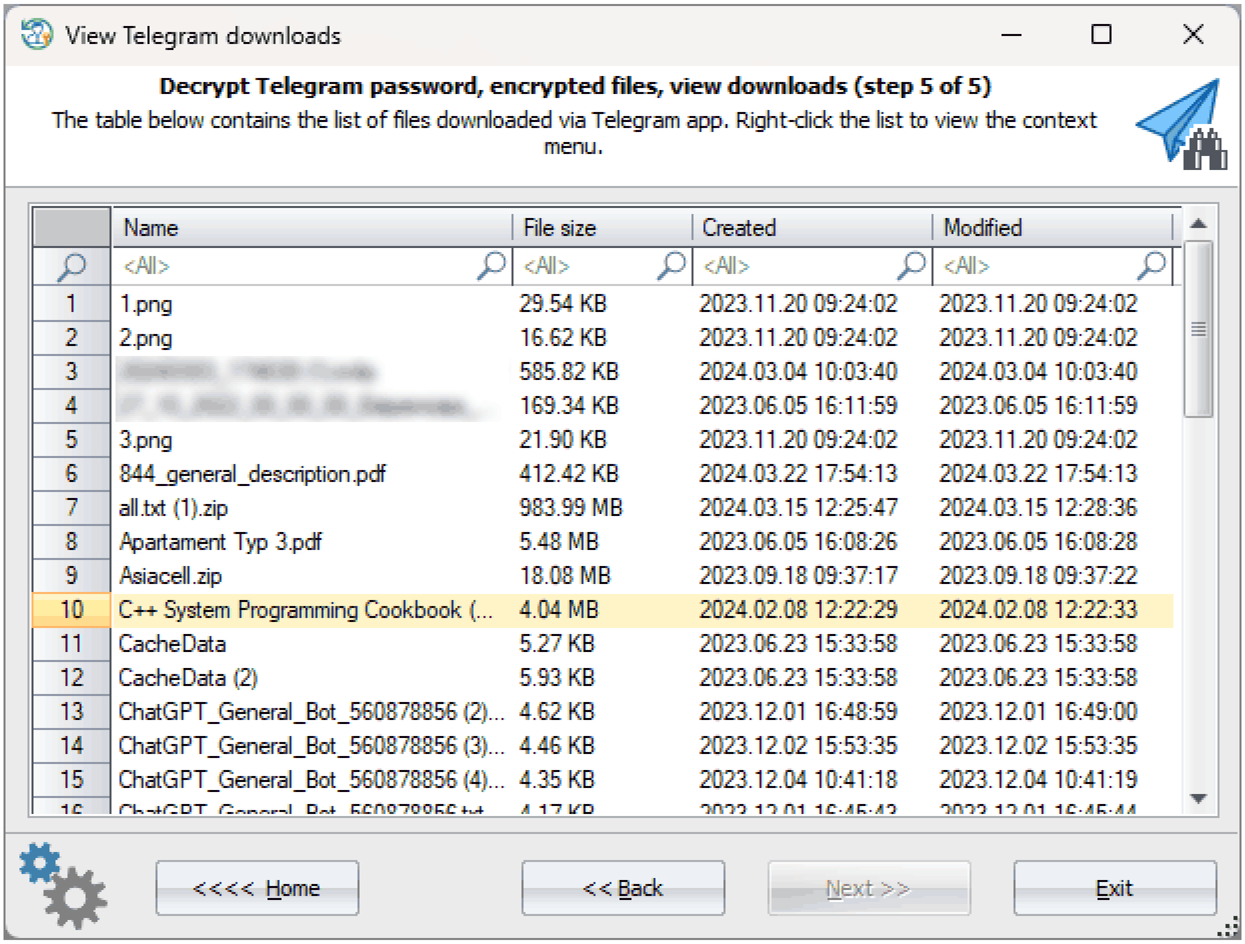
○ Decrypt Telegram password

○ Decrypt encrypted files

Choose from the following actions available for the found Telegram Desktop folder:

- Viewing and analyzing files downloaded via Telegram Desktop
- Recovering Telegram passcode
- Decrypting Telegram local files

3.7.13.1 Telegram Desktop downloads



Decrypt Telegram password, encrypted files, view downloads (step 5 of 5)

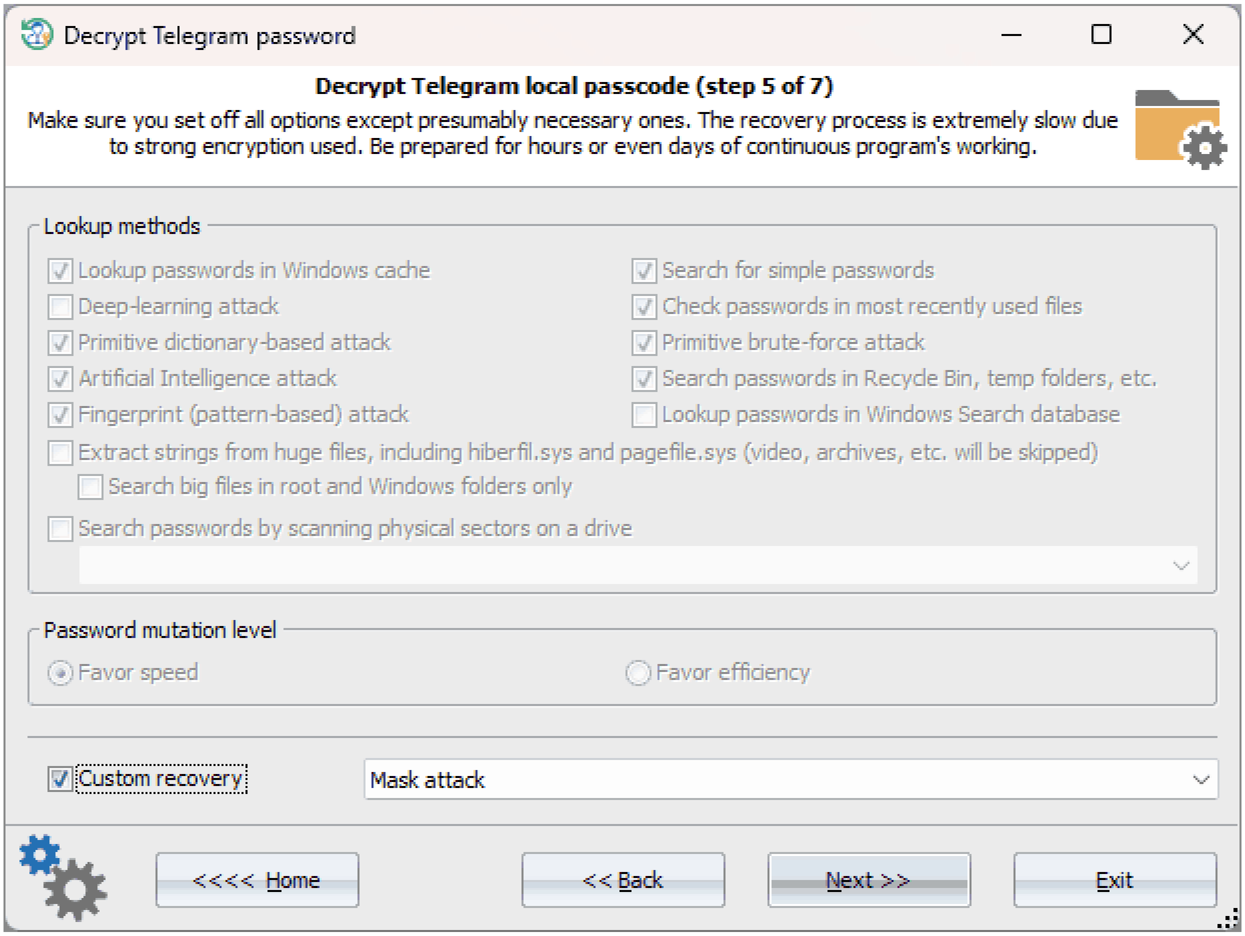
The table below contains the list of files downloaded via Telegram app. Right-click the list to view the context menu.

	Name	File size	Created	Modified
	<All>	<All>	<All>	<All>
1	1.png	29.54 KB	2023.11.20 09:24:02	2023.11.20 09:24:02
2	2.png	16.62 KB	2023.11.20 09:24:02	2023.11.20 09:24:02
3	[redacted]	585.82 KB	2024.03.04 10:03:40	2024.03.04 10:03:40
4	[redacted]	169.34 KB	2023.06.05 16:11:59	2023.06.05 16:11:59
5	3.png	21.90 KB	2023.11.20 09:24:02	2023.11.20 09:24:02
6	844_general_description.pdf	412.42 KB	2024.03.22 17:54:13	2024.03.22 17:54:13
7	all.txt (1).zip	983.99 MB	2024.03.15 12:25:47	2024.03.15 12:28:36
8	Apartament Typ 3.pdf	5.48 MB	2023.06.05 16:08:26	2023.06.05 16:08:28
9	Asiacell.zip	18.08 MB	2023.09.18 09:37:17	2023.09.18 09:37:22
10	C++ System Programming Cookbook (...	4.04 MB	2024.02.08 12:22:29	2024.02.08 12:22:33
11	CacheData	5.27 KB	2023.06.23 15:33:58	2023.06.23 15:33:58
12	CacheData (2)	5.93 KB	2023.06.23 15:33:58	2023.06.23 15:33:58
13	ChatGPT_General_Bot_560878856 (2)...	4.62 KB	2023.12.01 16:48:59	2023.12.01 16:49:00
14	ChatGPT_General_Bot_560878856 (3)...	4.46 KB	2023.12.02 15:53:35	2023.12.02 15:53:35
15	ChatGPT_General_Bot_560878856 (4)...	4.35 KB	2023.12.04 10:41:18	2023.12.04 10:41:19
16	ChatGPT_General_Bot_560878856.txt	4.17 KB	2023.12.01 16:45:43	2023.12.01 16:45:44

Files downloaded via **Telegram Desktop** are presented as a table. Here you can open the folder the files reside in, create a text or HTML reports on the list of found items, or back up one or more files.

3.7.13.2 Recover Telegram passcode

Choosing recovery attacks and methods



Decrypt Telegram password

Decrypt Telegram local passcode (step 5 of 7)

Make sure you set off all options except presumably necessary ones. The recovery process is extremely slow due to strong encryption used. Be prepared for hours or even days of continuous program's working.

Lookup methods

- ☑ Lookup passwords in Windows cache
- □ Deep-learning attack
- ☑ Primitive dictionary-based attack
- ☑ Artificial Intelligence attack
- ☑ Fingerprint (pattern-based) attack
- ☑ Search for simple passwords
- ☑ Check passwords in most recently used files
- ☑ Primitive brute-force attack
- ☑ Search passwords in Recycle Bin, temp folders, etc.
- □ Lookup passwords in Windows Search database
- □ Extract strings from huge files, including hiberfil.sys and pagefile.sys (video, archives, etc. will be skipped)
  - □ Search big files in root and Windows folders only
- □ Search passwords by scanning physical sectors on a drive

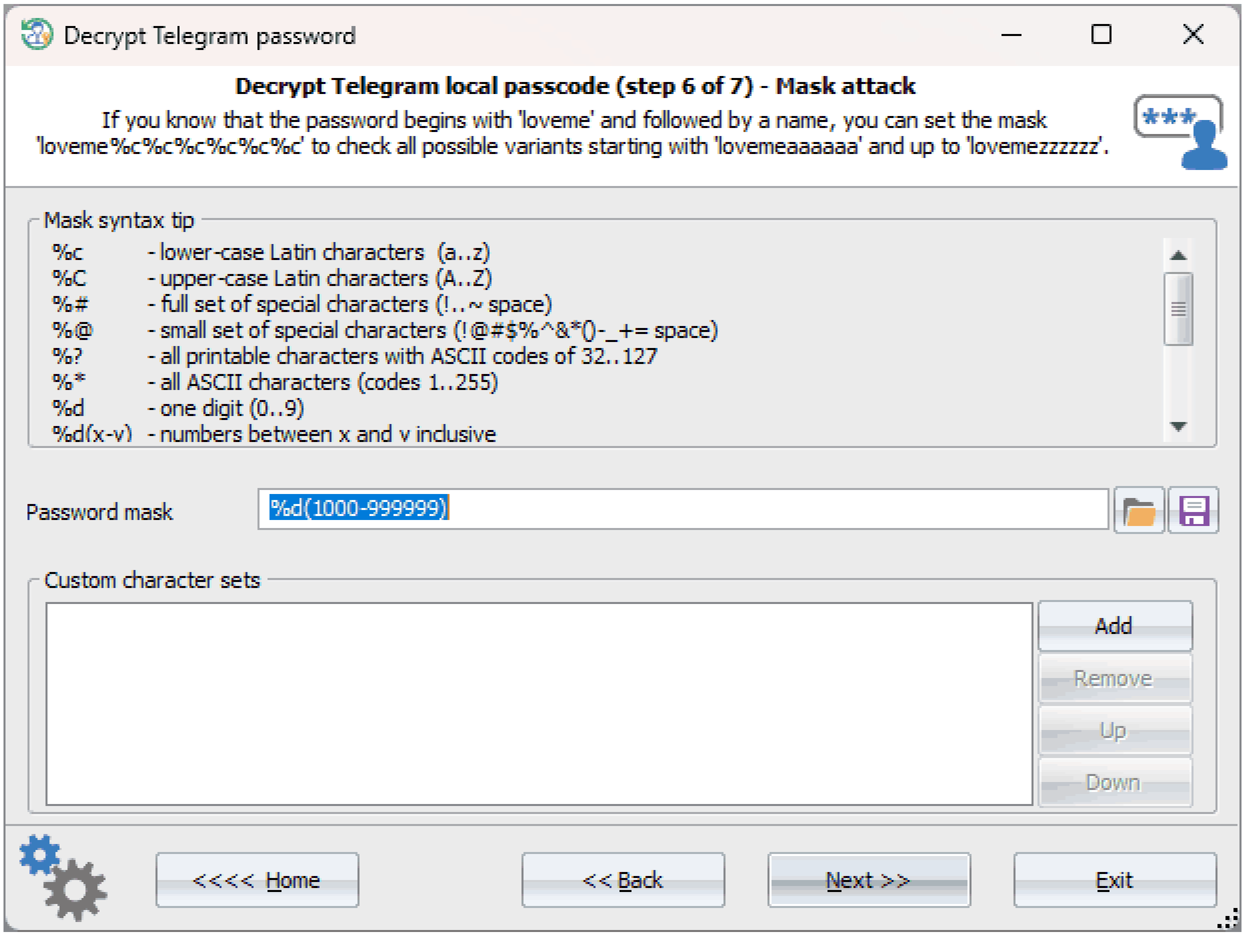
Password mutation level

● Favor speed ○ Favor efficiency

☑ Custom recovery: Mask attack

Telegram passcode has strong built-in protection. Brute-forcing such passwords runs at a rate of only a few passwords per second, which means that it is essential to choose an appropriate recovery method first. Otherwise, the process could take an indefinitely long time. If any information is available about the target passwords, it is recommended to utilize custom attacks. If not, you can switch to standard recovery, disabling the most time-consuming options, (such as primitive bruteforce and fingerprint attacks, searches in Recycle bin and temporary folders, etc.) while leaving at least two essential options: looking up for passwords in the Windows cache and using Artificial Intelligence attacks.

Setting up folders or user attacks



Decrypt Telegram password

Decrypt Telegram local passcode (step 6 of 7) - Mask attack

If you know that the password begins with 'loveme' and followed by a name, you can set the mask 'loveme%c%c%c%c%c%c' to check all possible variants starting with 'lovemeaaaaaa' and up to 'lovemezzzzzz'.

Mask syntax tip

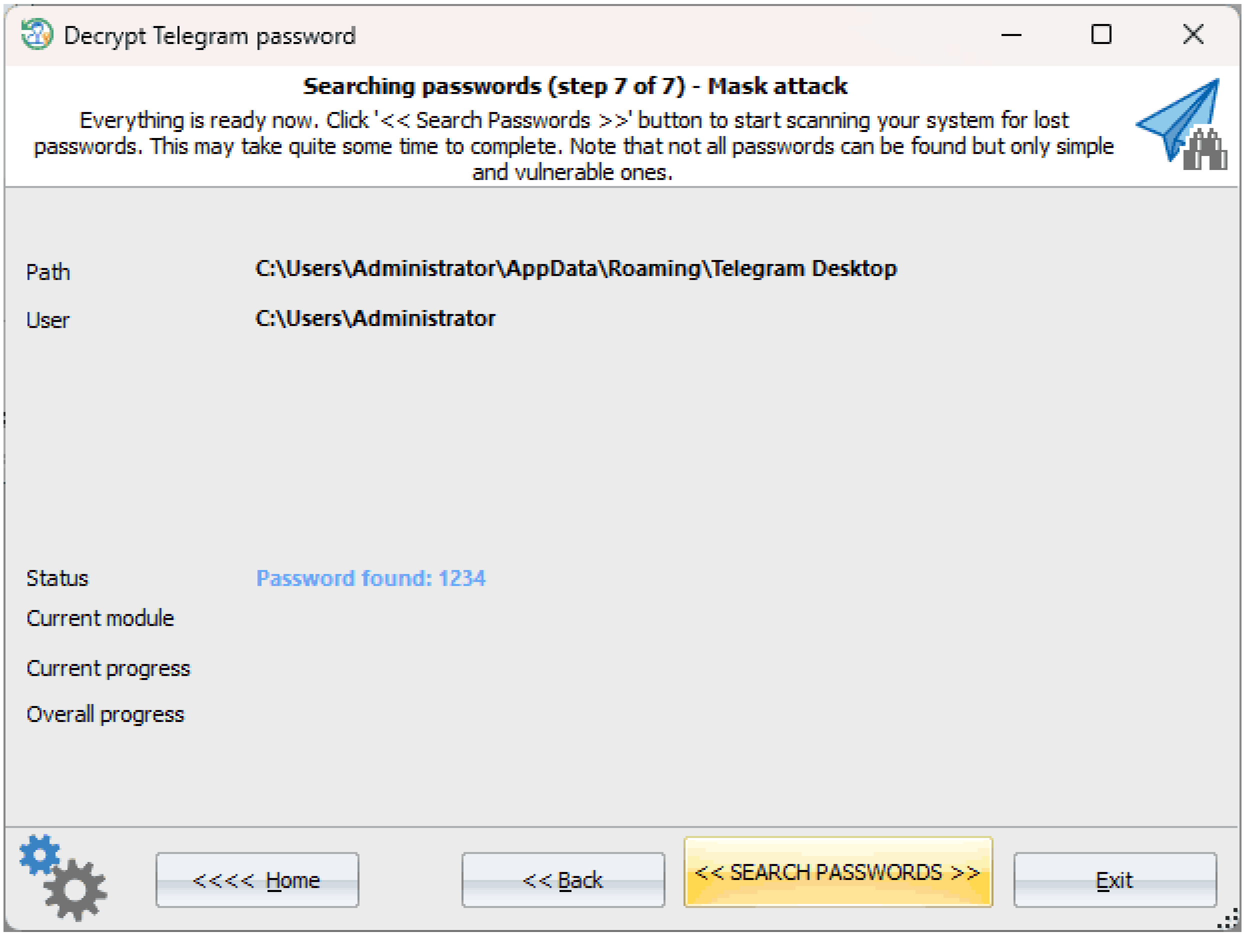
```
%c        - lower-case Latin characters  (a..z)
%C        - upper-case Latin characters (A..Z)
%#        - full set of special characters (!..~ space)
%@        - small set of special characters (!@#$%^&*()-_+= space)
%?        - all printable characters with ASCII codes of 32..127
%*        - all ASCII characters (codes 1..255)
%d        - one digit (0..9)
%d(x-y)   - numbers between x and y inclusive
```

Password mask: %d(1000-999999)

Custom character sets

If one of the custom attacks is chosen, it is necessary to configure its parameters first. For instance, in the picture above, the mask attack is specified, which will iteratively check digital passwords from 4 and up to 6 characters long. That is, from '1000' to '999999'.

Searching for Telegram passcode



Decrypt Telegram password

Searching passwords (step 7 of 7) - Mask attack

Everything is ready now. Click '<< Search Passwords >>' button to start scanning your system for lost passwords. This may take quite some time to complete. Note that not all passwords can be found but only simple and vulnerable ones.

Path **C:\Users\Administrator\AppData\Roaming\Telegram Desktop**

User **C:\Users\Administrator**

Status Password found: 1234

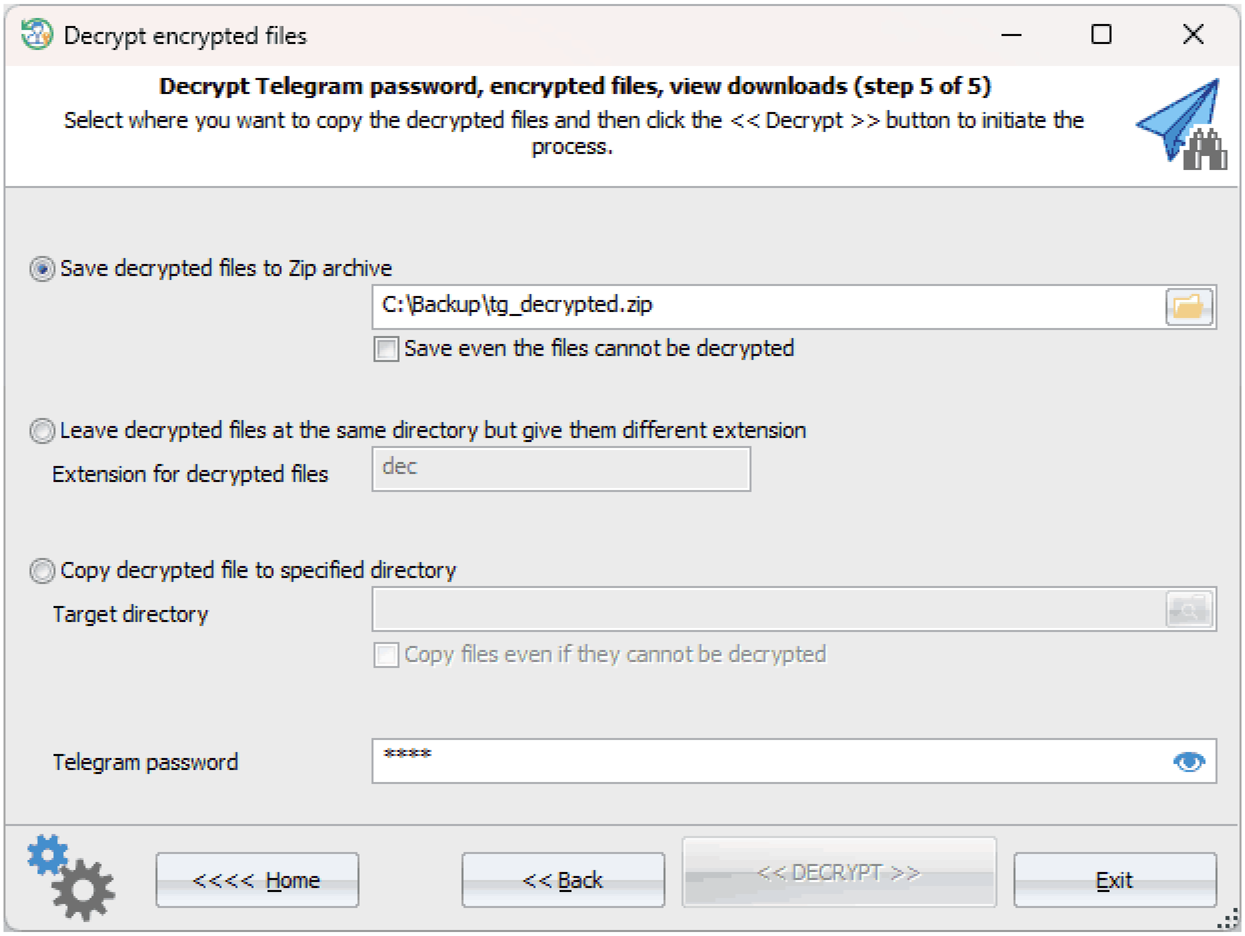
Current module

Current progress

Overall progress

Although the algorithms used in Telegram passcode encryption are highly optimized for speed, brute-forcing can still take a significant amount of time. Interestingly, the program is much faster than the popular Hashcat tool. However, unfortunately, the bootable environment is currently restricted to utilizing the CPU only, with no option available to leverage more powerful graphics cards.

3.7.13.3 Decrypt Telegram files



Decrypt encrypted files

Decrypt Telegram password, encrypted files, view downloads (step 5 of 5)

Select where you want to copy the decrypted files and then click the << Decrypt >> button to initiate the process.

● Save decrypted files to Zip archive

C:\Backup\tg_decrypted.zip

□ Save even the files cannot be decrypted

○ Leave decrypted files at the same directory but give them different extension

Extension for decrypted files: dec

○ Copy decrypted file to specified directory

Target directory:

□ Copy files even if they cannot be decrypted

Telegram password: ****

If the Telegram passcode is known or has not been set, decrypting the local files appears to be a relatively straightforward task. Otherwise, you'll need to decrypt the Telegram password first.

You can choose one of the three decryption methods that is more convenient for you:

- Creating a ZIP archive and copying all decrypted files into it.
- Keeping decrypted files within the original directory with a different file extension. For instance, if the extension is set to DEC, the decrypted files would appear as XXXXXX.DEC, YYYYYY.DEC, etc.
- Copying decrypted files to a specified directory.

Decrypted data can be used for further analysis. For example, the decrypted **maps** file contains the user's name and phone number.

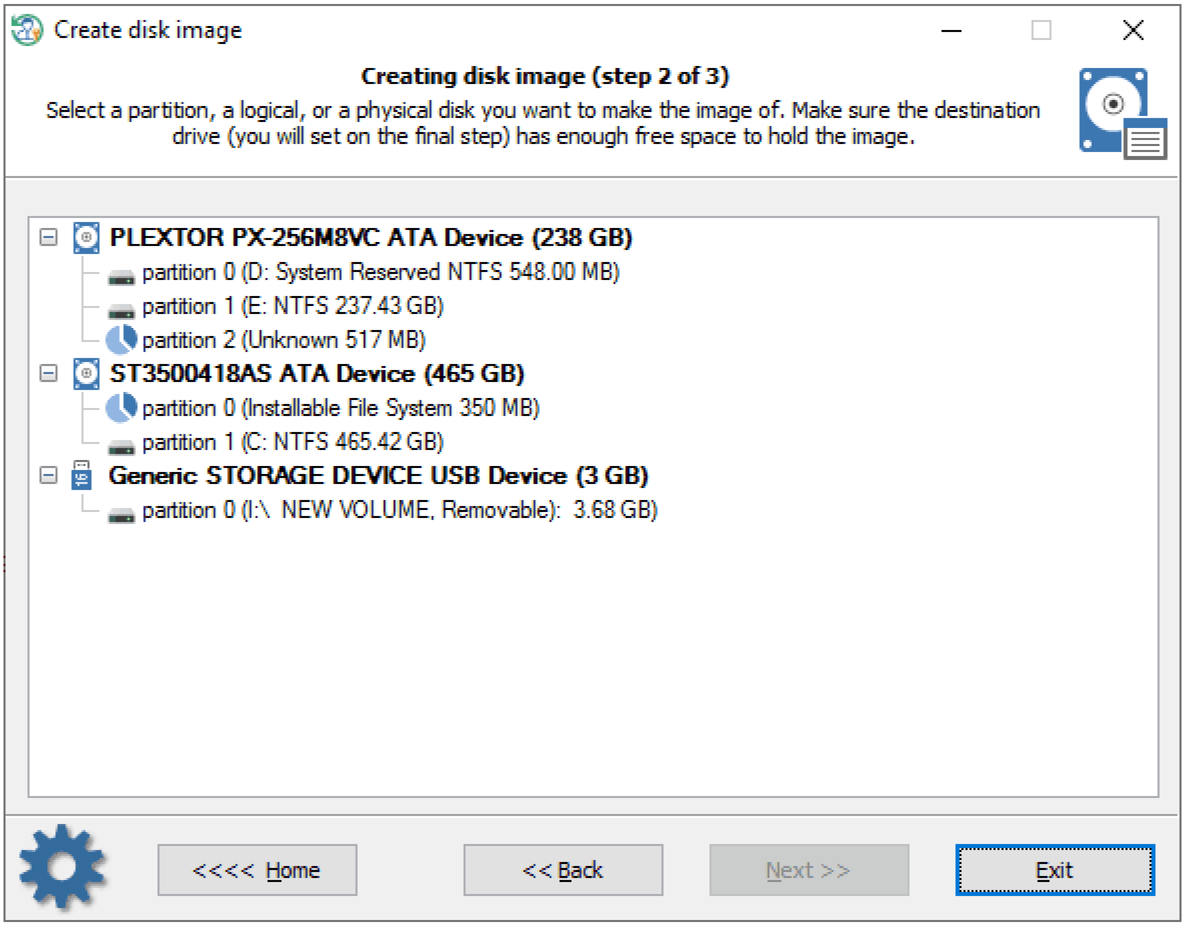
3.8 Files and drives

3.8.1 Create disk image

Sometimes when Windows becomes corrupt or your hard drive crashes, it is a nice idea to back up the entire content of your drive including disk encryption, OS state, settings, passwords, installed applications and drivers, all of your personal information, etc. One of the easiest ways to do it is to create an image of the entire hard drive.

In forensics, a disk image is a must-have and allows both saving some time during the initial investigation and ensuring nothing important will be missed during further in-depth analysis.

Creating a disk image in RWP is extremely simple.



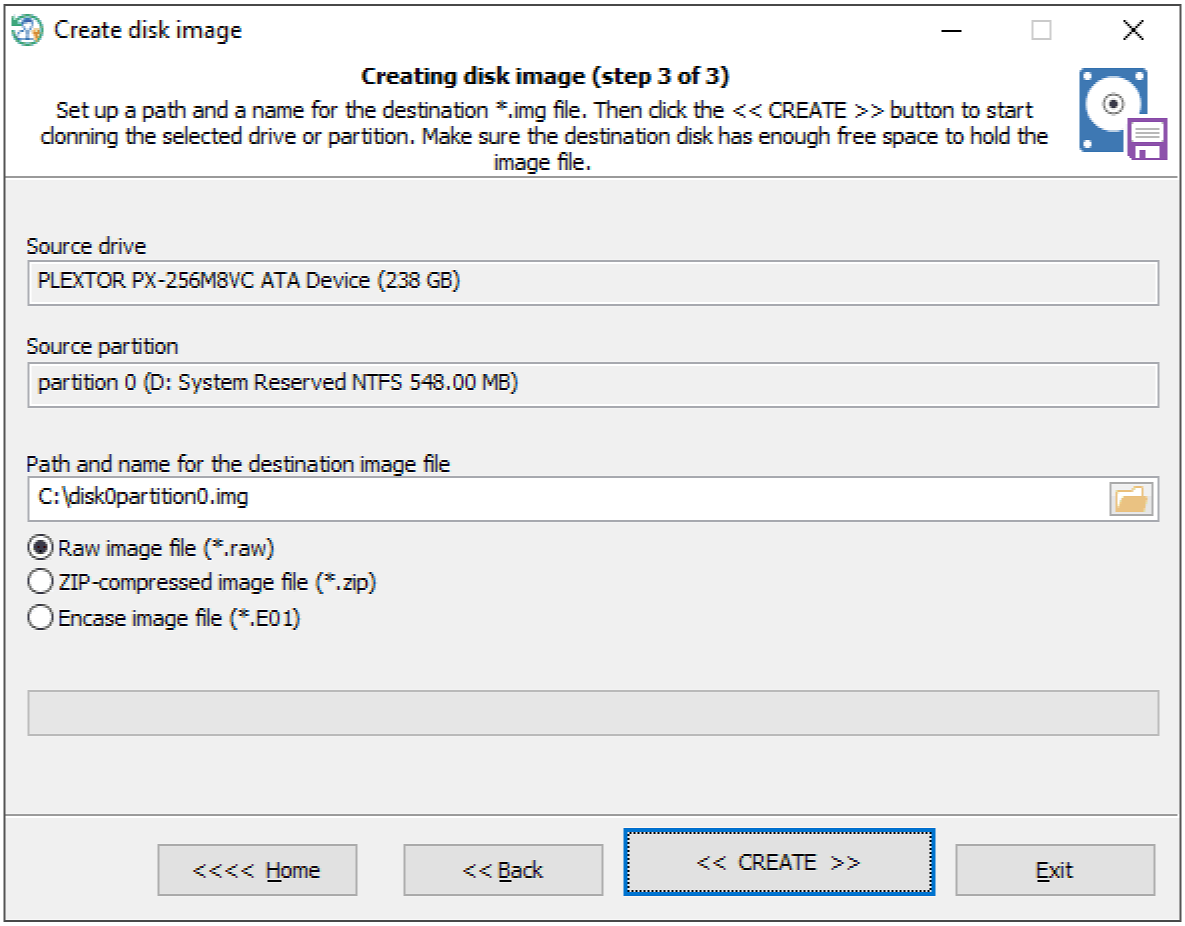
Create disk image

Creating disk image (step 2 of 3)

Select a partition, a logical, or a physical disk you want to make the image of. Make sure the destination drive (you will set on the final step) has enough free space to hold the image.

- **PLEXTOR PX-256M8VC ATA Device (238 GB)**
  - partition 0 (D: System Reserved NTFS 548.00 MB)
  - partition 1 (E: NTFS 237.43 GB)
  - partition 2 (Unknown 517 MB)
- **ST3500418AS ATA Device (465 GB)**
  - partition 0 (Installable File System 350 MB)
  - partition 1 (C: NTFS 465.42 GB)
- **Generic STORAGE DEVICE USB Device (3 GB)**
  - partition 0 (I:\ NEW VOLUME, Removable): 3.68 GB)

At the first dialog, the program displays a list of found partitions and disk drives the partitions belong to. Select a partition or the disk whose image you want to create.



Creating disk image (step 3 of 3)

Set up a path and a name for the destination *.img file. Then click the << CREATE >> button to start clonning the selected drive or partition. Make sure the destination disk has enough free space to hold the image file.

Source drive: PLEXTOR PX-256M8VC ATA Device (238 GB)

Source partition: partition 0 (D: System Reserved NTFS 548.00 MB)

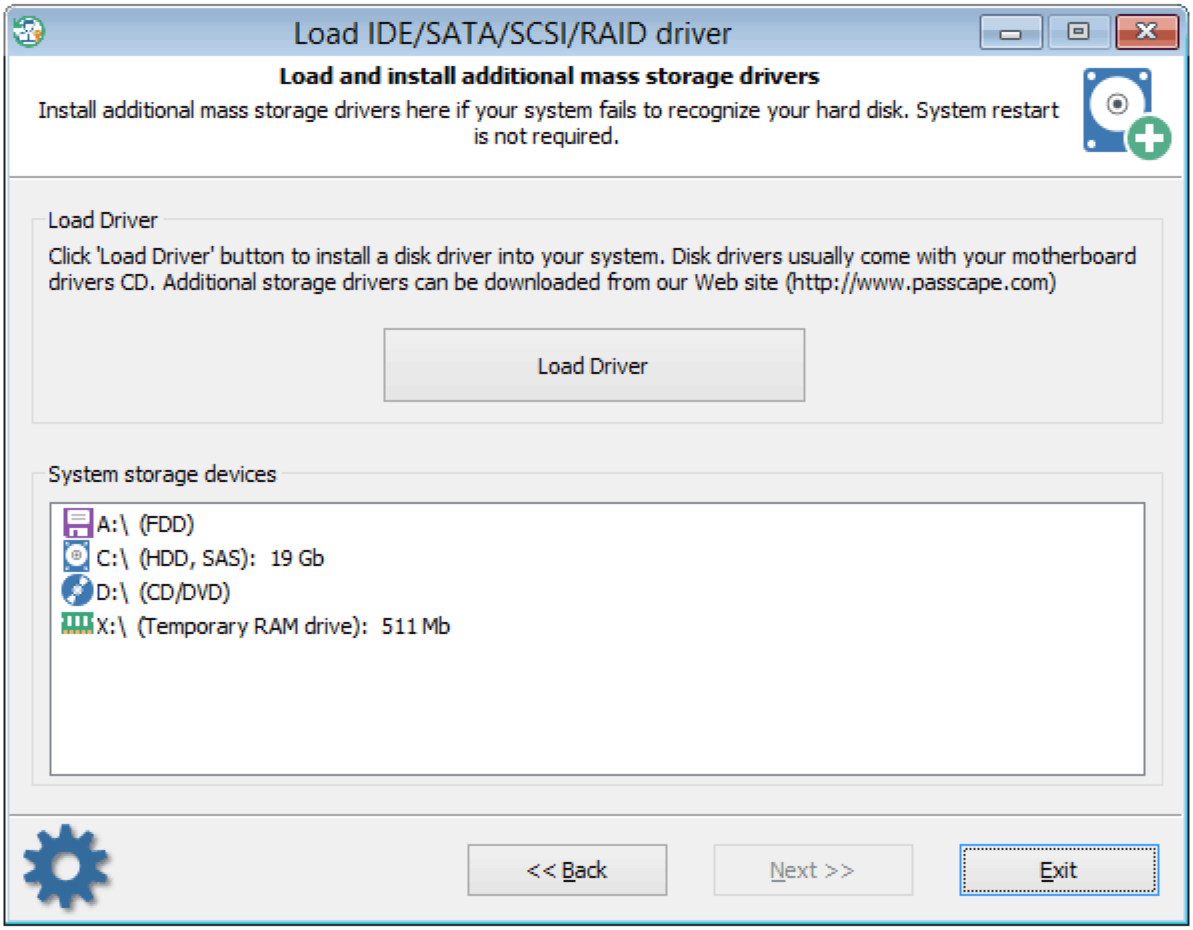
Path and name for the destination image file: C:\disk0partition0.img

● Raw image file (*.raw)
○ ZIP-compressed image file (*.zip)
○ Encase image file (*.E01)

At the final dialog, set the name of the image and the destination path the image to save to. Note that the destination path should be located on another physical drive. Make sure you have enough free space to hold the entire image file. Click the '<< Create >>' button to start the disk image creation. Be patient, it may take some time and depends on the speed of your source and target drives.

Optionally, image compression is available. Once set, the output image file will be compressed to *.ZIP or to *.E01 file.

3.8.2 Loading hard disk drivers



Load and install additional mass storage drivers

Install additional mass storage drivers here if your system fails to recognize your hard disk. System restart is not required.

Load Driver

Click 'Load Driver' button to install a disk driver into your system. Disk drivers usually come with your motherboard drivers CD. Additional storage drivers can be downloaded from our Web site (http://www.passcape.com)

System storage devices

A:\ (FDD)
C:\ (HDD, SAS): 19 Gb
D:\ (CD/DVD)
X:\ (Temporary RAM drive): 511 Mb

If when the application started it was unable to detect one or several hard disk drives, you will most likely need to install a driver for that device. In the main window, on the task list, select '*Load IDE/SATA/SCSI/RAID/NVME driver*' and go to the driver installation dialog. The software comes with several popular hard drive controller drivers: ATI, Highpoint, Intel, Jmicron, Marvell, Nvidia, Silicion Image, Sis, Uli, Via, Vmware.

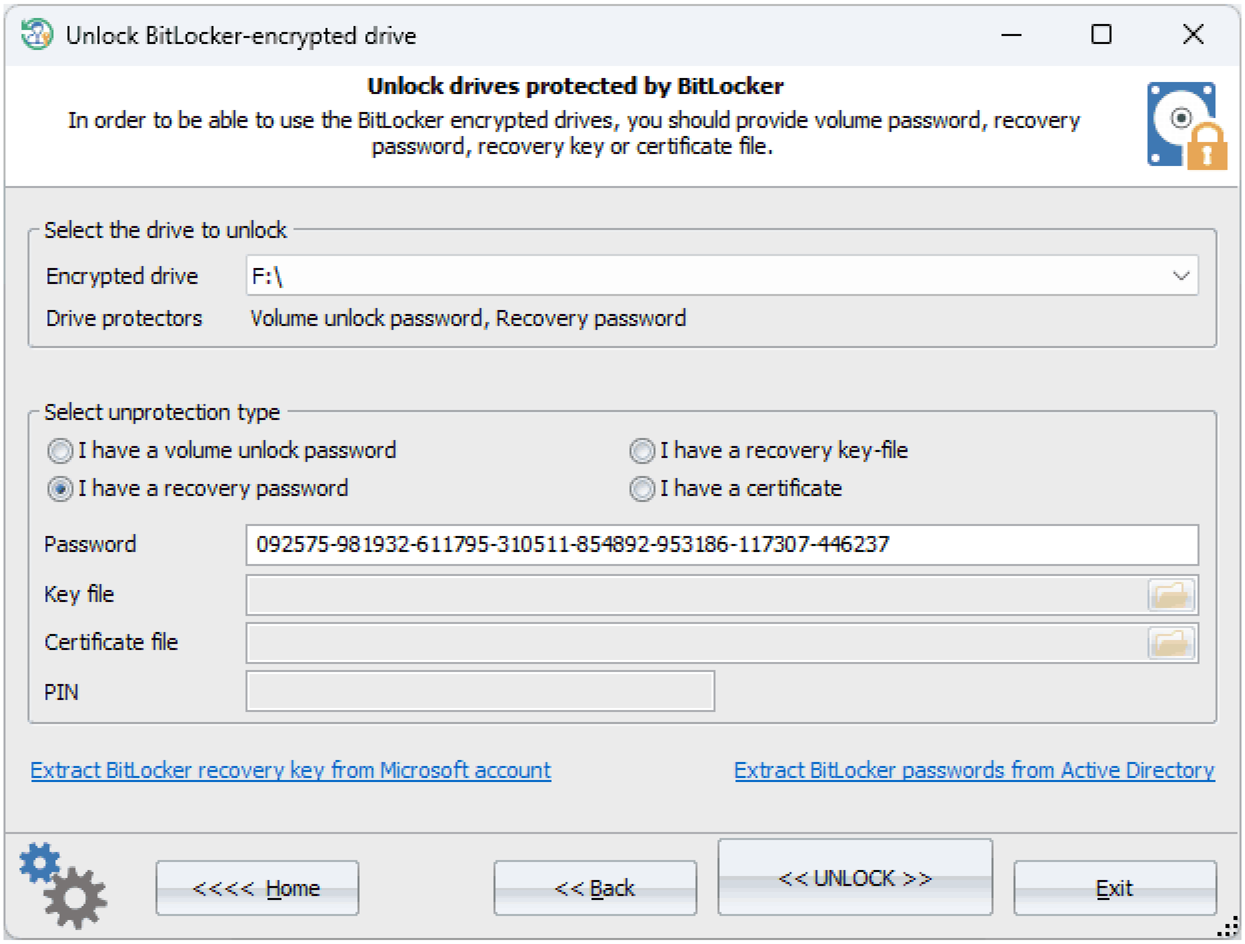
They all are stored in the folder **X:\Apps\Drivers**. For example, if your HDD controller is built upon the Nvidia chipset, load the corresponding *.INF file from the folder X:\Apps\Drivers\Nvidia.

Normally when you buy a new PC you get loaded with a CD with the motherboard and hard disk drivers. You can, and even are highly encouraged to use that disk for installing drivers for the missing devices. Be careful; the drivers should be compatible with Windows 11 x64 operating system! Please refer to the manual on your motherboard for more information on installing the drivers.

In Reset Windows Password drivers are installed 'on the fly'; therefore, rebooting the system is not required. Upon the completion, the found devices should appear on the list of data storage devices. Once the required driver is installed and the hard disk drive is found, you can go on with the next steps.

3.8.3 Unlock Bitlocker encrypted drives

Bitlocker is a full drive encryption. It was first introduced in Windows Vista and is aimed to protect your data even if someone has physical access to your PC or laptop.



Unlock BitLocker-encrypted drive

Unlock drives protected by BitLocker

In order to be able to use the BitLocker encrypted drives, you should provide volume password, recovery password, recovery key or certificate file.

Select the drive to unlock

Encrypted drive: F:\

Drive protectors: Volume unlock password, Recovery password

Select unprotection type

○ I have a volume unlock password
○ I have a recovery key-file
● I have a recovery password
○ I have a certificate

Password: 092575-981932-611795-310511-854892-953186-117307-446237

Key file:

Certificate file:

PIN:

Extract BitLocker recovery key from Microsoft account
Extract BitLocker passwords from Active Directory
<<<< Home
<< Back
<< UNLOCK >>
Exit

BitLocker encrypts all files on a drive, including those needed for startup. So its content is invisible to the system. In order to unlock the drive and get access to its content, you should use one of the following unprotection methods:

- Unlock the drive with volume unlock password
- Unlock using recovery (numerical) password
- Unlock using external recovery key
- Unlock using Bitlocker certificate

Just select your Bitlocker-encrypted drive along with required unlock type and click <<*UNLOCK*>> button to decrypt it. The operation takes several seconds.

To get a BitLocker recovery password stored in a domain, click the *'Extract BitLocker passwords from Active Directory'* link and follow the program's instructions.

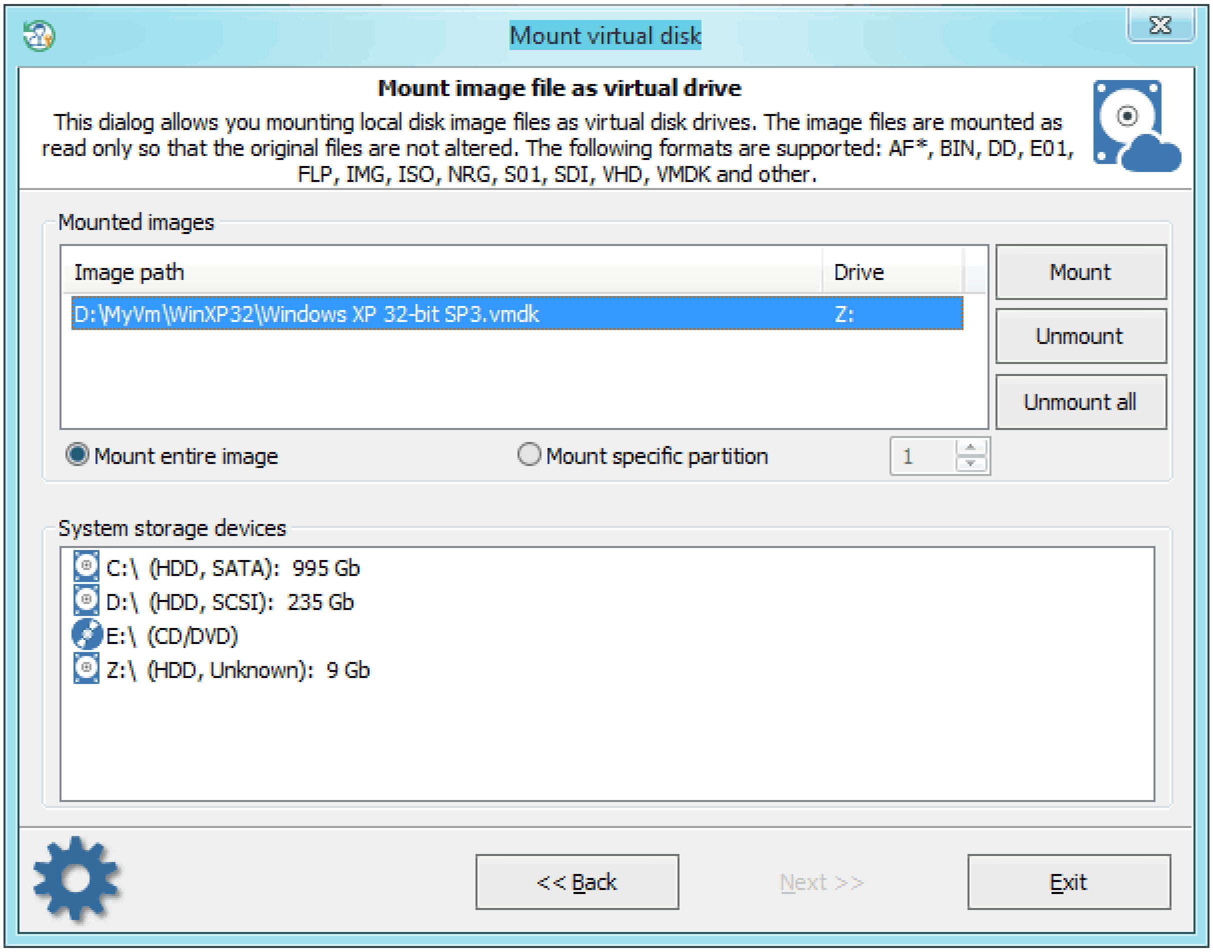
Often, the BitLocker recovery key is stored in your Microsoft account. If this is your case, use the following simple instruction to get the recovery key:

- Make sure you have a wired connection to the internet.
- Make sure you remember your Microsoft account login (e-mail) and password. If not, recover it first.
- Click the *'Extract BitLocker recovery key from Microsoft account'* link in the bottom left corner. After installing network drivers and connecting to the Internet, the program will open your Microsoft account page where you should type in your account email and password.
- Follow the on-screen instructions to log in to your Microsoft account. You might be asked to pass a second authentication factor. For example, to provide a security key sent to your email address. Be prepared for this.
- Once logged in, identify your device and locate the 48-digit BitLocker recovery key. Copy the key to the clipboard.
- Now switch back to the RWP dialog, select the *'I have a recover password'* and paste the recovery key there.
- Click the <<*UNLOCK*>> button to unlock the drive.

You can use this instruction to get access to your BitLocker encrypted drive even if Windows prompts for BitLocker recovery key and fails to boot. For example, after hardware changes (such as adding or removing video or network card), BIOS update or changing some BIOS options such as TPM or Secure Boot.

Exact location of your recovery key depends on the method that you used to back it up when enabling the BitLocker encryption.

3.8.4 Mounting virtual drives



Mount virtual disk

Mount image file as virtual drive

This dialog allows you mounting local disk image files as virtual disk drives. The image files are mounted as read only so that the original files are not altered. The following formats are supported: AF*, BIN, DD, E01, FLP, IMG, ISO, NRG, S01, SDI, VHD, VMDK and other.

Mounted images

Image path	Drive
D:\MyVm\WinXP32\Windows XP 32-bit SP3.vmdk	Z:

● Mount entire image ○ Mount specific partition 1

System storage devices

C:\ (HDD, SATA): 995 Gb
D:\ (HDD, SCSI): 235 Gb
E:\ (CD/DVD)
Z:\ (HDD, Unknown): 9 Gb

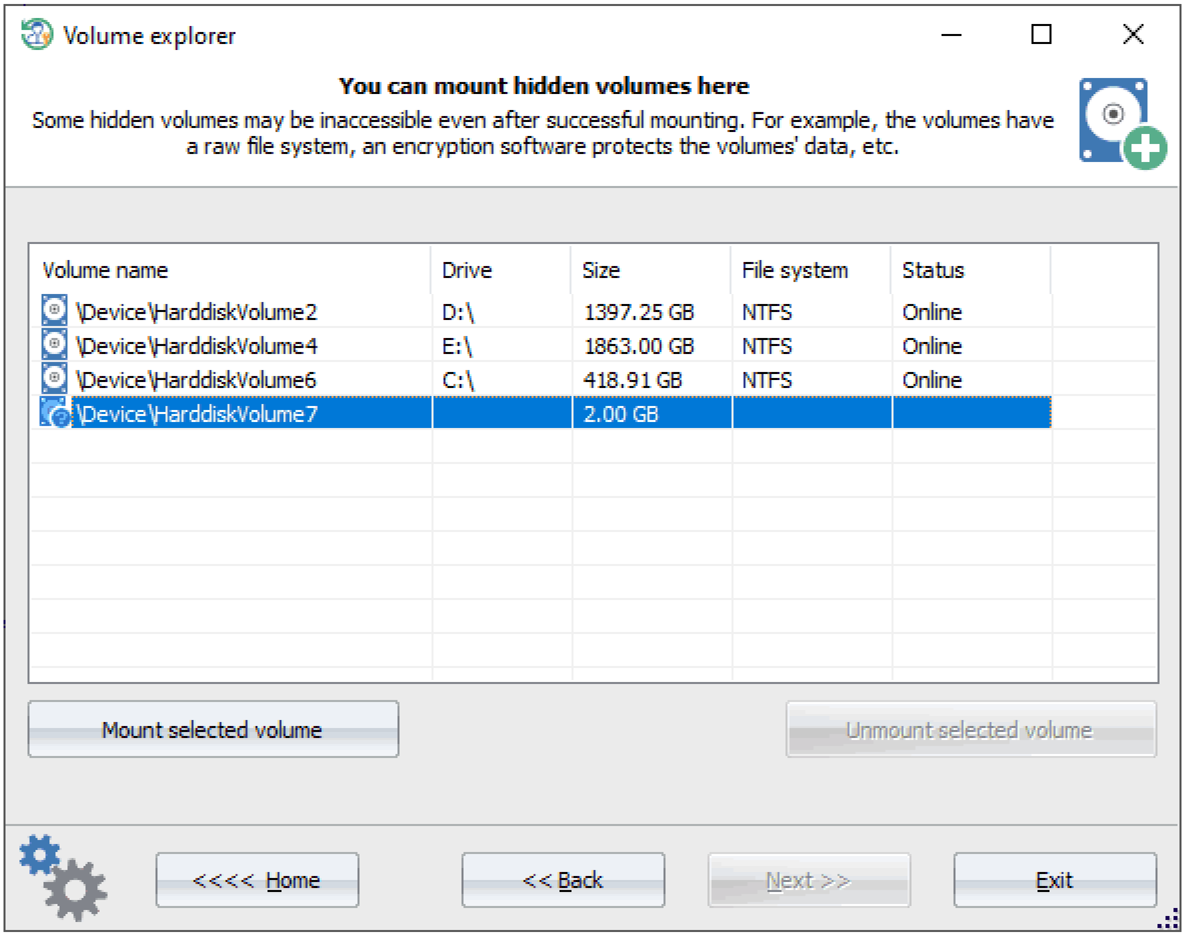
This dialog allows you to mount a disk image to the system as virtual drive. You can then refer to the new drive by it's volume letter. Images are mounted as read-only so that the original file is not altered. The following formats are supported:
AF*, BIN, DD, E01, FLP, IMG, ISO, NRG, S01, SDI, VHD, VMDK and some others.

If you need to attach a BitLocker-encrypted image, first mount the image file and then unlock it using a known recovery password or key.

Be patient, mounting some image types may take up to several minutes to complete.

3.8.5 Volume explorer

Most modern Windows systems require at least one hidden partition for successful functioning. These invisible to users partitions are used by OS during startup, recovery or system update. Furthermore, some advanced users can create their own hidden partitions to prevent others from viewing and accessing private files and personal information.

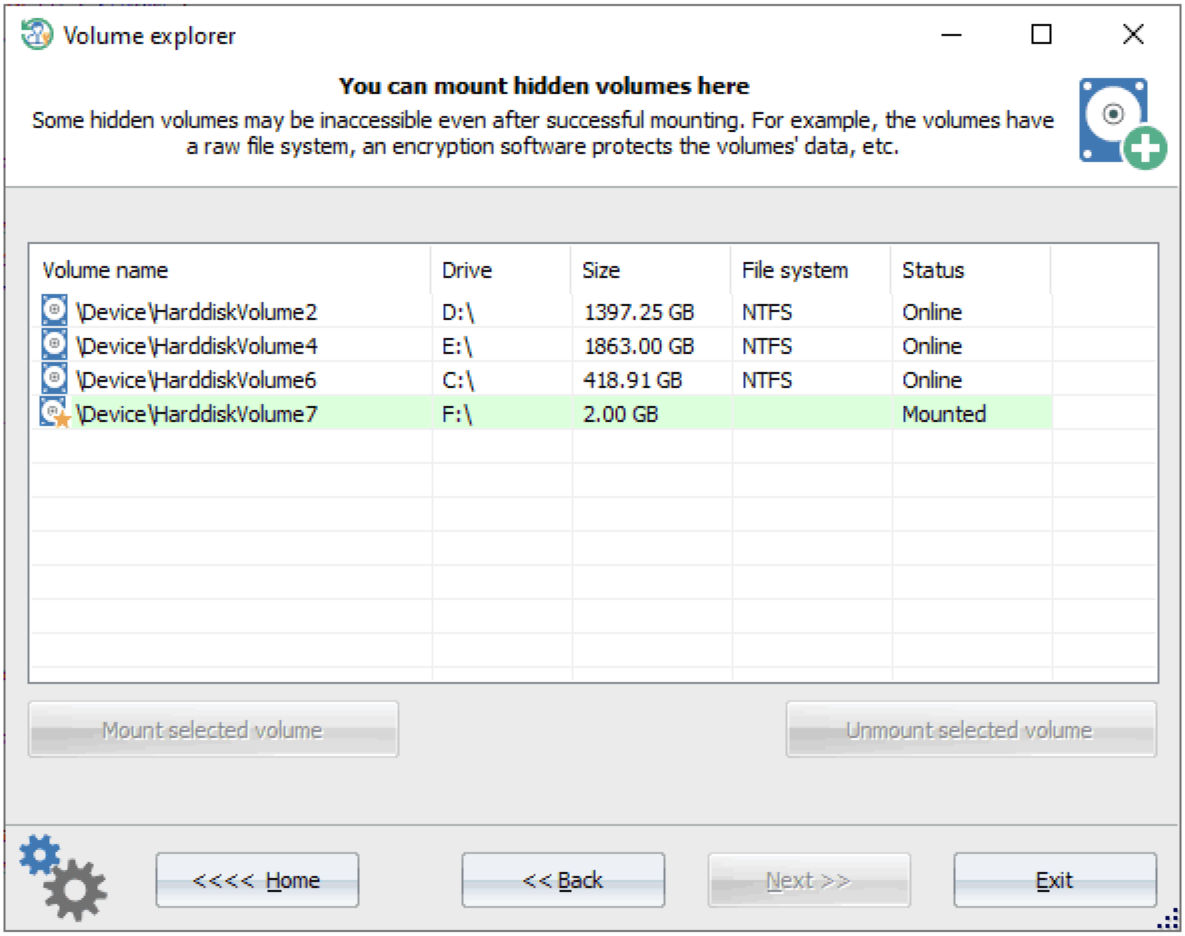


You can mount hidden volumes here

Some hidden volumes may be inaccessible even after successful mounting. For example, the volumes have a raw file system, an encryption software protects the volumes' data, etc.

Volume name	Drive	Size	File system	Status
\Device\HarddiskVolume2	D:\	1397.25 GB	NTFS	Online
\Device\HarddiskVolume4	E:\	1863.00 GB	NTFS	Online
\Device\HarddiskVolume6	C:\	418.91 GB	NTFS	Online
\Device\HarddiskVolume7		2.00 GB		

The **Volume Explorer** tool can mount hidden partitions temporarily and use them as regular logical drives.
To attach a hidden partition, select it from the list of found volumes and click the *'Mount selected volume'* button.



Volume explorer

You can mount hidden volumes here

Some hidden volumes may be inaccessible even after successful mounting. For example, the volumes have a raw file system, an encryption software protects the volumes' data, etc.

Volume name	Drive	Size	File system	Status
\Device\HarddiskVolume2	D:\	1397.25 GB	NTFS	Online
\Device\HarddiskVolume4	E:\	1863.00 GB	NTFS	Online
\Device\HarddiskVolume6	C:\	418.91 GB	NTFS	Online
\Device\HarddiskVolume7	F:\	2.00 GB		Mounted

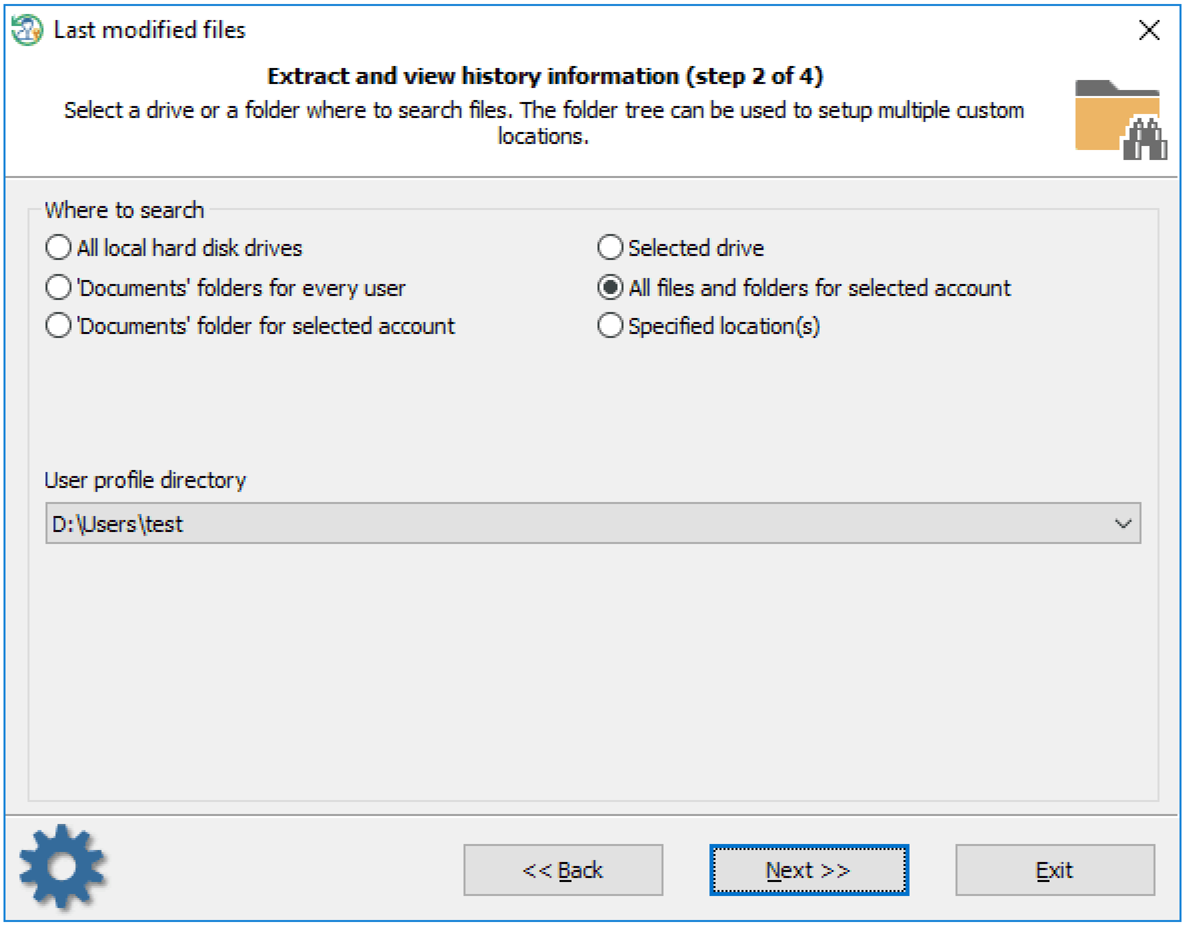
Don't forget to detach it if you no longer need it.

Do know that some partitions may be unusable even after a successful mounting. For example, the partition has a raw file system, some encryption software protects it and so on.

3.8.6 View last modified files

Sometimes it is required to figure out what files or folders were created or modified in a certain time. This is what this tool was created for. We tried to make it as simple as possible. All you need is to set the search location and to specify the time range for the sought files/folders.

Setting search location



Last modified files

Extract and view history information (step 2 of 4)

Select a drive or a folder where to search files. The folder tree can be used to setup multiple custom locations.

Where to search

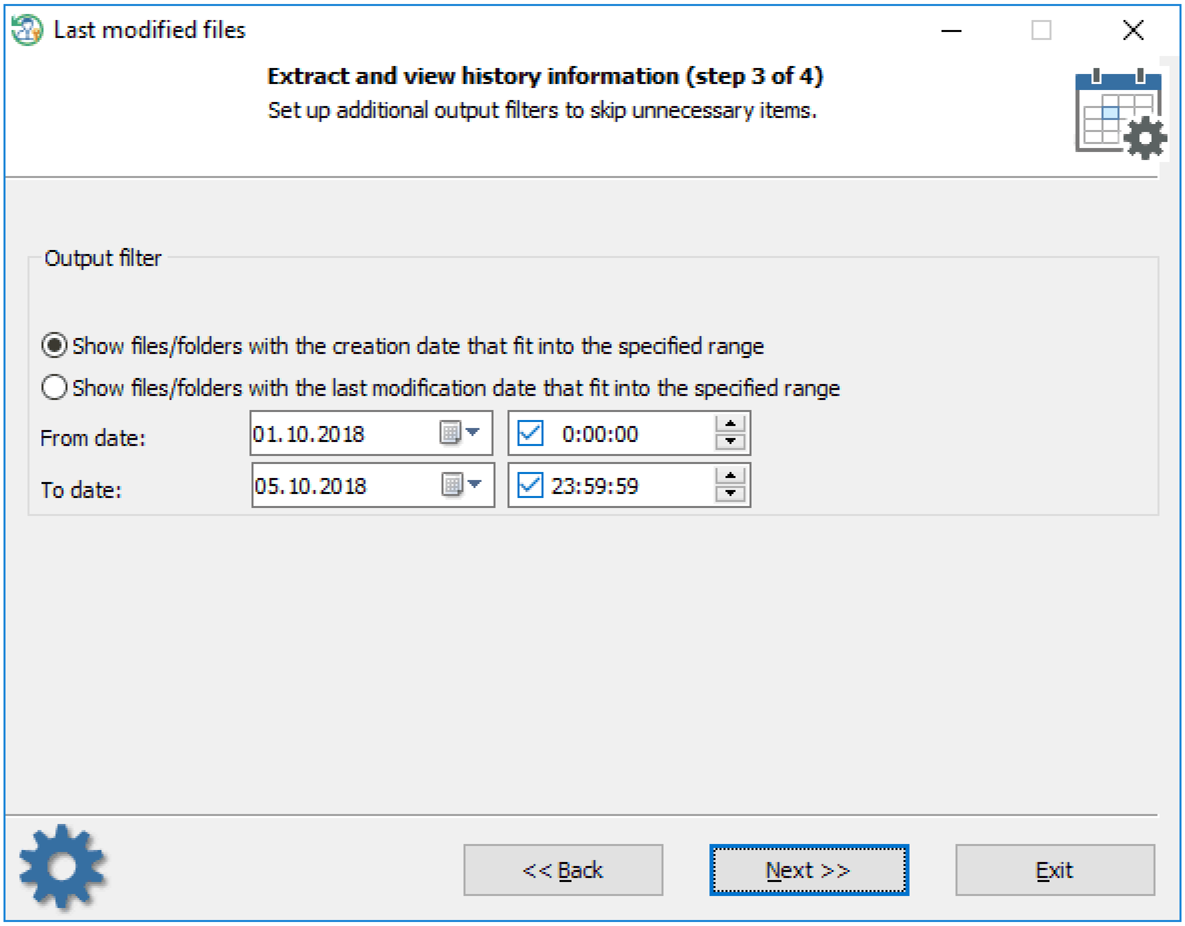
○ All local hard disk drives
○ 'Documents' folders for every user
○ 'Documents' folder for selected account
○ Selected drive
● All files and folders for selected account
○ Specified location(s)

User profile directory

D:\Users\test

To point the program the starting point for the files to search, select one of some predefined values like documents folder of a certain user, the whole user's profile, etc. You can also specify your own location by setting a custom path or a hard drive.

Setting the time range



Extract and view history information (step 3 of 4)

Set up additional output filters to skip unnecessary items.

Output filter

● Show files/folders with the creation date that fit into the specified range

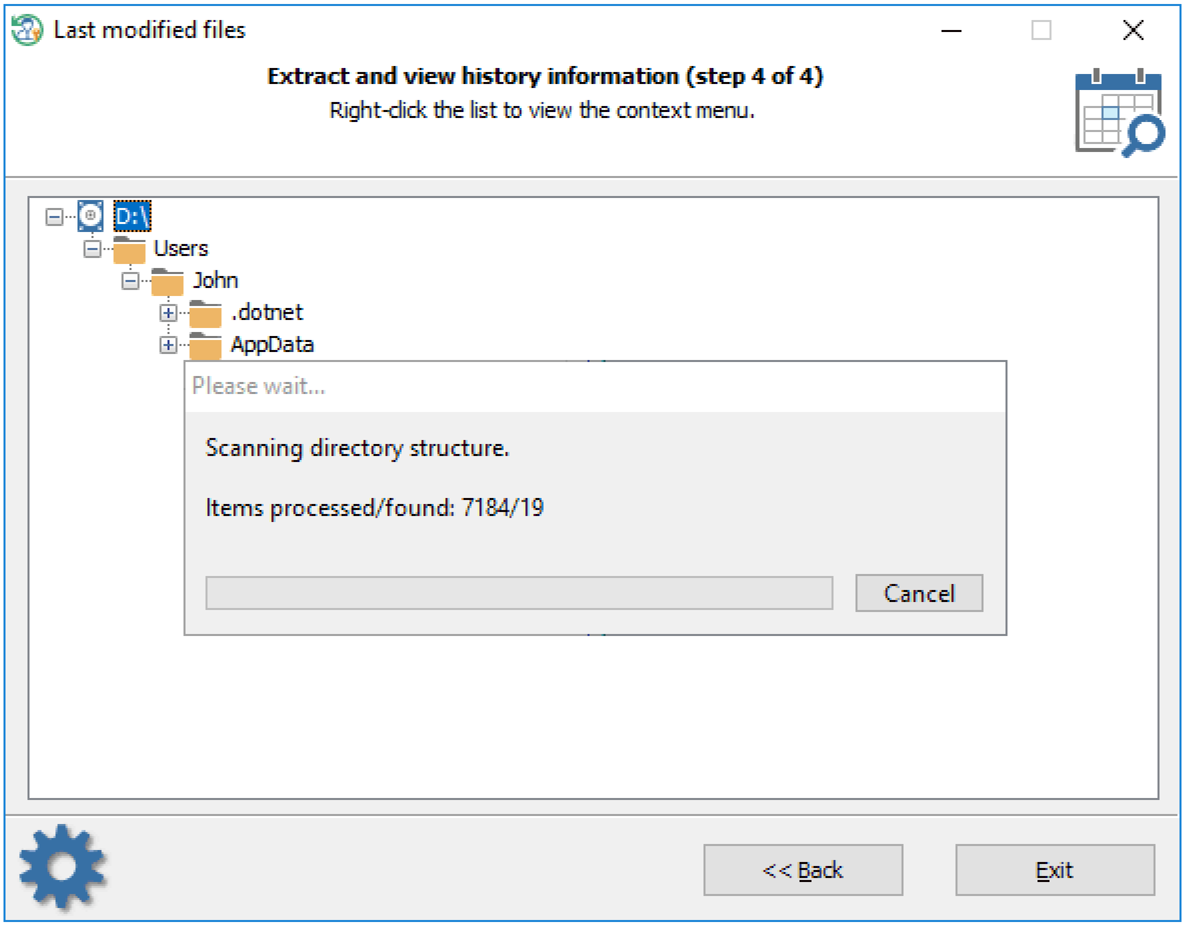
○ Show files/folders with the last modification date that fit into the specified range

From date: 01.10.2018 ☑ 0:00:00

To date: 05.10.2018 ☑ 23:59:59

Specify here if you need to search for files/folders with a certain creation date or a modification date. You can set up the time up to seconds or turn the seconds off completely.

[Displaying last modified files](#)


Last modified files
Extract and view history information (step 4 of 4)
Right-click the list to view the context menu.
D:\
Users
John
.dotnet
AppData
Please wait...
Cancel
<< Back
Exit

Scanning directory structure.

Items processed/found: 7184/19

Be patient, searching may take quite a lot of time.

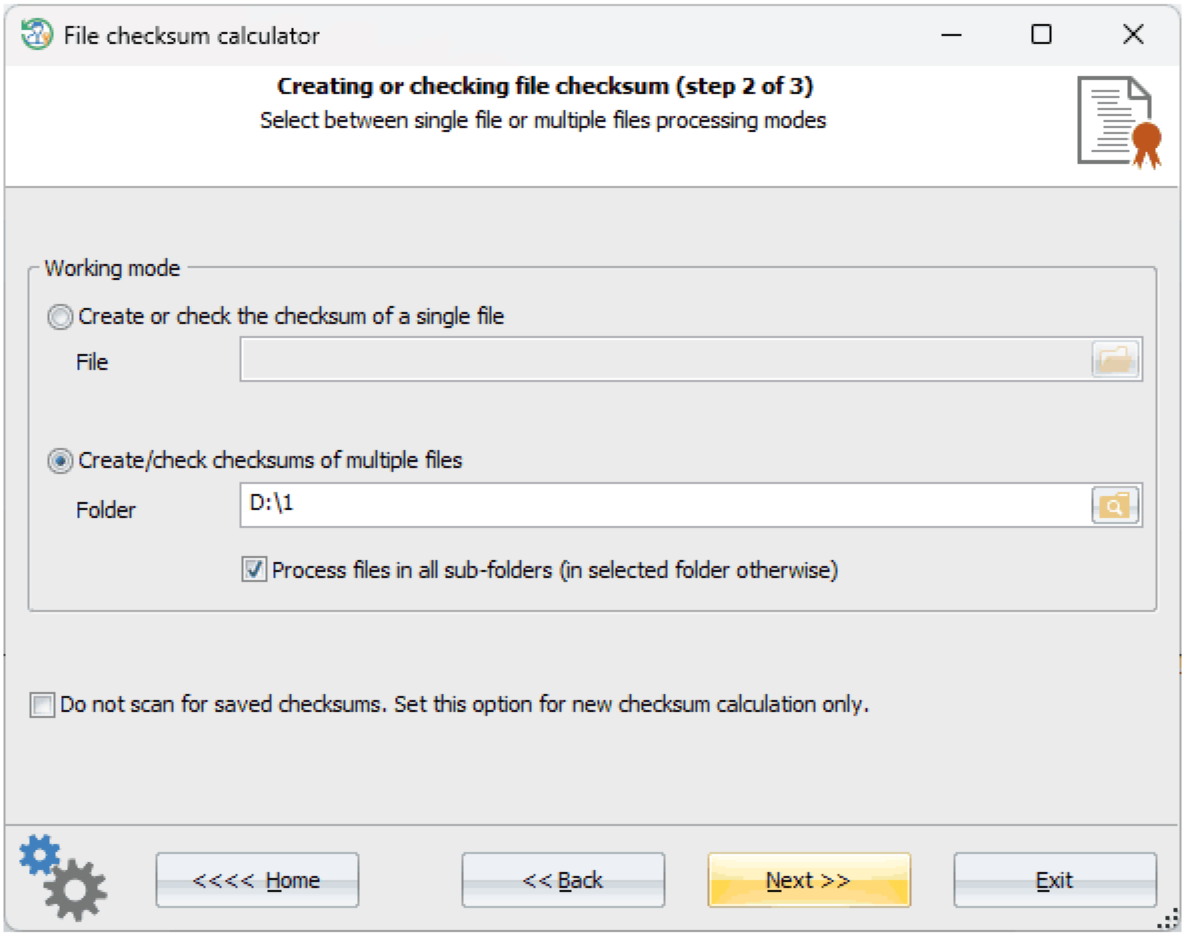
3.8.7 View last modified directories

This tool behaves exactly like the previous one except that it searches for the folders instead of files. Please, refer to the file search tool for more information.

3.8.8 File checksum calculator

This is a tool for creating file checksums, as well as for hashing files to ensure data integrity. The tool uses different hashing algorithms, such as CRC-32, MD5, SHA1, SHA-256, and SHA-512. It can work in a batch mode computing and verifying checksums of multiple files of any requested directory.

Setting source file or directory



File checksum calculator

Creating or checking file checksum (step 2 of 3)

Select between single file or multiple files processing modes

Working mode

○ Create or check the checksum of a single file

File

● Create/check checksums of multiple files

Folder: D:\1

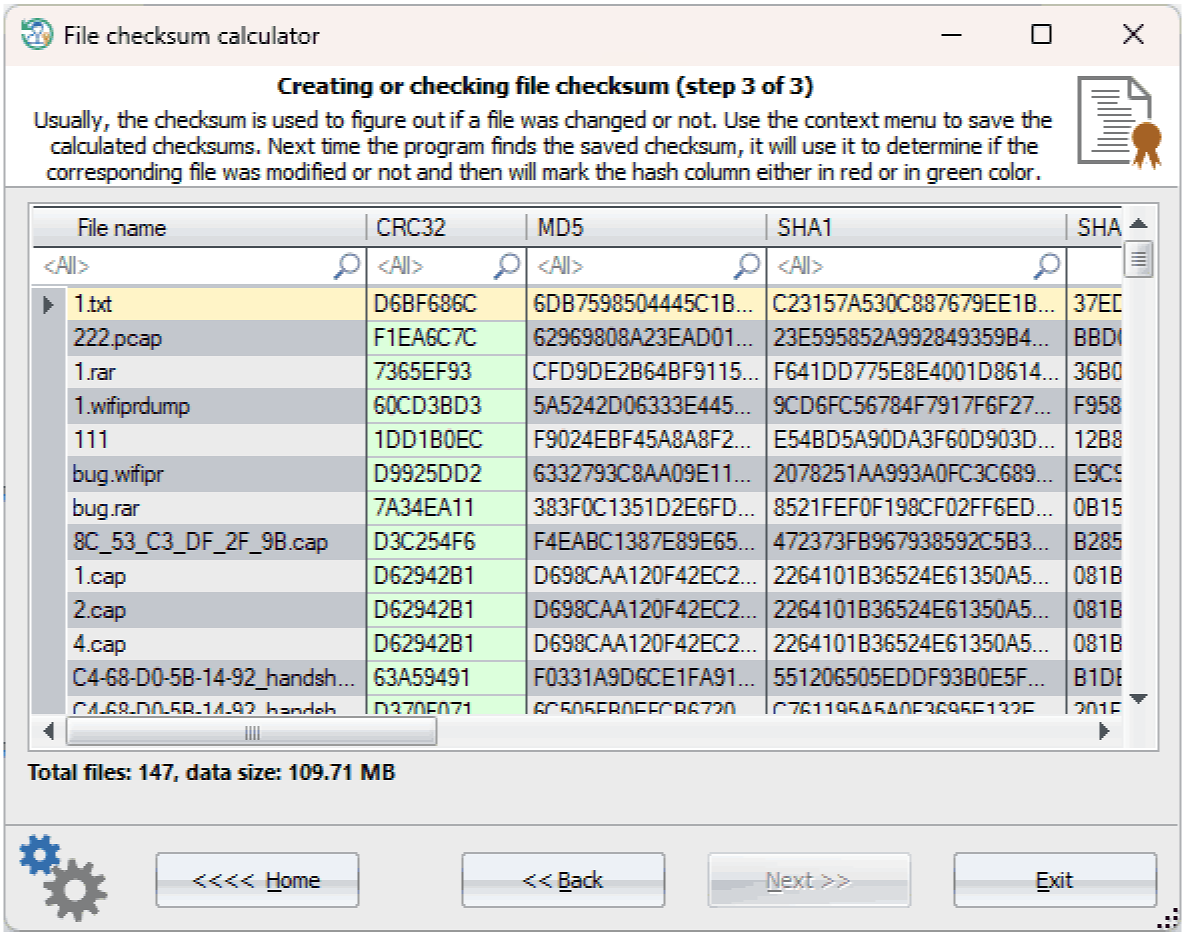
☑ Process files in all sub-folders (in selected folder otherwise)

□ Do not scan for saved checksums. Set this option for new checksum calculation only.

The program can operate in two modes processing either a single or multiple files at once. Select one you need. When using multiple files mode, be careful setting a directory that contains a lot of files. Even though the checksum calculation will not take much, outputting the result may stall the program for some while.

By default, the program simultaneously calculates and checks files checksums. You can set off scanning for saved checksums setting on the appropriate option.

View calculated checksum and hashes



Creating or checking file checksum (step 3 of 3)

Usually, the checksum is used to figure out if a file was changed or not. Use the context menu to save the calculated checksums. Next time the program finds the saved checksum, it will use it to determine if the corresponding file was modified or not and then will mark the hash column either in red or in green color.

File name	CRC32	MD5	SHA1	SHA
<All>	<All>	<All>	<All>	
1.txt	D6BF686C	6DB7598504445C1B...	C23157A530C887679EE1B...	37ED
222.pcap	F1EA6C7C	62969808A23EAD01...	23E595852A992849359B4...	BBD(
1.rar	7365EF93	CFD9DE2B64BF9115...	F641DD775E8E4001D8614...	36B0
1.wifiprdump	60CD3BD3	5A5242D06333E445...	9CD6FC56784F7917F6F27...	F958
111	1DD1B0EC	F9024EBF45A8A8F2...	E54BD5A90DA3F60D903D...	12B8
bug.wifipr	D9925DD2	6332793C8AA09E11...	2078251AA993A0FC3C689...	E9C9
bug.rar	7A34EA11	383F0C1351D2E6FD...	8521FEF0F198CF02FF6ED...	0B15
8C_53_C3_DF_2F_9B.cap	D3C254F6	F4EABC1387E89E65...	472373FB967938592C5B3...	B285
1.cap	D62942B1	D698CAA120F42EC2...	2264101B36524E61350A5...	081B
2.cap	D62942B1	D698CAA120F42EC2...	2264101B36524E61350A5...	081B
4.cap	D62942B1	D698CAA120F42EC2...	2264101B36524E61350A5...	081B
C4-68-D0-5B-14-92_handsh...	63A59491	F0331A9D6CE1FA91...	551206505EDDF93B0E5F...	B1DE
C4-68-D0-5B-14-92_handsh	D370F071	6C505FB0FFCB6720	C761195A5A0F3695F132F	201F

Total files: 147, data size: 109.71 MB

The algorithm of scanning saved checksum is pretty straightforward. Once the program detects a file with appropriate extension (*.crc, *.md5, *.sha, *.sha256 or *.sha512), it will use it to compare with the calculated one.

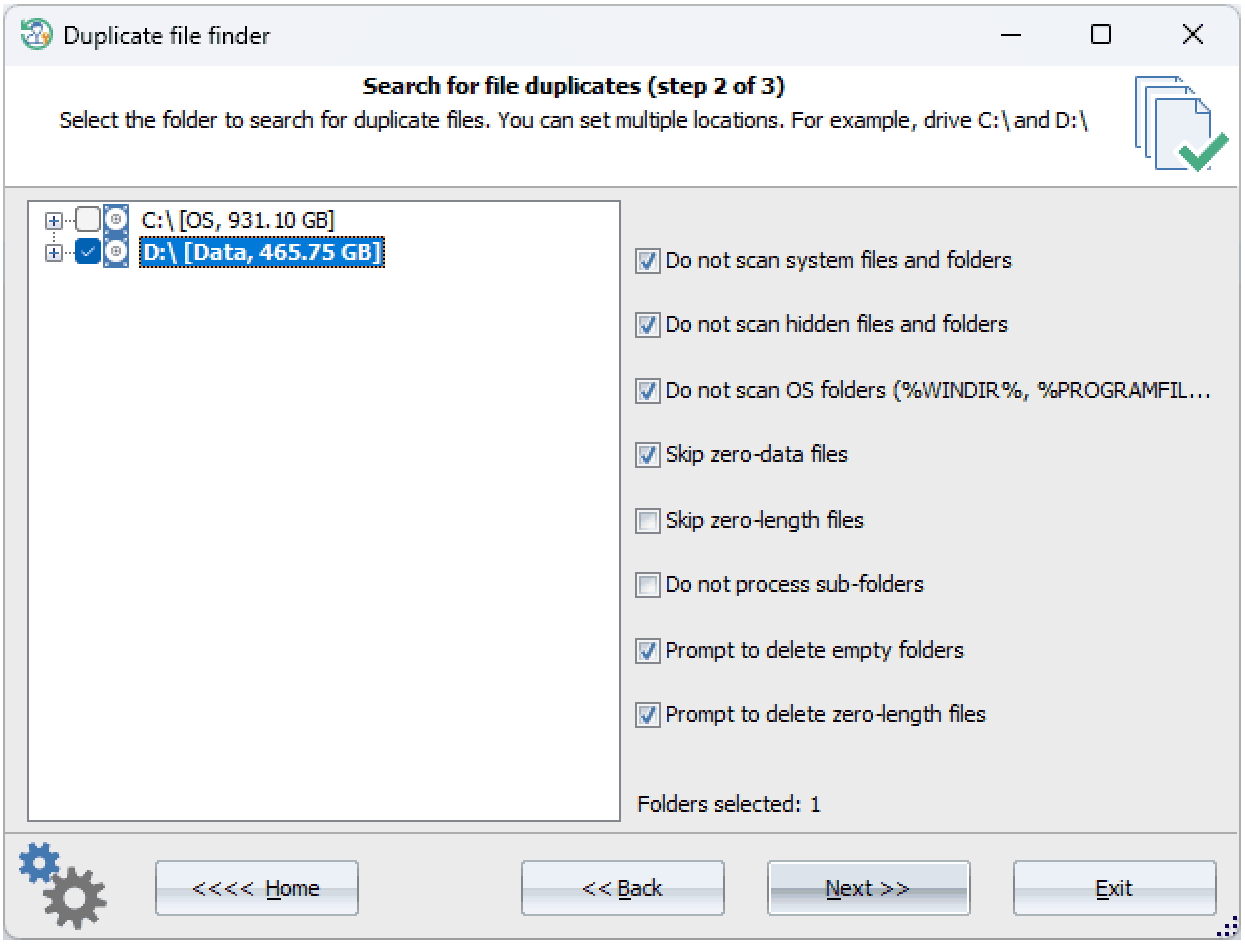
For example, when the program finds the file named readme.txt, it first calculates the file's CRC32, MD5, SHA-1, SHA256 and SHA512 hashes. Then it scans the current directory for readme.txt.crc, readme.txt.md5 … readme.sha512 files and, if one is found, reads the hash from this file and compares it to the calculated hash. If the hashes are match, the tool marks the appropriate table column in green, otherwise in red color (which means the file was modified since the time the hash was saved).

To save the calculated hash(es), right-click the table to open the context menu and select 'Save'.

3.8.9 Duplicate file finder

If you have thousands of music files, documents, photos or videos and you are running out of disk space, this tool is right for you. It will help you to locate and remove useless file duplicates, empty files and folders literally, in a couple of mouse-clicks. We tried to make this tool as fast as possible and optimized the speed of the duplicate search algorithm for modern hardware with SSDs and multi-core CPUs.

Selecting source folder to scan for file duplicates



Search for file duplicates (step 2 of 3)

Select the folder to search for duplicate files. You can set multiple locations. For example, drive C:\ and D:\

- □ C:\ [OS, 931.10 GB]
- ☑ D:\ [Data, 465.75 GB]

☑ Do not scan system files and folders

☑ Do not scan hidden files and folders

☑ Do not scan OS folders (%WINDIR%, %PROGRAMFIL...

☑ Skip zero-data files

□ Skip zero-length files

□ Do not process sub-folders

☑ Prompt to delete empty folders

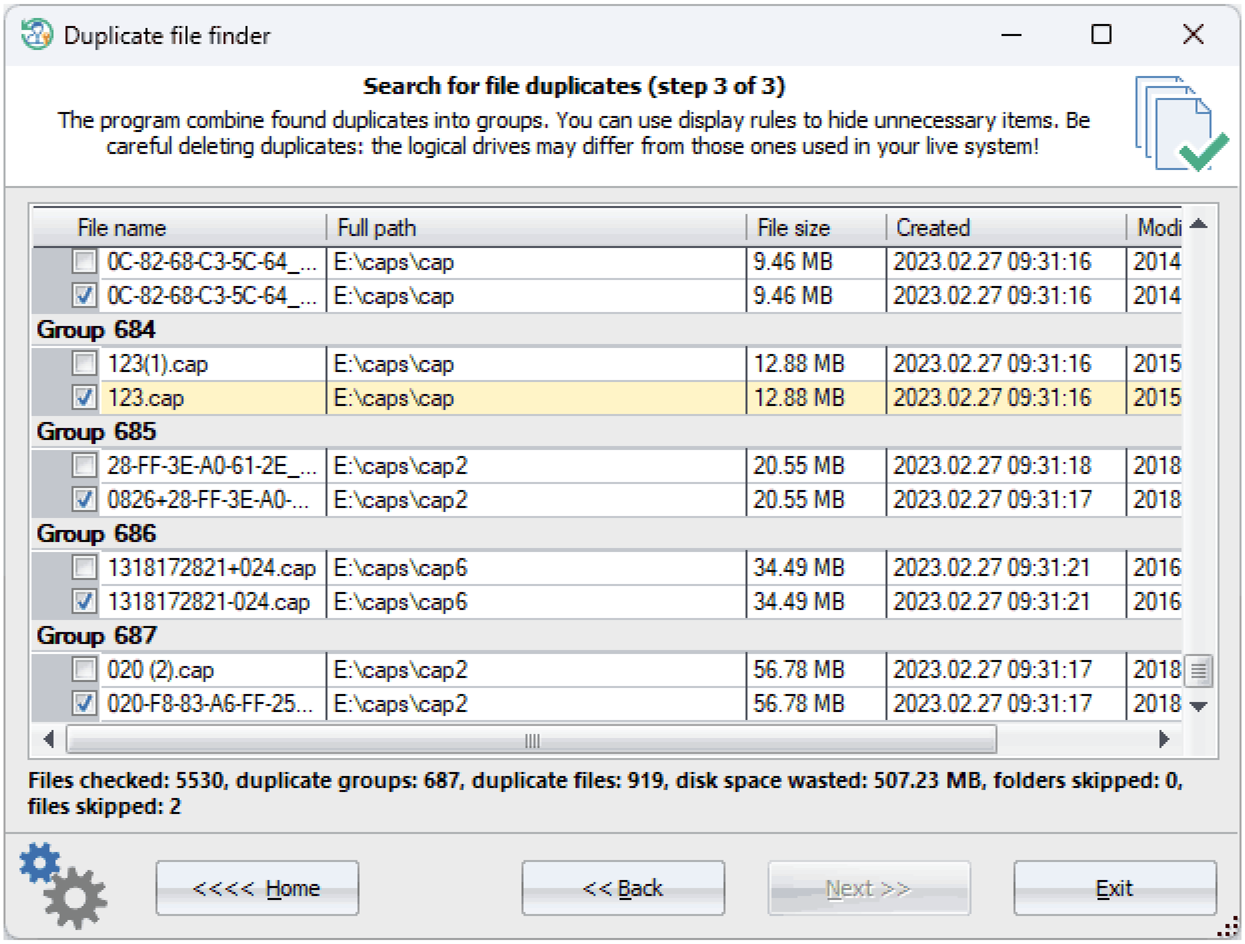
☑ Prompt to delete zero-length files

Folders selected: 1

Select the source drive or folder where to search for duplicate files. There are a set of additional options you can play around:

- **Do not scan system files or folders.** Skip files and folders that have the SYSTEM attribute set on.
- **Do not scan hidden files or folders.** Skip file and folder items that have the HIDDEN attribute set on.
- **Do not scan OS folders.** Skip Windows system folders, such as %WINDIR%, %PROGRAMFILES%, %PROGRAMDATA%, etc.
- **Skip empty-data files.** Do not process files filled up with zeros.
- **Skip zero-length files.** Do not process files with zero length.
- **Do not process sub-folders.** Scan the current directory only.
- **Prompt to delete empty folders.** Prompt to delete directories that do not contain any files or folders. Use with care. Windows may use some empty folders.
- **Prompt to delete zero-length files.** Prompt to delete files with zero length.

Processing file duplicates



Search for file duplicates (step 3 of 3)

The program combine found duplicates into groups. You can use display rules to hide unnecessary items. Be careful deleting duplicates: the logical drives may differ from those ones used in your live system!

File name	Full path	File size	Created	Modi
□ 0C-82-68-C3-5C-64_...	E:\caps\cap	9.46 MB	2023.02.27 09:31:16	2014
☑ 0C-82-68-C3-5C-64_...	E:\caps\cap	9.46 MB	2023.02.27 09:31:16	2014
Group 684				
□ 123(1).cap	E:\caps\cap	12.88 MB	2023.02.27 09:31:16	2015
☑ 123.cap	E:\caps\cap	12.88 MB	2023.02.27 09:31:16	2015
Group 685				
□ 28-FF-3E-A0-61-2E_...	E:\caps\cap2	20.55 MB	2023.02.27 09:31:18	2018
☑ 0826+28-FF-3E-A0-...	E:\caps\cap2	20.55 MB	2023.02.27 09:31:17	2018
Group 686				
□ 1318172821+024.cap	E:\caps\cap6	34.49 MB	2023.02.27 09:31:21	2016
☑ 1318172821-024.cap	E:\caps\cap6	34.49 MB	2023.02.27 09:31:21	2016
Group 687				
□ 020 (2).cap	E:\caps\cap2	56.78 MB	2023.02.27 09:31:17	2018
☑ 020-F8-83-A6-FF-25...	E:\caps\cap2	56.78 MB	2023.02.27 09:31:17	2018

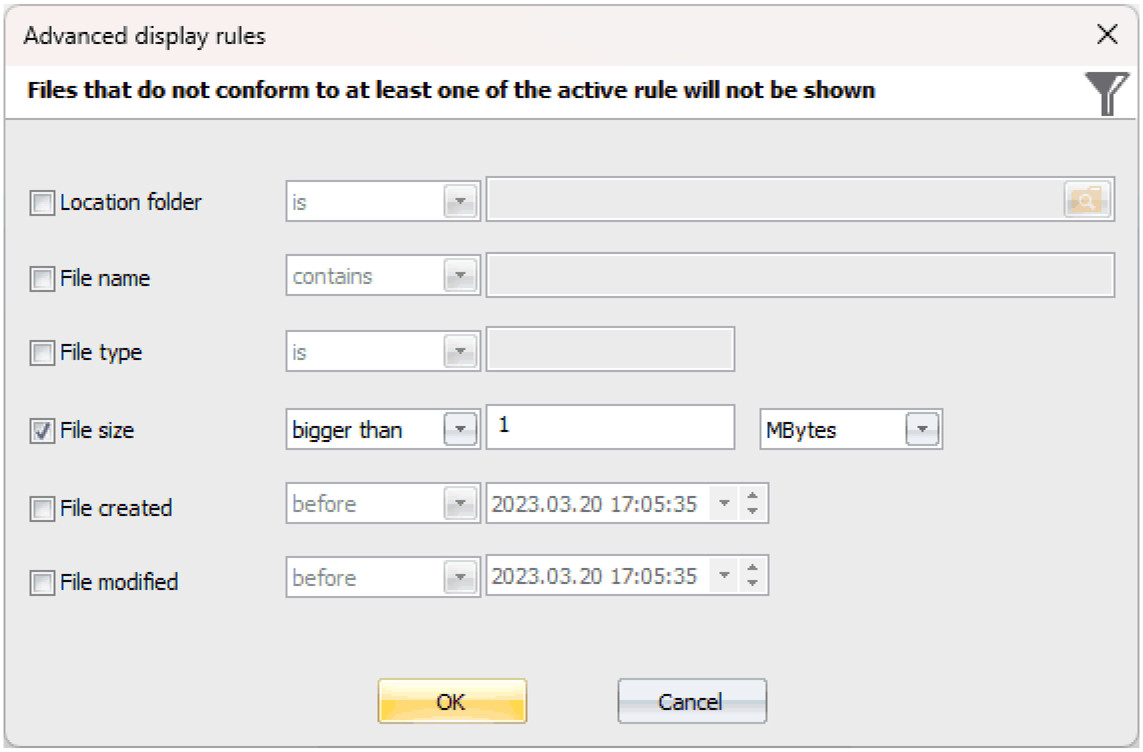
Files checked: 5530, duplicate groups: 687, duplicate files: 919, disk space wasted: 507.23 MB, folders skipped: 0, files skipped: 2

Once the scan process is over, the program first asks to delete all found empty files and folders (if the appropriate options are set). Be careful, some empty items may be used by Windows. This option is often used to clear the directory structure.

For example, both Windows 10 and 11 have a bug that leave thousand of empty folders in the following directory:
C:\Windows\System32\config\systemprofile\AppData\Local
All folders looks like this **tw-XXXX-XXXX-XXXXXX.tmp**, where **X** is a hexadecimal value.
You can use the program to delete all empty sub-folders out of the initial folder. To do that, make sure you have set at least two options:

- Do not process sub-folders. This option ensures the program will not process any empty folders deeper down the first level sub-folder.
- Prompt to delete empty folders

RWP combines all found file duplicates into groups. A group consists of at least two identical files. By default, the program automatically sets for deletion every item after the first one in every group. You are free to select/deselect any necessary file items or to set up your own display rules. For example, to hide all files less than 1 MB, use the display rule as shown below.



Advanced display rules

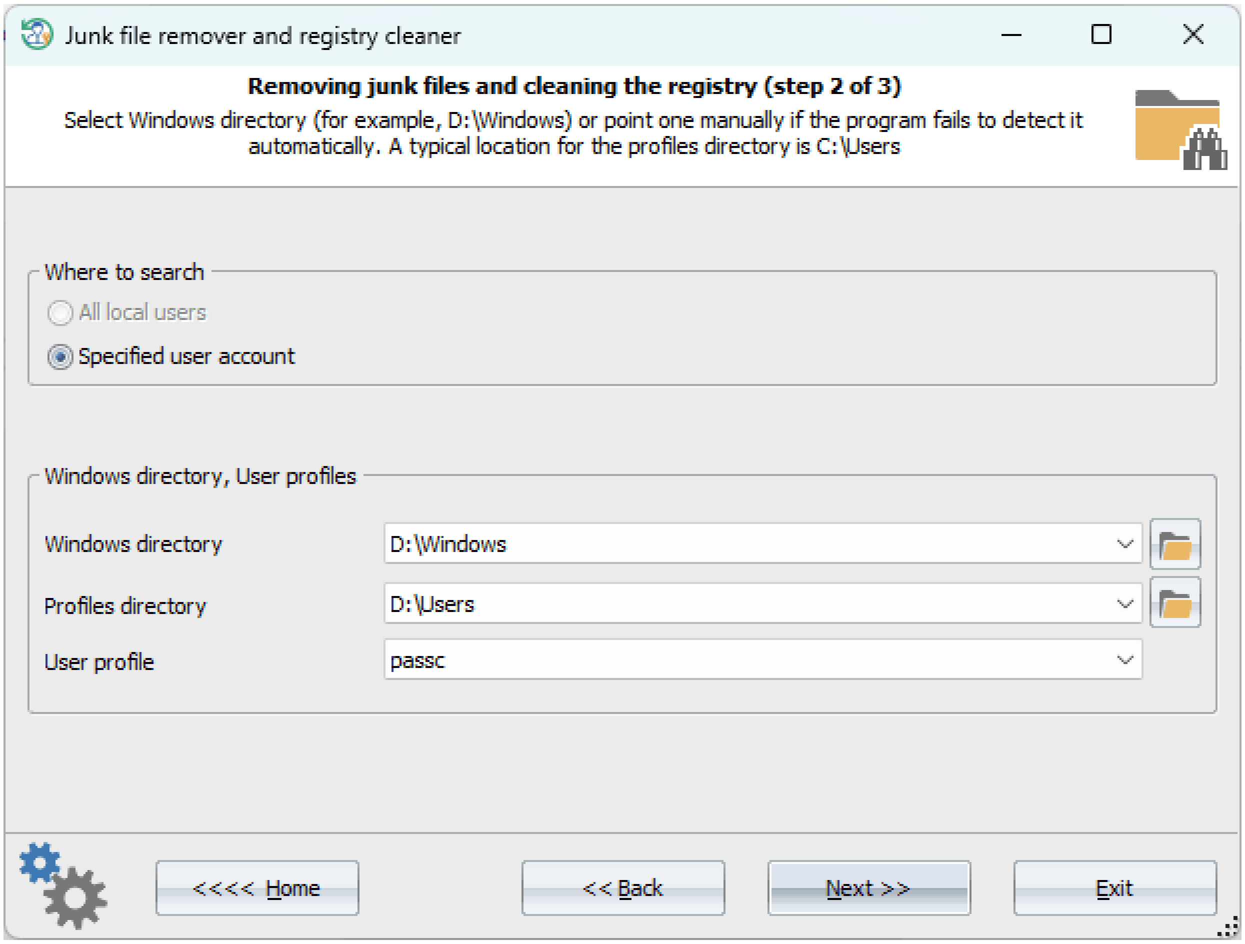
Files that do not conform to at least one of the active rule will not be shown

□ Location folder	is		
□ File name	contains		
□ File type	is		
☑ File size	bigger than	1	MBytes
□ File created	before	2023.03.20 17:05:35	
□ File modified	before	2023.03.20 17:05:35	

3.8.10 Junk file remover and registry cleaner

This feature of the program helps you eliminate redundant entries from your computer's registry, improving system stability and resolving various performance issues to revitalize the system. It also goes the extra mile by performing a comprehensive disk cleanup, targeting junk files that accumulate over time. These include temporary files, system and browser caches, old downloads, unnecessary backups, and much more. Removing these digital burdens frees up substantial disk space, resulting in faster program and system loading times, improved responsiveness, and smoother overall performance.

Setting system directories and user profile



Junk file remover and registry cleaner

Removing junk files and cleaning the registry (step 2 of 3)

Select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it automatically. A typical location for the profiles directory is C:\Users

Where to search

○ All local users

● Specified user account

Windows directory, User profiles

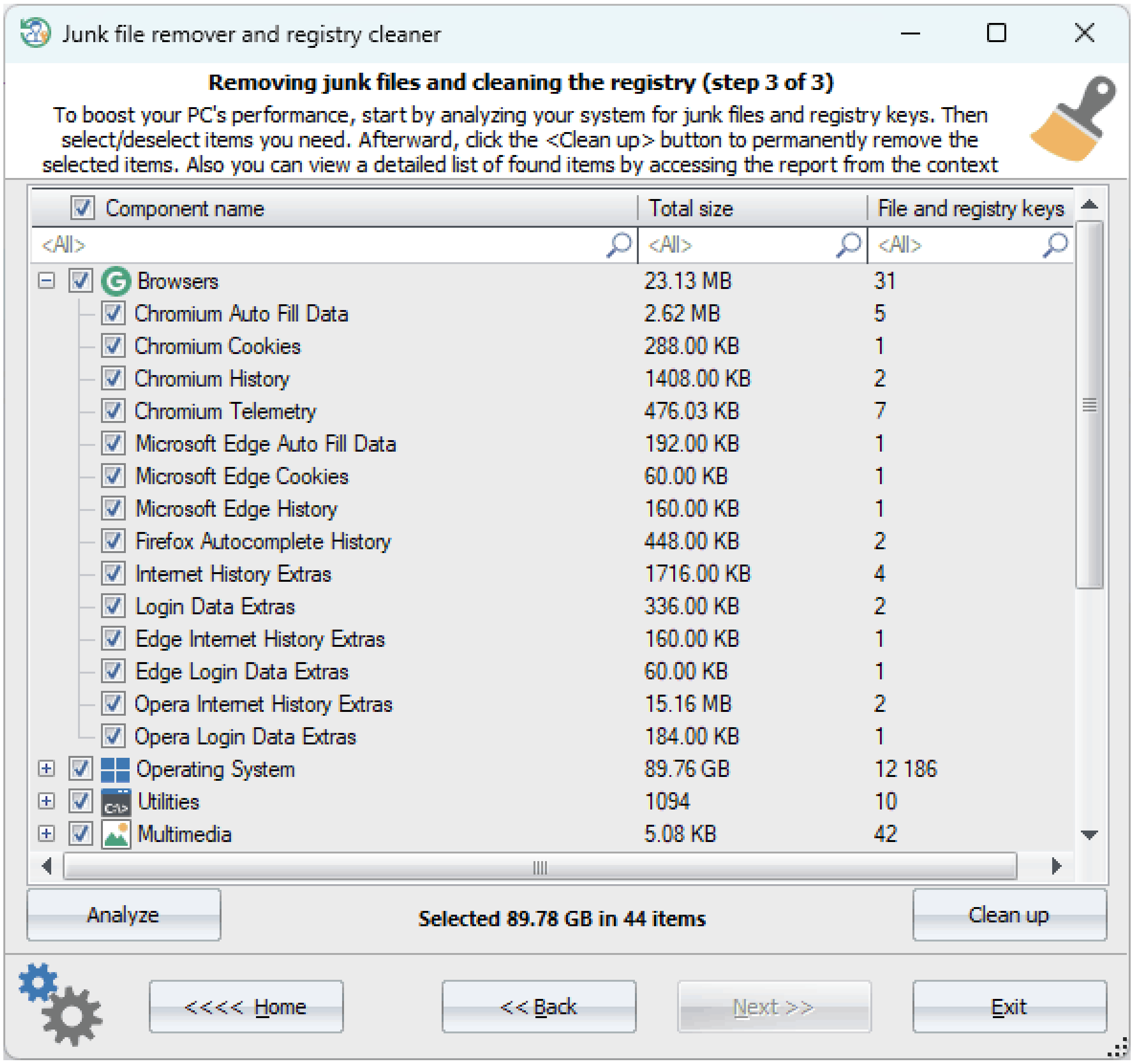
Windows directory: D:\Windows

Profiles directory: D:\Users

User profile: passc

With its easy-to-use, sleek, and intuitive interface, the program ensures hassle-free optimization, even for novice users. To get started, simply select the Windows directory and the target user whose profile you want to scan.

Removing found junk files and registry keys



Removing junk files and cleaning the registry (step 3 of 3)

To boost your PC's performance, start by analyzing your system for junk files and registry keys. Then select/deselect items you need. Afterward, click the <Clean up> button to permanently remove the selected items. Also you can view a detailed list of found items by accessing the report from the context

☑ Component name	Total size	File and registry keys
<All>	<All>	<All>
⊟ ☑ Browsers	23.13 MB	31
☑ Chromium Auto Fill Data	2.62 MB	5
☑ Chromium Cookies	288.00 KB	1
☑ Chromium History	1408.00 KB	2
☑ Chromium Telemetry	476.03 KB	7
☑ Microsoft Edge Auto Fill Data	192.00 KB	1
☑ Microsoft Edge Cookies	60.00 KB	1
☑ Microsoft Edge History	160.00 KB	1
☑ Firefox Autocomplete History	448.00 KB	2
☑ Internet History Extras	1716.00 KB	4
☑ Login Data Extras	336.00 KB	2
☑ Edge Internet History Extras	160.00 KB	1
☑ Edge Login Data Extras	60.00 KB	1
☑ Opera Internet History Extras	15.16 MB	2
☑ Opera Login Data Extras	184.00 KB	1
⊞ ☑ Operating System	89.76 GB	12 186
⊞ ☑ Utilities	1094	10
⊞ ☑ Multimedia	5.08 KB	42

Selected 89.78 GB in 44 items

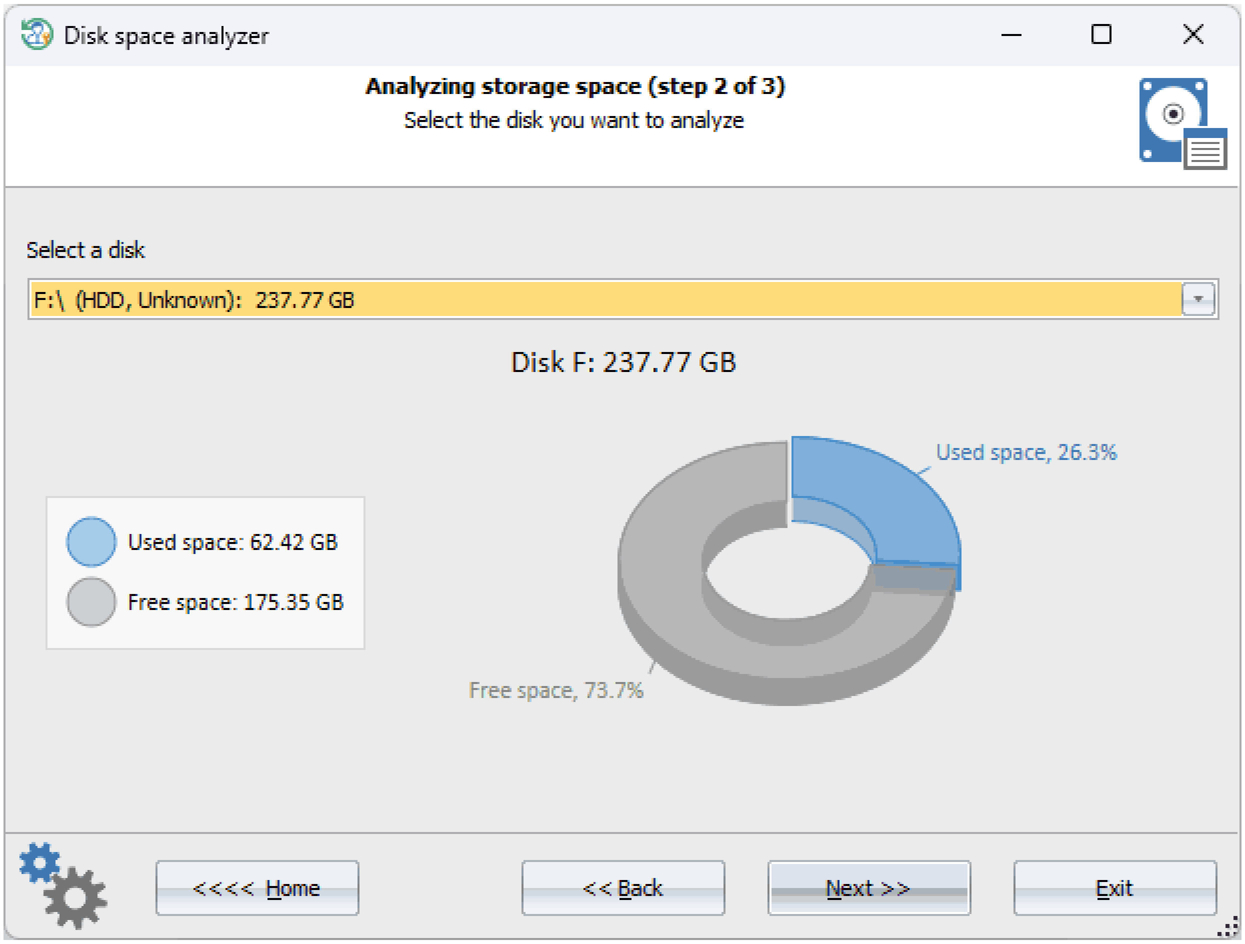
In the final dialog, click the *'Analyze'* button to initiate the scanning process, which populates a table with the list of found junk files and registry keys. From there, you can select or deselect specific items in the table before proceeding with the final cleanup. Once you are ready, click the *'Clean up'* button to remove the selected junk items that were found.

Remember, it's always recommended to create a backup of your registry and important files before making any changes to ensure that you can revert back in case any unexpected issues arise. This precautionary step will help safeguard your data and provide peace of mind as you optimize your system with this powerful tool.

3.8.11 Disk space analyzer

Analyzing your computer's disk space can be a daunting task, but with this new feature, it has become easy and extremely fast. All you need to do is select the disk and the program will sort out all the files and folders by the valuable space they are using, in literally a blink of an eye. In fact, this is one of the fastest tools for that. Once the analysis is complete, you can generate and view the disk report, or delete unnecessary items to free up some disk space.

Selecting logical disk



Analyzing storage space (step 2 of 3)

Select the disk you want to analyze

Select a disk

F:\ (HDD, Unknown): 237.77 GB

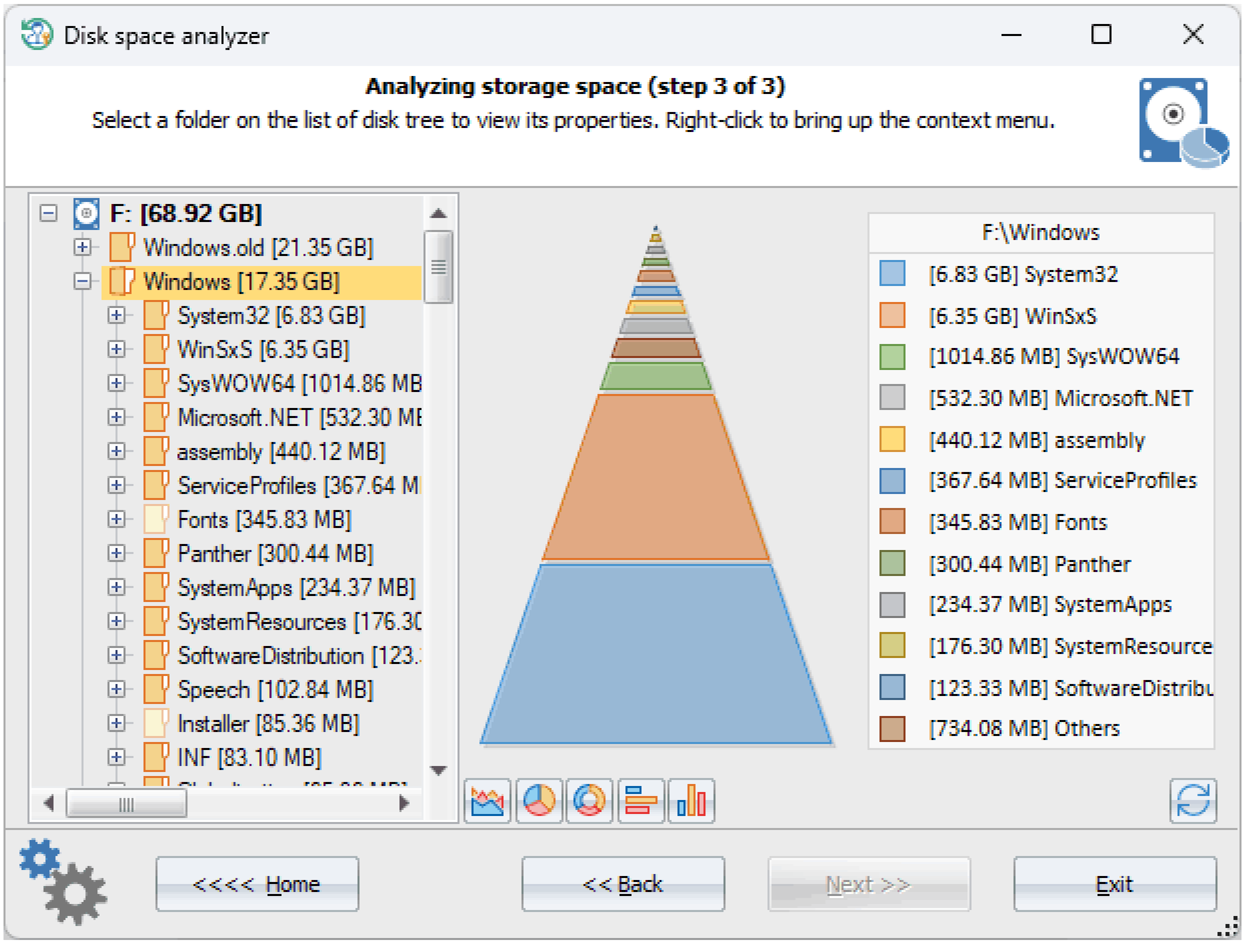
Disk F: 237.77 GB

Used space: 62.42 GB

Free space: 175.35 GB

Choose the logical disk you want to analyze. Upon the program's initial access to the disk, it analyzes the disk structure and saves it to a cache file. Typically, this process takes less than a minute, but may greatly depend on the disk's item count and its speed. After that, every subsequent access to the disk occurs nearly instantaneously.

Disk space analyzer



Analyzing storage space (step 3 of 3)

Select a folder on the list of disk tree to view its properties. Right-click to bring up the context menu.

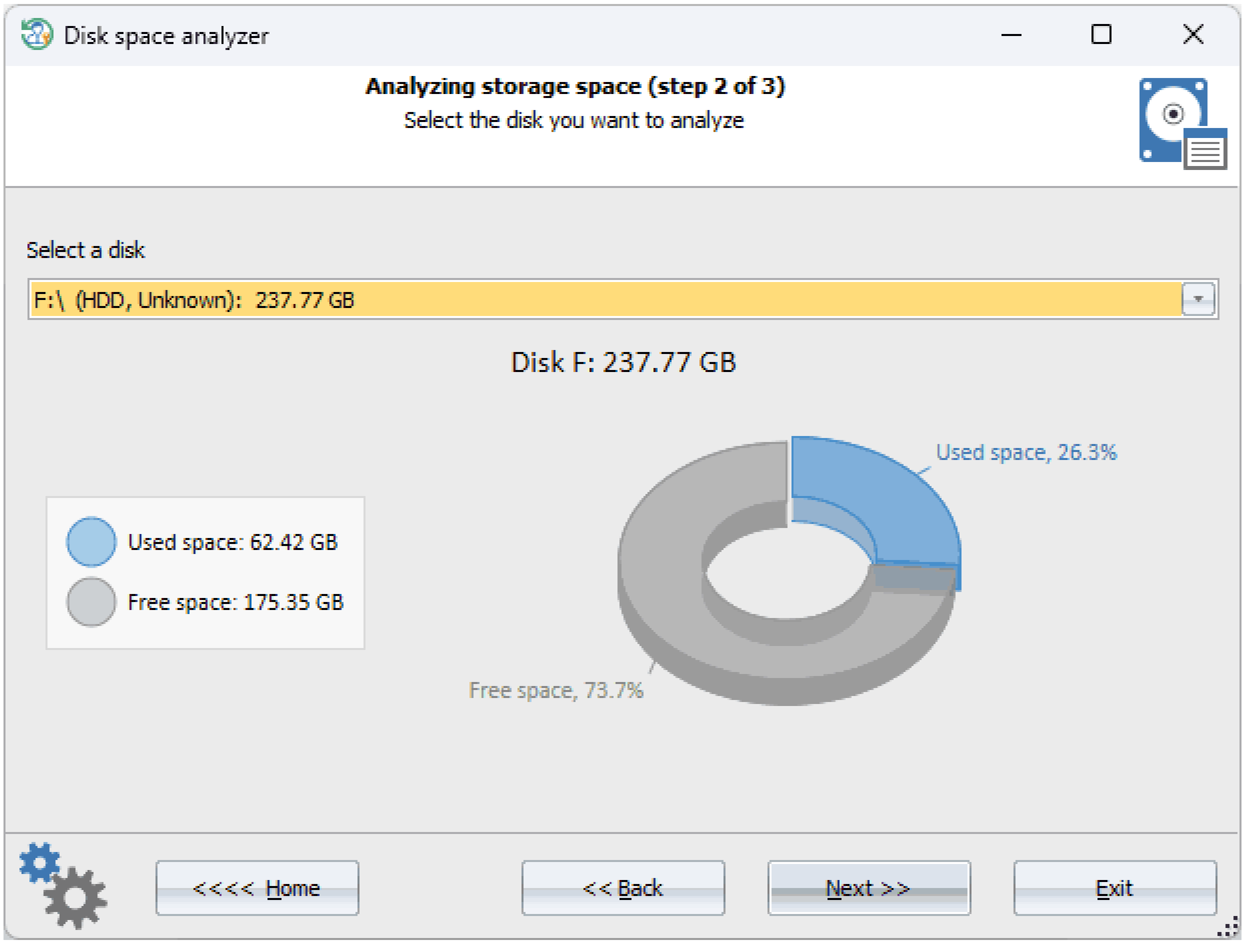
The program automatically organizes files and folders based on their size, ensuring that the largest ones appear first in the list. This way, you can quickly figure out which are the top files or folders consuming valuable disk space. Users can utilize the context menu to open the folder location, free up space by deleting selected items, or generate a file report.

3.8.12 File statistics

This comprehensive file and folder analysis tool allows you to:

- Gain in-depth insights into the structure and contents of your hard drives
- Scan instantly individual folders or entire drive
- Categorize and sort files based on type or size
- Instantly locate files of specific formats, such as images, videos, or documents
- Generate detailed reports outlining file types, sizes, attributes, date of modification/creation, etc.

Selecting logical disk



Disk space analyzer

Analyzing storage space (step 2 of 3)

Select the disk you want to analyze

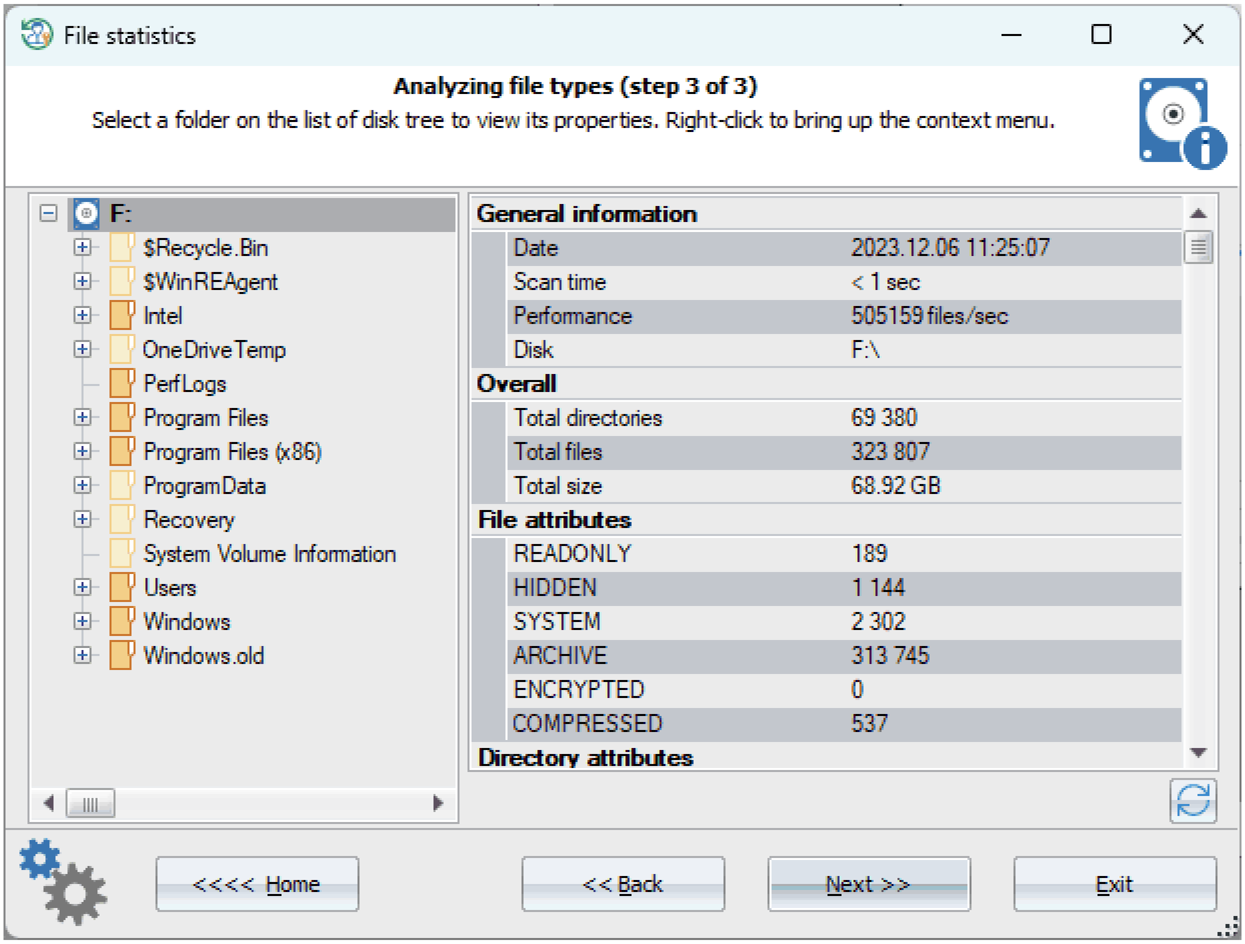
Select a disk

F:\ (HDD, Unknown): 237.77 GB

Disk F: 237.77 GB

Select the logical disk you need to analyze. Upon initial access, the program saves the file and folder structure to a cache file. This process usually takes less than a minute, although the duration may vary depending on the volume of items on the disk and the disk speed. Following this, every subsequent access to the cached disk occurs nearly instantaneously.

Analyzing files and folders



Analyzing file types (step 3 of 3)

Select a folder on the list of disk tree to view its properties. Right-click to bring up the context menu.

- F:
  - $Recycle.Bin
  - $WinREAgent
  - Intel
  - OneDriveTemp
  - PerfLogs
  - Program Files
  - Program Files (x86)
  - ProgramData
  - Recovery
  - System Volume Information
  - Users
  - Windows
  - Windows.old

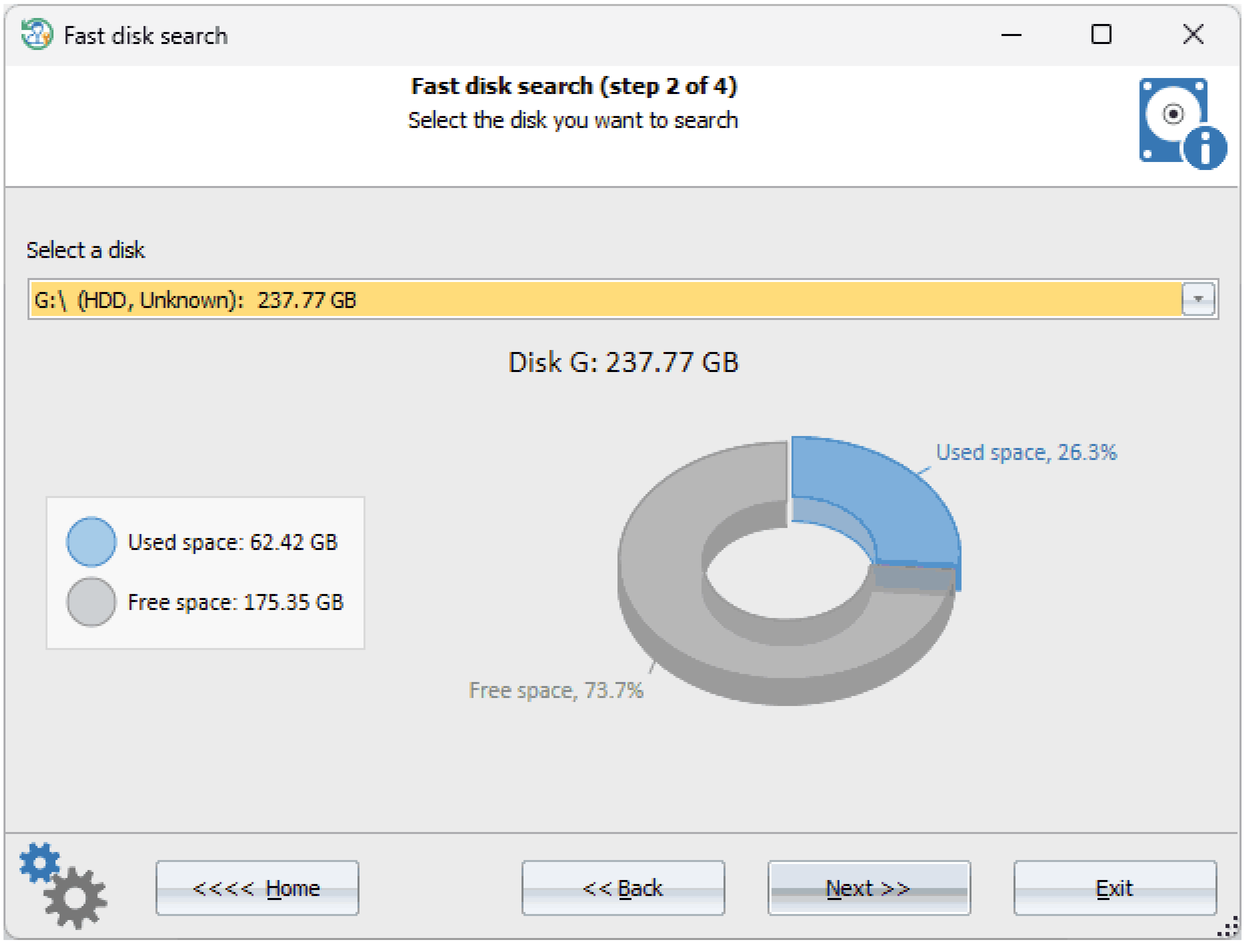
General information	
Date	2023.12.06 11:25:07
Scan time	< 1 sec
Performance	505159 files/sec
Disk	F:\
Overall	
Total directories	69 380
Total files	323 807
Total size	68.92 GB
File attributes	
READONLY	189
HIDDEN	1 144
SYSTEM	2 302
ARCHIVE	313 745
ENCRYPTED	0
COMPRESSED	537
Directory attributes	

You have the option to view statistics for either the entire drive or individual folders. Simply select the one you need. To generate an HTML report, utilize the context menu.

3.8.13 Fast disk search

This program's feature is designed to quickly search for files and their contents on a selected disk. Our innovative searching algorithm sets a new standard for speed and precision among Windows programs. For instance, locating a file by name or mask on a standard disk containing approximately 1 million files is practically instantaneous, clocking in at just about 1 second. Moreover, the program boasts advanced search rules that cater to the needs of even the most discerning and sophisticated users.

Selecting source disk



Fast disk search

Fast disk search (step 2 of 4)

Select the disk you want to search

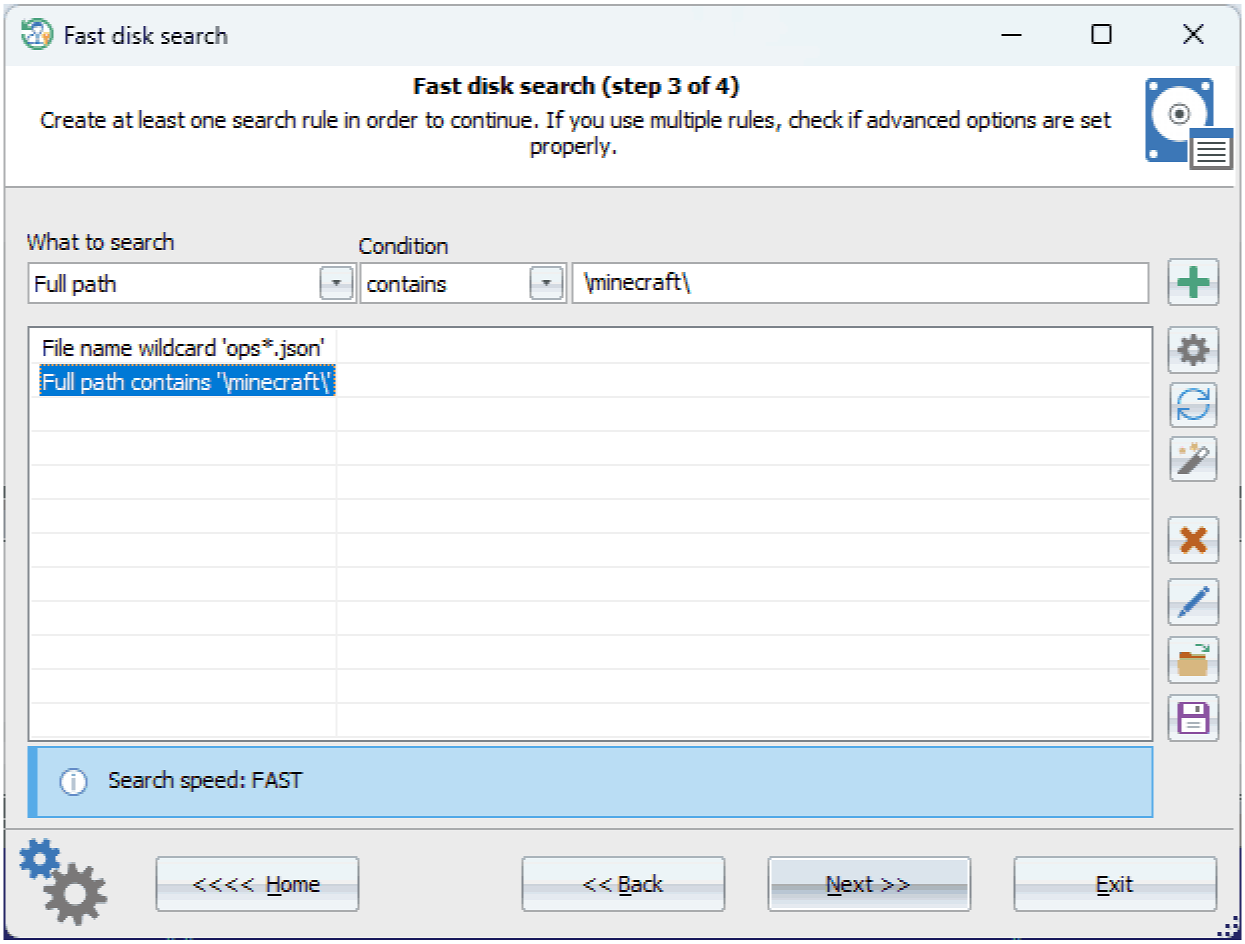
Select a disk

G:\ (HDD, Unknown): 237.77 GB

Disk G: 237.77 GB

Select the disk you want to search through.

Setting up searching rules



Fast disk search

Fast disk search (step 3 of 4)

Create at least one search rule in order to continue. If you use multiple rules, check if advanced options are set properly.

What to search: Full path

Condition: contains

\minecraft\

File name wildcard 'ops*.json'

Full path contains '\minecraft\'

Search speed: FAST

The program offers a wide range of rules that can be combined with each other. The Settings button defines how to process multiple rules:

- If you select '*Match all rules*', the search is considered successful if the searched file or folder satisfies all the specified rules
- If you select *'Match at least one rule*', the search is considered successful if the searched file or folder matches at least one rule.

Rules can be added, deleted, edited, as well as saved to disk or read from disk. It is also possible to use ready-made rule sets to search for secret keys, passwords, dumps, etc.

Each rule consists of three elements: a search object, an operation on the search object, and the condition itself. For example, on the screenshot above, the following is specified:
Search object - **full path**
Operation - **contains**
Condition - **\minecraft**

Search objects
Filename - the name of the file along with extension. For example, readme.txt
File extension - the extension of the file (without a dot). For example, EXE
File size - the size of the file
File type - the type of file. For example, *Code* - source code files.
File attributes - e.g., archive, system, read-only, etc.
File creation date - creation date without time
File modification date - the date of modification without time

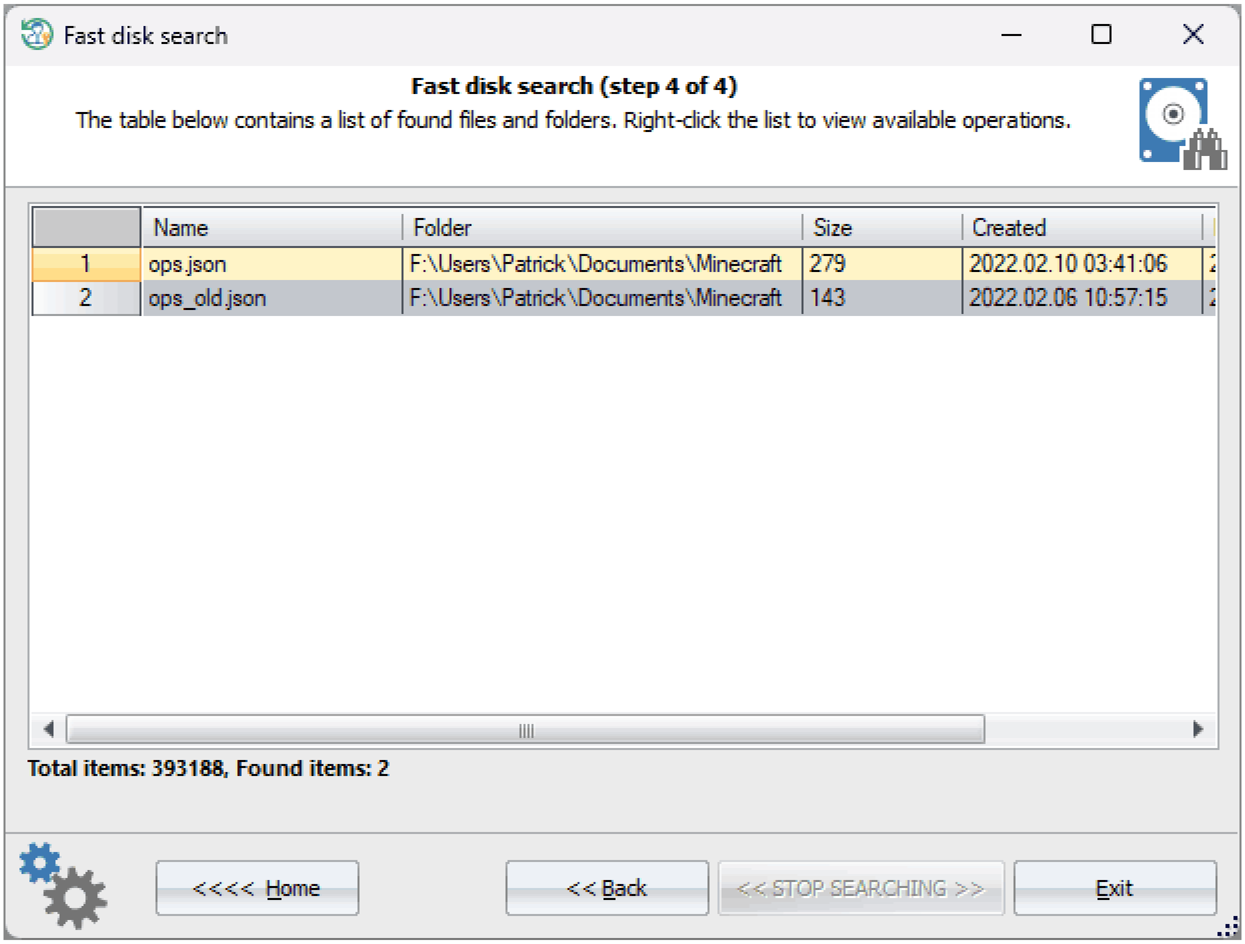
File creation time - full creation date with time
File modification time - full date of last modification with time
Text string in content - a text string. The program performs a 3-pass lookup, automatically searching for ANSI, UTF8 and UTF16 strings
Binary data in the content - binary data in the file
Folder name - folder name with extension, if any. For example, windows.old
Folder extension - the folder extension
Folder size - the size of all files in the folder (including files in any subfolders found)
Folder attributes - similar to file attributes
Folder creation date - similar to file
Folder modification date - similar to file
Folder creation time - similar to file
Folder modification time - similar to file
Full path - full path of a folder or file

Operations
The available operations depend on the search objects. For example, if you select a file/folder name or extension, the following operations are available:

- **Contains**
- **Does not contain**
- **Completely matches**
- **Does not match**
- **Begins with**
- **Ends with**
- **File mask**
- **Regular expression**

Be careful, specifying regular expressions as well as content search can slow down the search speed considerably.

Search results



Fast disk search

Fast disk search (step 4 of 4)

The table below contains a list of found files and folders. Right-click the list to view available operations.

	Name	Folder	Size	Created
1	ops.json	F:\Users\Patrick\Documents\Minecraft	279	2022.02.10 03:41:06
2	ops_old.json	F:\Users\Patrick\Documents\Minecraft	143	2022.02.06 10:57:15

Total items: 393188, Found items: 2

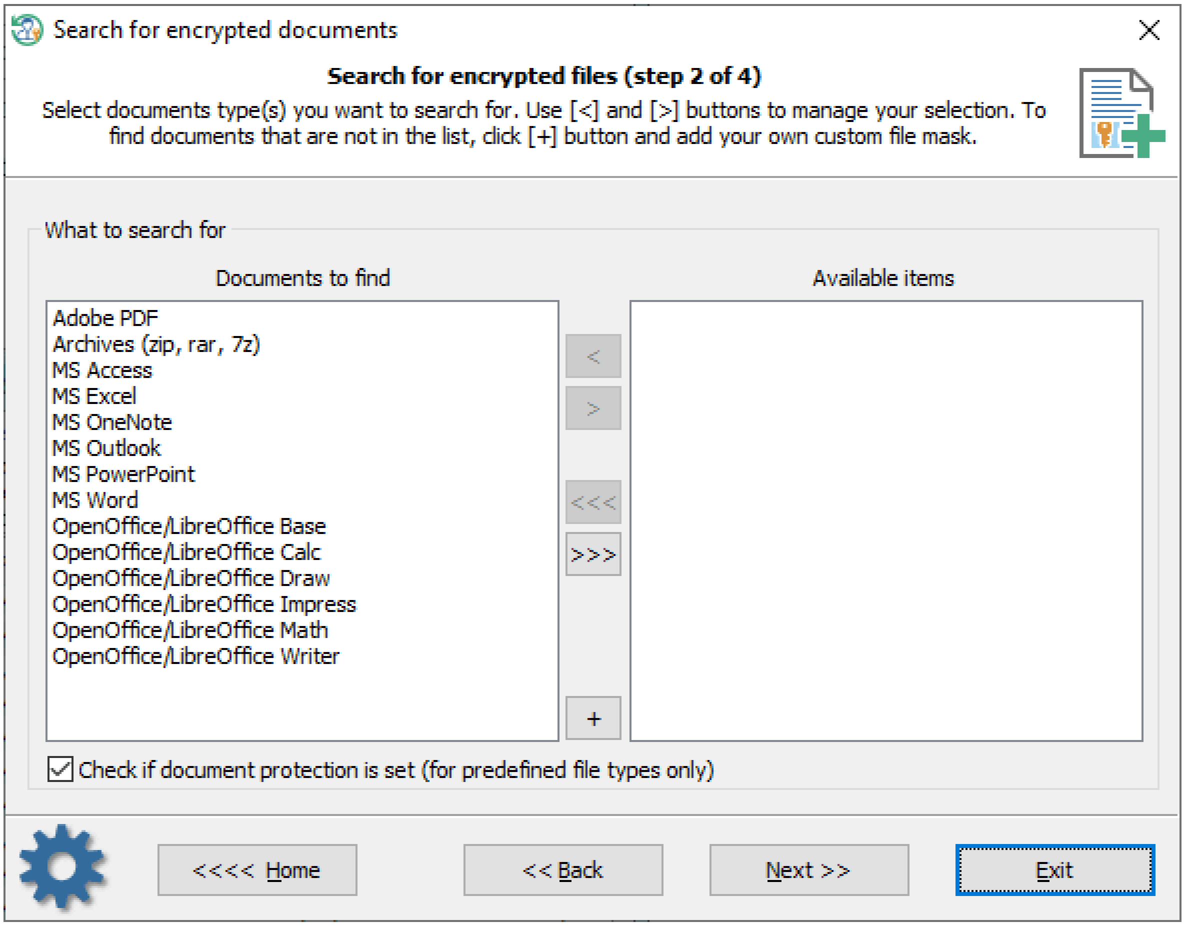
You can copy the search results to the clipboard, create an HTML report, or save them to a ZIP archive.

3.9 Utilities

3.9.1 Search for password-protected documents

This program's feature is aimed to scan and search a PC for encrypted documents, password-protected archives and files. It is easy to use, and fast and flexible in its configuration. You can even specify your own file types to look for. The search process is divided into three simple steps:

1 Selecting document type



Search for encrypted documents

Search for encrypted files (step 2 of 4)

Select documents type(s) you want to search for. Use [<] and [>] buttons to manage your selection. To find documents that are not in the list, click [+] button and add your own custom file mask.

What to search for

Documents to find	Available items
Adobe PDF Archives (zip, rar, 7z) MS Access MS Excel MS OneNote MS Outlook MS PowerPoint MS Word OpenOffice/LibreOffice Base OpenOffice/LibreOffice Calc OpenOffice/LibreOffice Draw OpenOffice/LibreOffice Impress OpenOffice/LibreOffice Math OpenOffice/LibreOffice Writer	

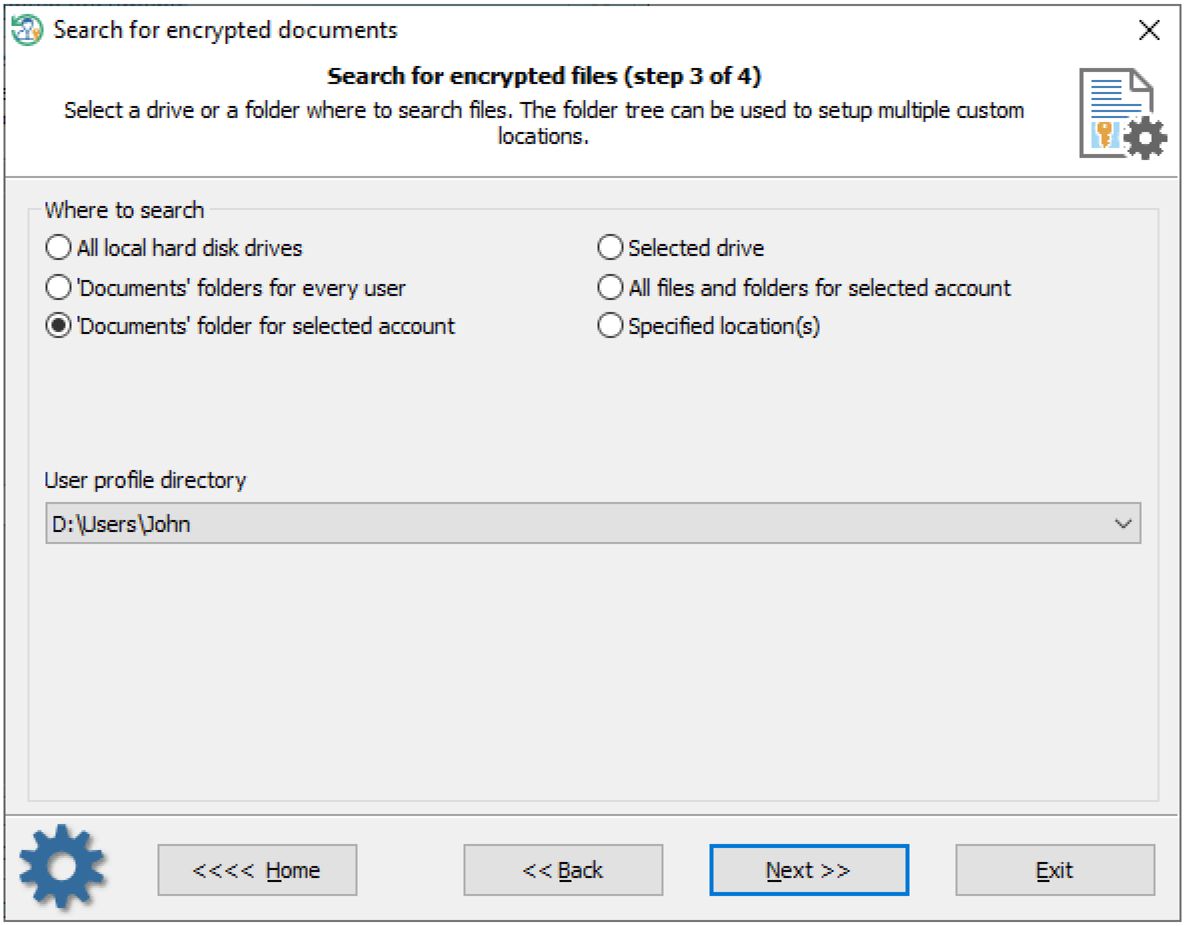
☑ Check if document protection is set (for predefined file types only)

By default, the program searches for the following pre-defined documents:

- File archives (zip, rar, 7z)
- Adobe PDF documents
- MS Word documents
- MS Excel tables
- MS Access databases
- MS PowerPoint presentations
- MS OneNote notes
- MS Outlook data files
- OpenOffice/LibreOffice Writer documents
- OpenOffice/LibreOffice Calc tables
- OpenOffice/LibreOffice Base databases
- OpenOffice/LibreOffice Impress presentations
- OpenOffice/LibreOffice Draw documents
- OpenOffice/LibreOffice Math documents

Use the [>] and [<] buttons to include or exclude available documents from the search process. If you want to add your own file types to search for, use the [+] button and specify your description and a search mask. For example, the following mask can be used to search for KeePass data files:
***.kdbx, *.kdb, *.pwd**
Keep in mind that password protection analysis is not used for the custom masks.
The 'Check if document protection is set...' option is used to completely turn off the password protection analysis. That could significantly speed up the search process in some cases.

2 Selecting where to search



Search for encrypted documents

Search for encrypted files (step 3 of 4)

Select a drive or a folder where to search files. The folder tree can be used to setup multiple custom locations.

Where to search

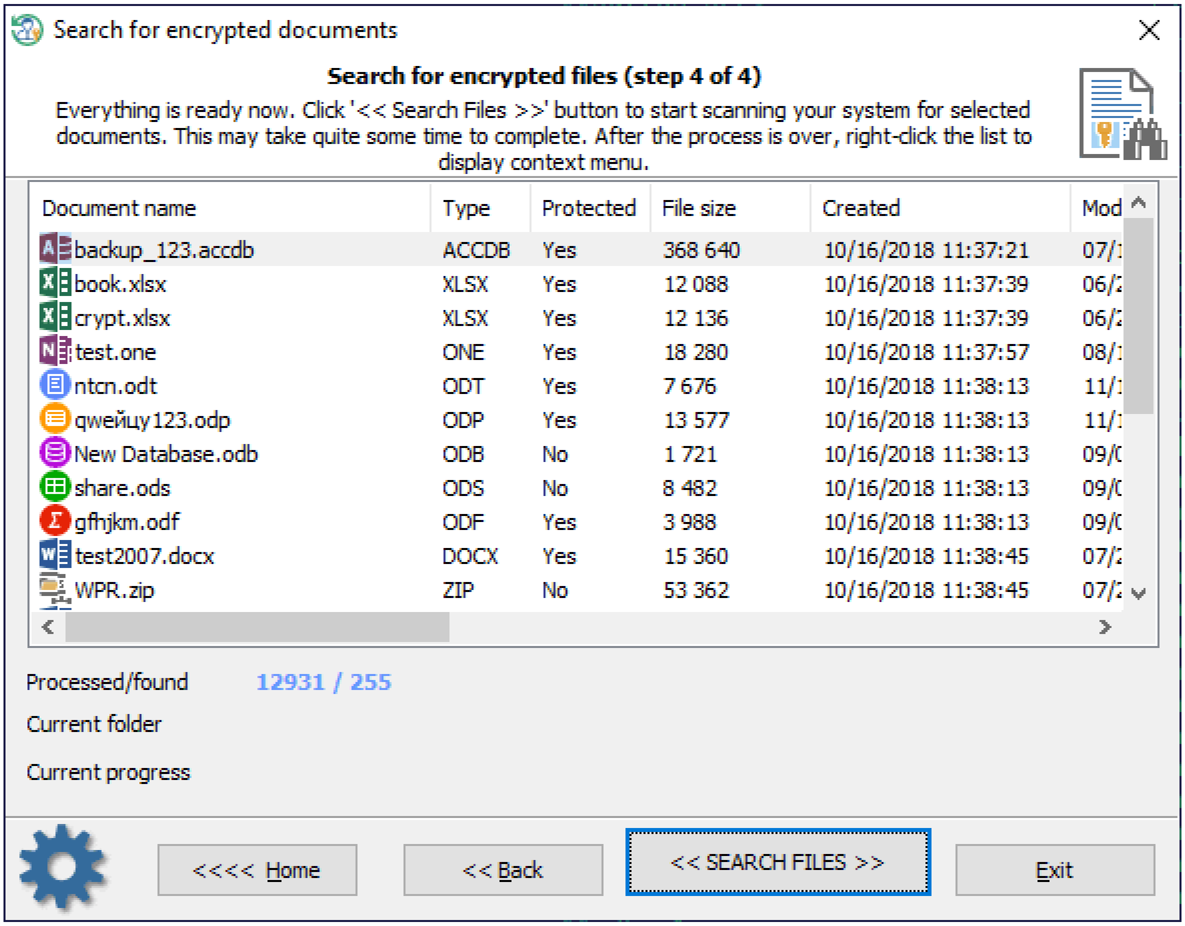
○ All local hard disk drives
○ 'Documents' folders for every user
● 'Documents' folder for selected account
○ Selected drive
○ All files and folders for selected account
○ Specified location(s)

User profile directory

D:\Users\John

You can narrow down the scanning range by setting up, for example, the 'Documents' folder for a selected account, or choosing a certain directory.

3 Searching for documents



Search for encrypted documents

Search for encrypted files (step 4 of 4)

Everything is ready now. Click '<< Search Files >>' button to start scanning your system for selected documents. This may take quite some time to complete. After the process is over, right-click the list to display context menu.

Document name	Type	Protected	File size	Created	Mod
backup_123.accdb	ACCDB	Yes	368 640	10/16/2018 11:37:21	07/1
book.xlsx	XLSX	Yes	12 088	10/16/2018 11:37:39	06/2
crypt.xlsx	XLSX	Yes	12 136	10/16/2018 11:37:39	06/2
test.one	ONE	Yes	18 280	10/16/2018 11:37:57	08/1
ntcn.odt	ODT	Yes	7 676	10/16/2018 11:38:13	11/1
qwейцу123.odp	ODP	Yes	13 577	10/16/2018 11:38:13	11/1
New Database.odb	ODB	No	1 721	10/16/2018 11:38:13	09/0
share.ods	ODS	No	8 482	10/16/2018 11:38:13	09/0
gfhjkm.odf	ODF	Yes	3 988	10/16/2018 11:38:13	09/0
test2007.docx	DOCX	Yes	15 360	10/16/2018 11:38:45	07/2
WPR.zip	ZIP	No	53 362	10/16/2018 11:38:45	07/2

Processed/found 12931 / 255

Current folder

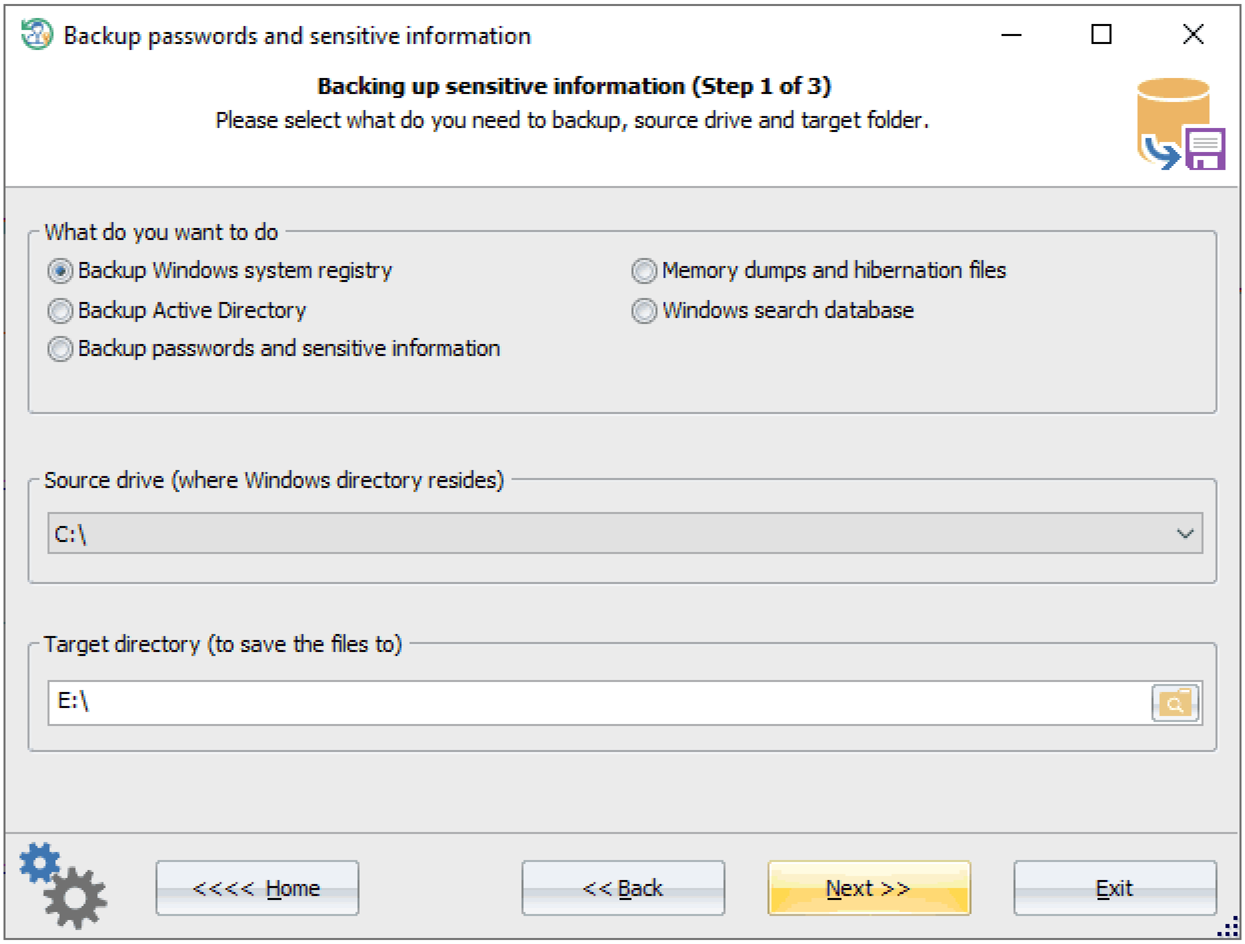
Current progress

Even though the program was optimized for fast search, scanning hard disks with a lot of files may take a long time. After the search is over, right-click the list of found documents to specify the available operations. For example, you can save the list of files found to a text/ html file, or create a single zip archive for the selected items.

3.9.2 Backup passwords and sensitive information

Sometimes it is vital to make a copy of Windows registry or an Active Directory database. **Reset Windows Password** is a lifesaver for those who need to back up the files easily. It can even make a snapshot of all sensitive data of the target PC in just a couple of clicks.

Setting what do you want to backup



Backup passwords and sensitive information

Backing up sensitive information (Step 1 of 3)

Please select what do you need to backup, source drive and target folder.

What do you want to do

- ● Backup Windows system registry
- ○ Backup Active Directory
- ○ Backup passwords and sensitive information
- ○ Memory dumps and hibernation files
- ○ Windows search database

Source drive (where Windows directory resides): C:\

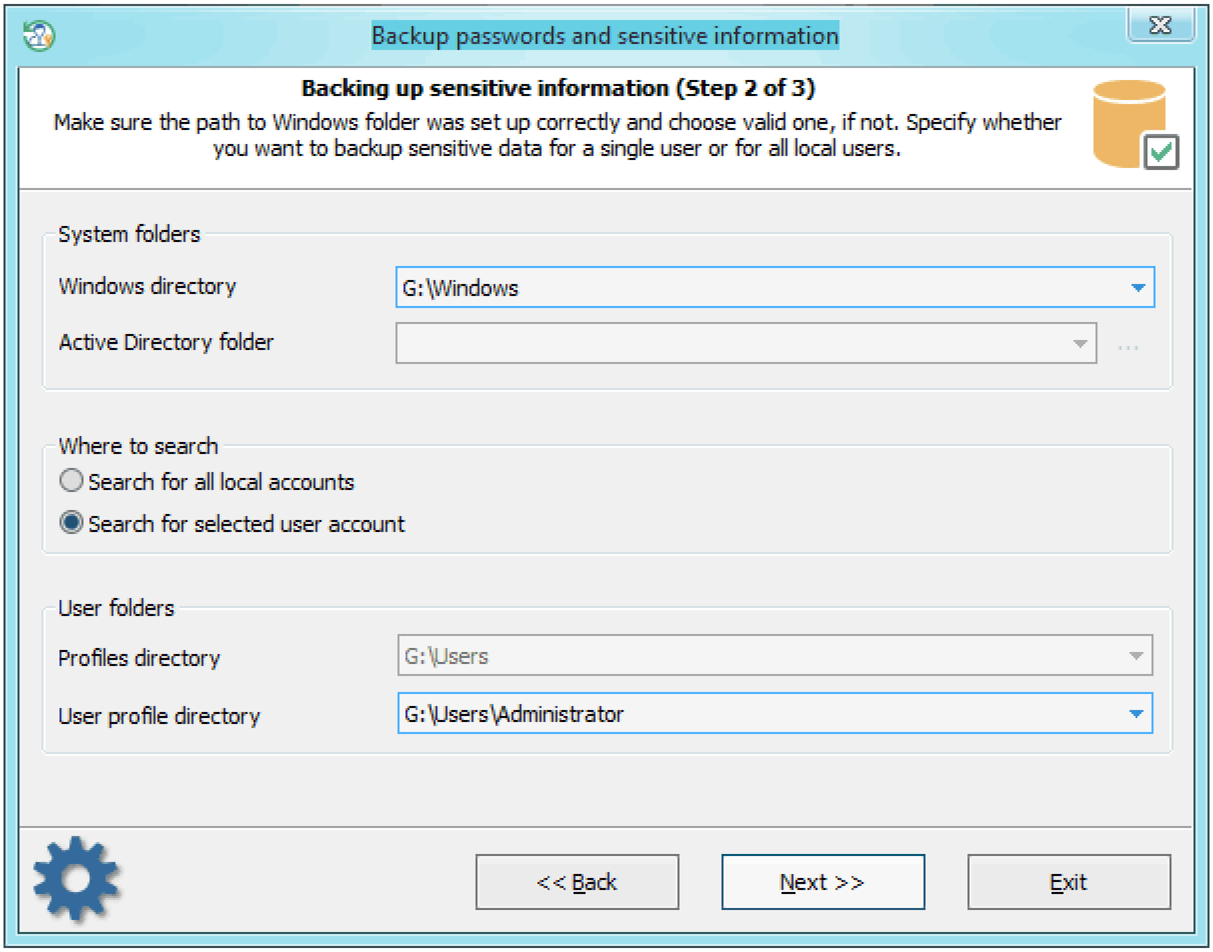
Target directory (to save the files to): E:\

First, we need to set up what to backup:

- Windows registry files
- Active Directory database
- All sensitive information including user registry, passwords, certificates, encryption keys, system and user activity data, forensic artifacts, etc.
- Found memory dumps and hibernation files
- Windows search database

You will have to set a source drive where the target Windows directory resides and a target path. The target path will be used to save the output archived files. By default, the program suggests first hard drive as the source and first removable drive as the target.

Setting Windows directory and user account



Backup passwords and sensitive information

Backing up sensitive information (Step 2 of 3)

Make sure the path to Windows folder was set up correctly and choose valid one, if not. Specify whether you want to backup sensitive data for a single user or for all local users.

System folders

Windows directory: G:\Windows

Active Directory folder:

Where to search

○ Search for all local accounts

● Search for selected user account

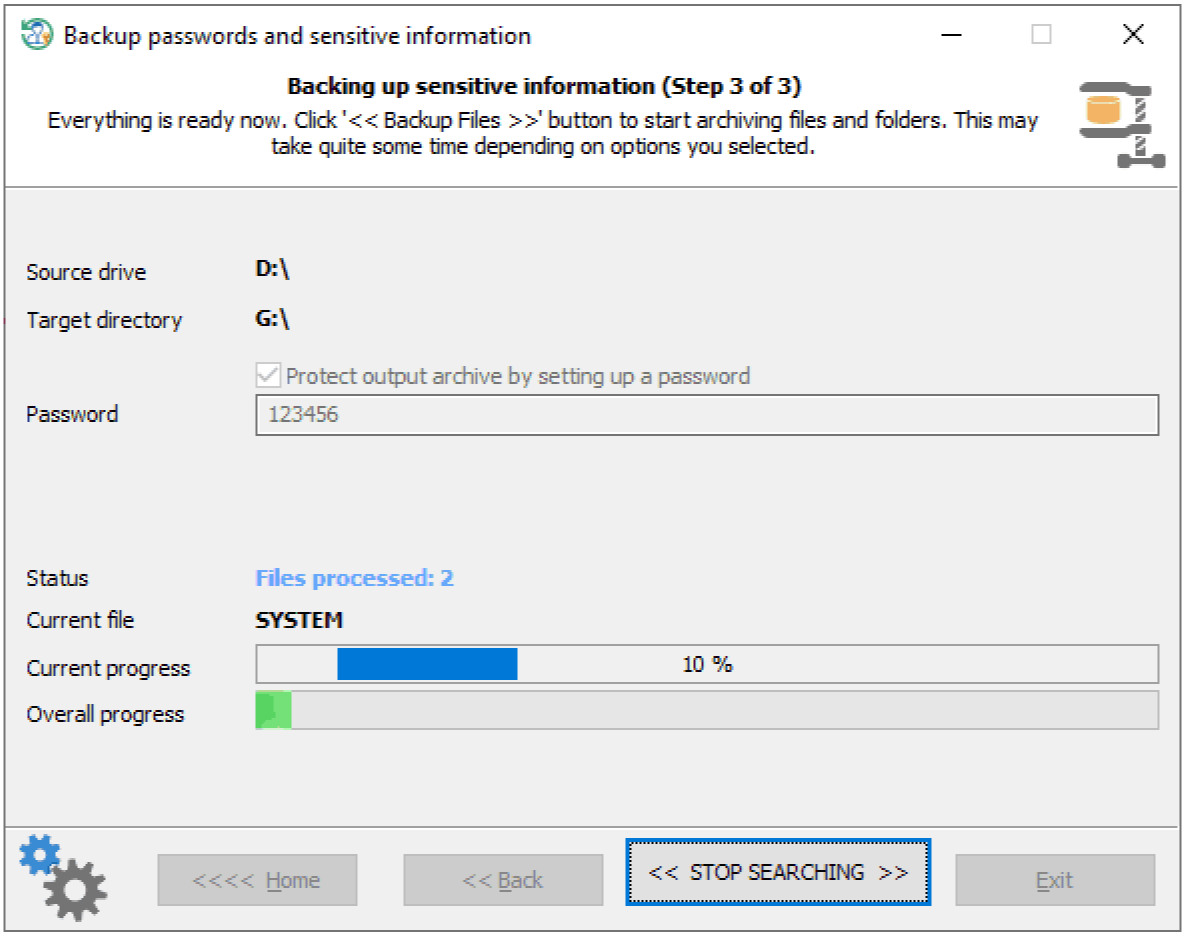
User folders

Profiles directory: G:\Users

User profile directory: G:\Users\Administrator

Next step is a bit simpler. In case you selected Registry/Active Directory backup on the previous step, all you need here is to confirm Windows/AD folders. Otherwise, you'll additionally have to select either profiles directory or profile directory for selected user, depending on options you choose.

Locating and backing up the found data



Backup passwords and sensitive information

Backing up sensitive information (Step 3 of 3)

Everything is ready now. Click '<< Backup Files >>' button to start archiving files and folders. This may take quite some time depending on options you selected.

Source drive **D:\**

Target directory **G:\**

☑ Protect output archive by setting up a password

Password 123456

Status **Files processed: 2**

Current file **SYSTEM**

Current progress 10 %

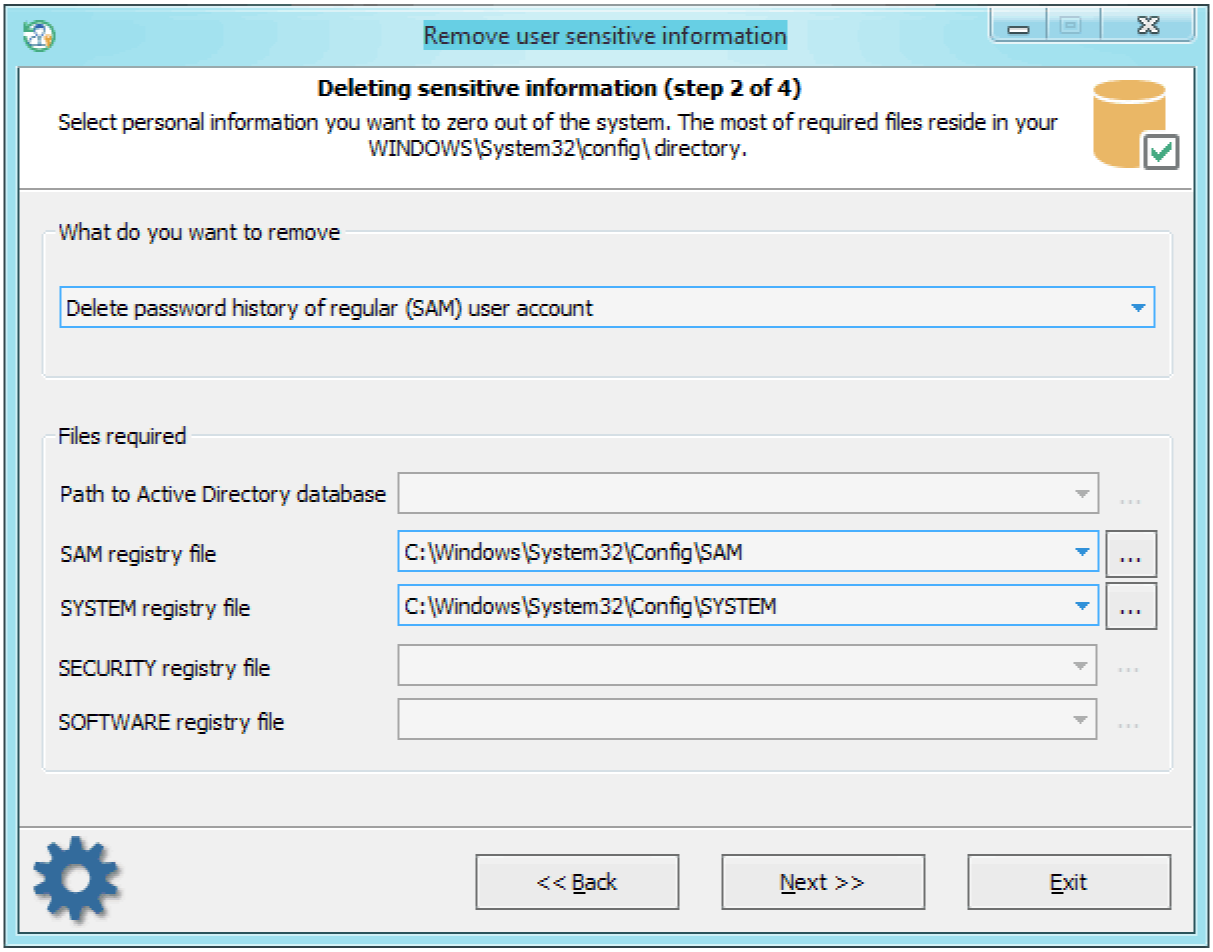
Overall progress

And the final dialog is just a progress for the backup operation. Click **<< Back up files >>** button to start the process. By successful completion, you should get a *.ZIP archive which holds all found files. To protect your private data against unauthorized access, you are free to set a password for the output ZIP archive.

Later you can use the found files to further security analysis, password recovery, and audit in any 3d-party software. For example, using our Windows Password Recovery tool.

3.9.3 Removing user's private information

Selecting data to be removed



Remove user sensitive information

Deleting sensitive information (step 2 of 4)

Select personal information you want to zero out of the system. The most of required files reside in your WINDOWS\System32\config\ directory.

What do you want to remove

Delete password history of regular (SAM) user account

Files required

Path to Active Directory database:

SAM registry file: C:\Windows\System32\Config\SAM

SYSTEM registry file: C:\Windows\System32\Config\SYSTEM

SECURITY registry file:

SOFTWARE registry file:

The application has a number of advanced features. One of them is deleting information that can be used by potential malefactors for recovering account passwords on your computer. Be careful; the information will be removed permanently with no chances for recovery. So, it includes the following items:

1. Deleting password history for standard SAM accounts and Active Directory user accounts. SAM password history, for example, is set in the groups policy of the local computer. Start -> Run -> gpedit.msc -> click OK. Under Computer Configuration, drill down under Windows Settings -> Security Settings -> Local Policies -> Security Options. Here look for policy: *Interactive Logon: Number of previous logons to cache*.
2. Deleting domain cached passwords. More on domain cached passwords can be read here.
3. Deleting cached Windows logon password.
4. Deleting password reset diskette information. With that information and the password reset disk, one can recover the original textual password.
5. Deleting password hints.
6. Resetting Syskey

To continue with the application, provide (or select from available) the following files:
- Deletion of AD password history – **SYSTEM** registry file and Active Directory database file (**ntds.dit**)
- Deletion of SAM password history – **SAM** and **SYSTEM** registry files
- Deletion of cached domain passwords – files **SECURITY** and **SYSTEM**
- Deletion of cached logon passwords – files **SECURITY**, **SOFTWARE** and **SYSTEM**
- Deletion of password reset information - files **SAM**, **SECURITY** and **SYSTEM**
- Deletion of password hints - **SAM**, **SOFTWARE** and **SYSTEM**

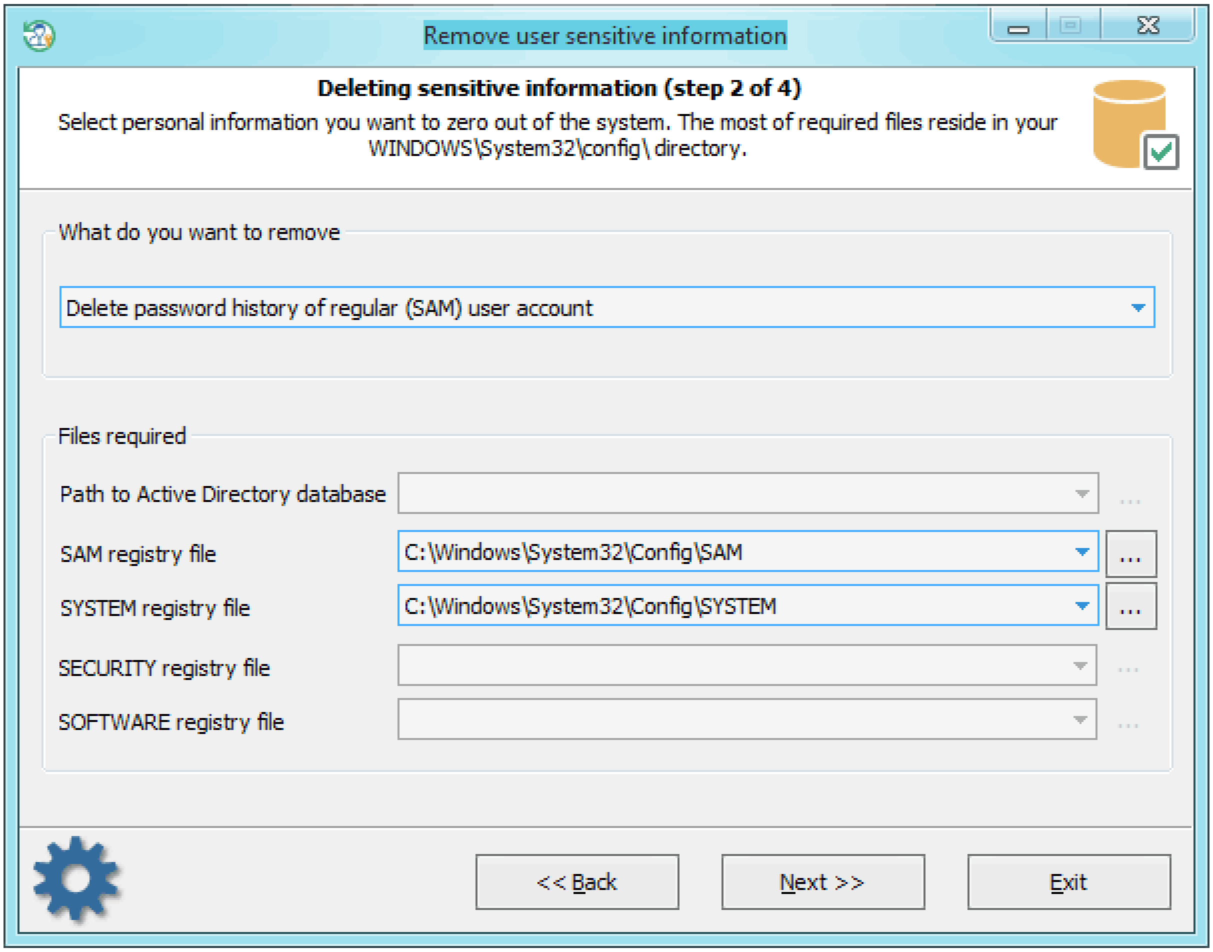
- Resetting SYSKEY - **SAM**, **SECURITY** and **SYSTEM**

All registry files, except Active Directory database, are stored in the following directory **%WINDIR%\system32\config**. Where %WINDIR% stands for the Windows folder, by default - C:\Windows.

The location of the AD database is set during installation. By default, that's the **%WINDIR%\NTDS** folder.

3.9.3.1 Removing password history of SAM or Active Directory users

Selecting data source



Remove user sensitive information

Deleting sensitive information (step 2 of 4)

Select personal information you want to zero out of the system. The most of required files reside in your WINDOWS\System32\config\ directory.

What do you want to remove

Delete password history of regular (SAM) user account

Files required

Path to Active Directory database:

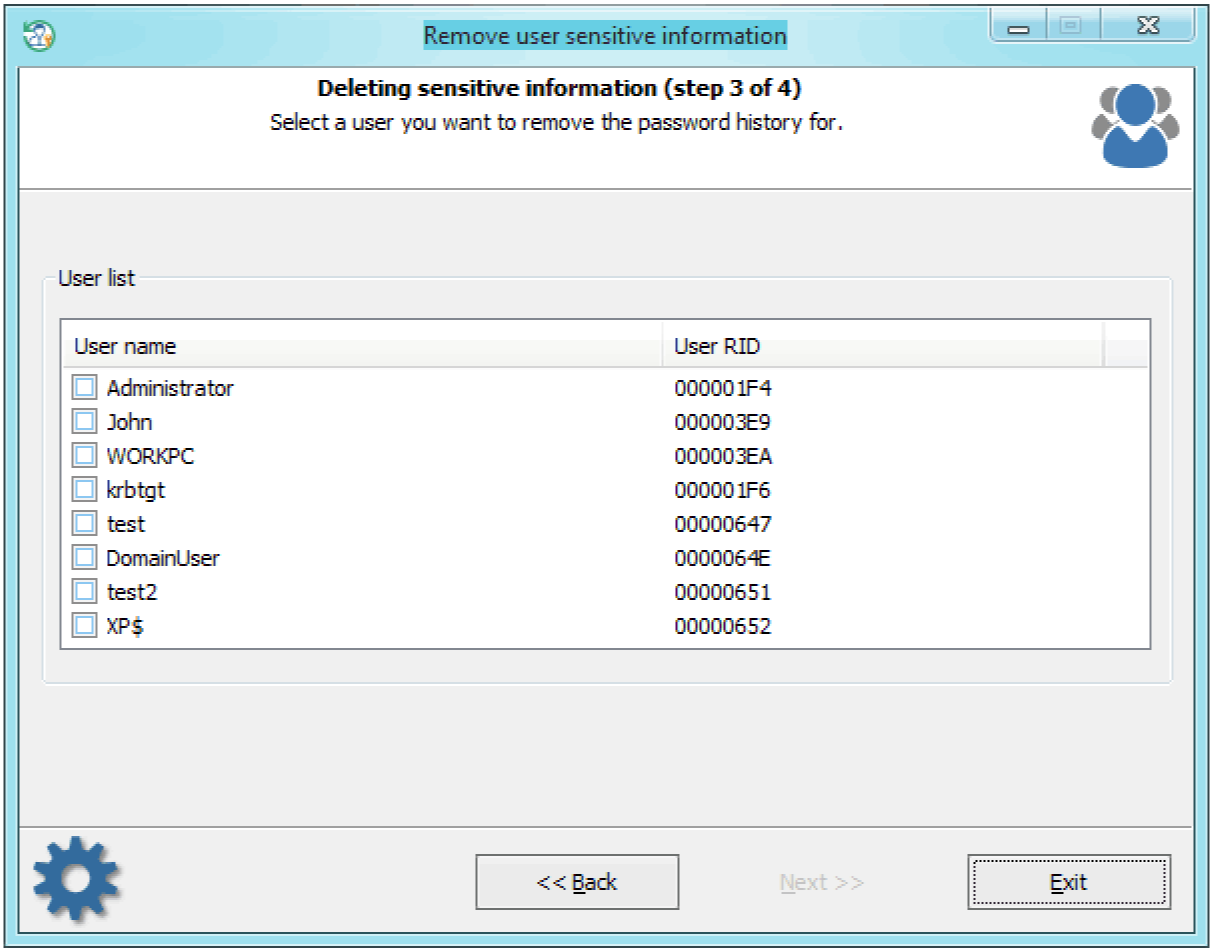
SAM registry file: C:\Windows\System32\Config\SAM

SYSTEM registry file: C:\Windows\System32\Config\SYSTEM

SECURITY registry file:

SOFTWARE registry file:

Selecting user account



Deleting sensitive information (step 3 of 4)

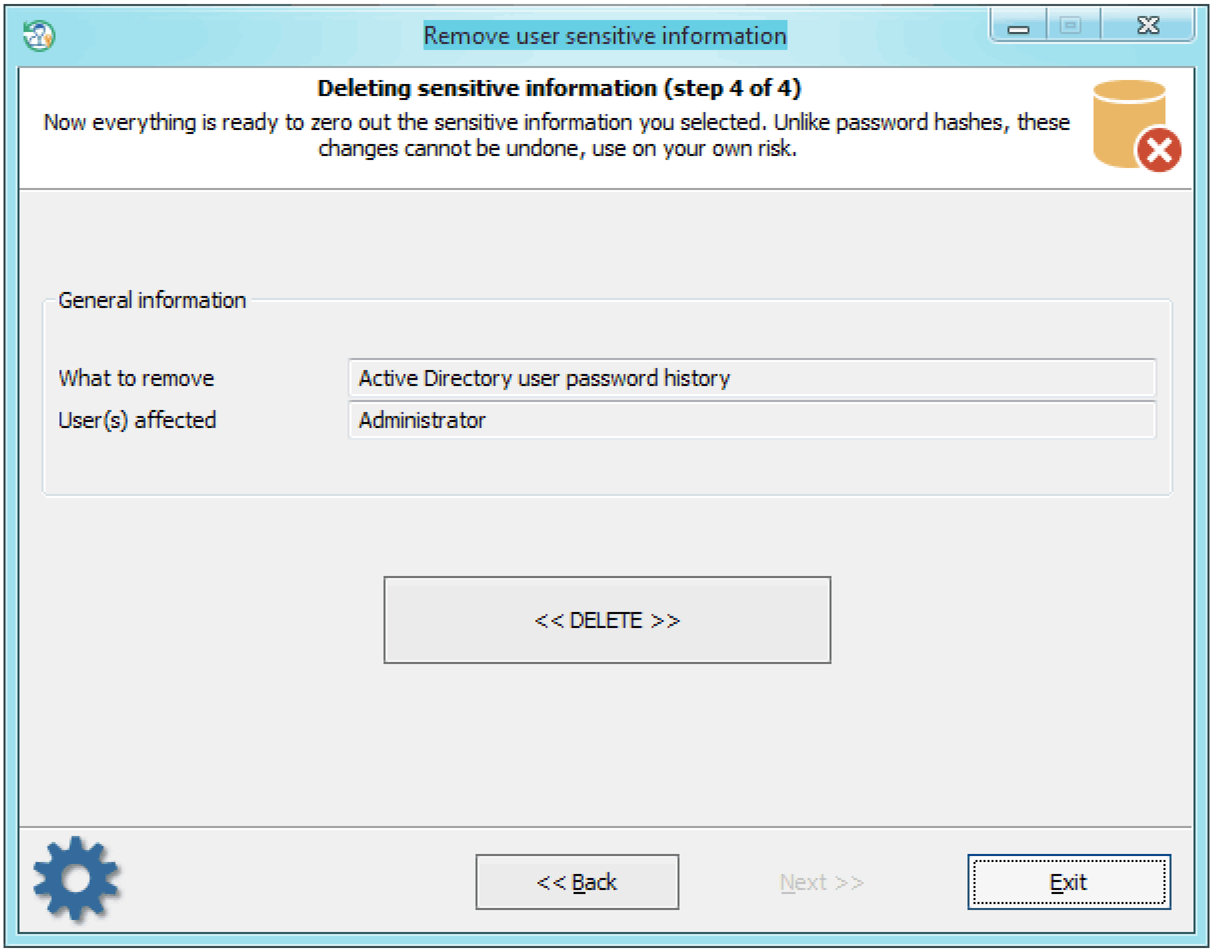
Select a user you want to remove the password history for.

User list

User name	User RID
□ Administrator	000001F4
□ John	000003E9
□ WORKPC	000003EA
□ krbtgt	000001F6
□ test	00000647
□ DomainUser	0000064E
□ test2	00000651
□ XP$	00000652

On the account list, select the one we need to delete password history for. The application displays only users that have history.

Deleting password history



Remove user sensitive information

Deleting sensitive information (step 4 of 4)

Now everything is ready to zero out the sensitive information you selected. Unlike password hashes, these changes cannot be undone, use on your own risk.

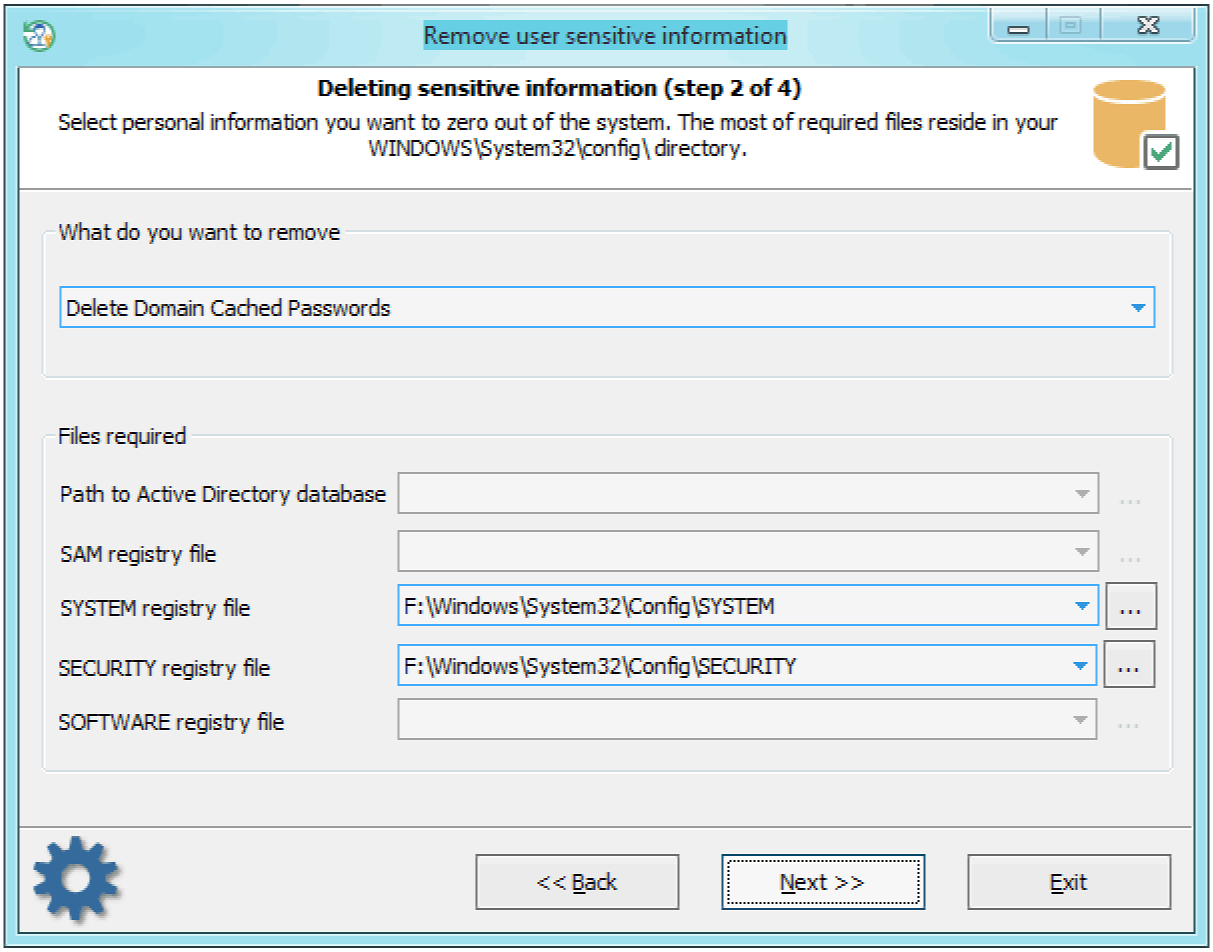
General information

What to remove	Active Directory user password history
User(s) affected	Administrator

Click <<Delete>> and get rid of the unnecessary information permanently.

3.9.3.2 Removing domain cached passwords

Selecting data source



Remove user sensitive information

Deleting sensitive information (step 2 of 4)

Select personal information you want to zero out of the system. The most of required files reside in your WINDOWS\System32\config\ directory.

What do you want to remove: Delete Domain Cached Passwords

Files required

Path to Active Directory database:

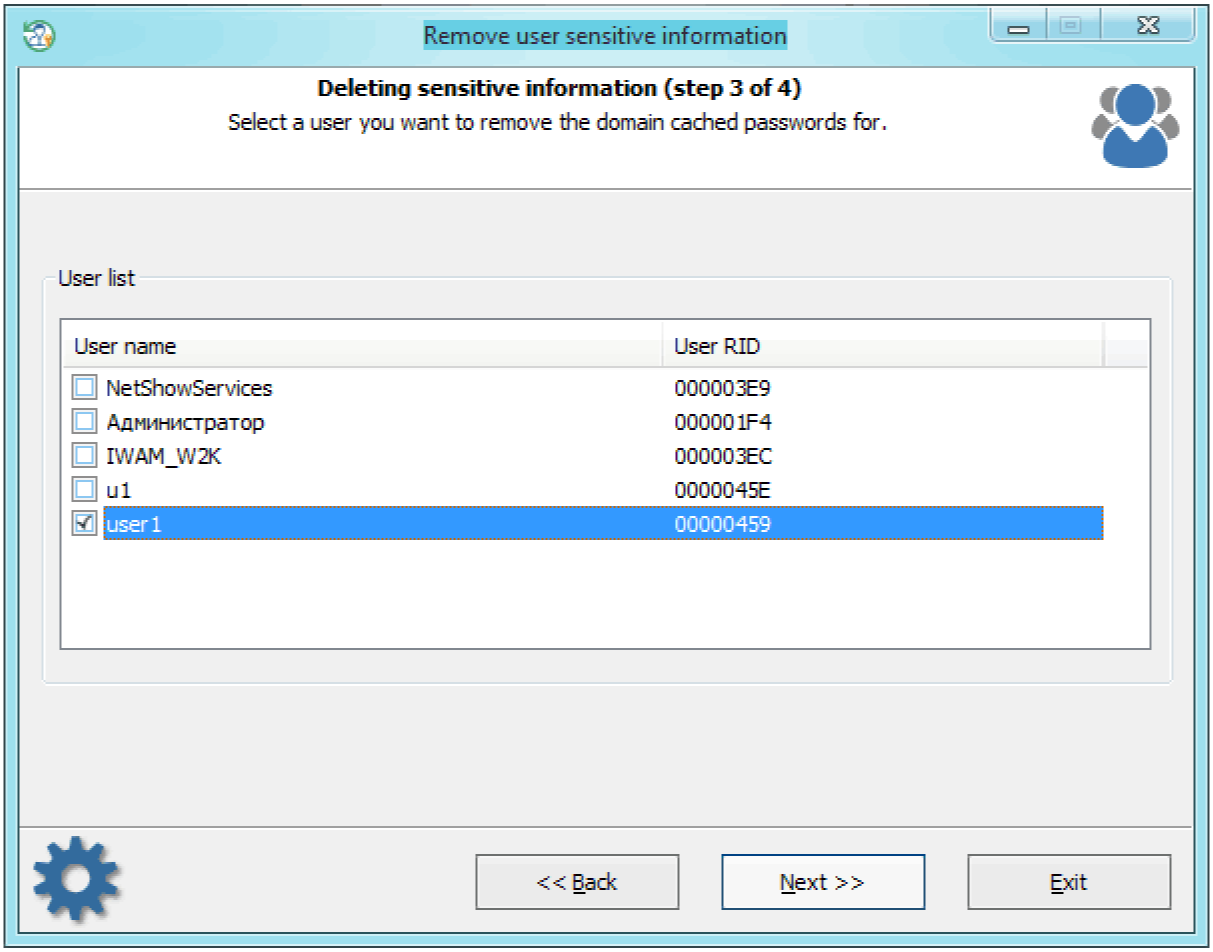
SAM registry file:

SYSTEM registry file: F:\Windows\System32\Config\SYSTEM

SECURITY registry file: F:\Windows\System32\Config\SECURITY

SOFTWARE registry file:

[Selecting user account]



Deleting sensitive information (step 3 of 4)

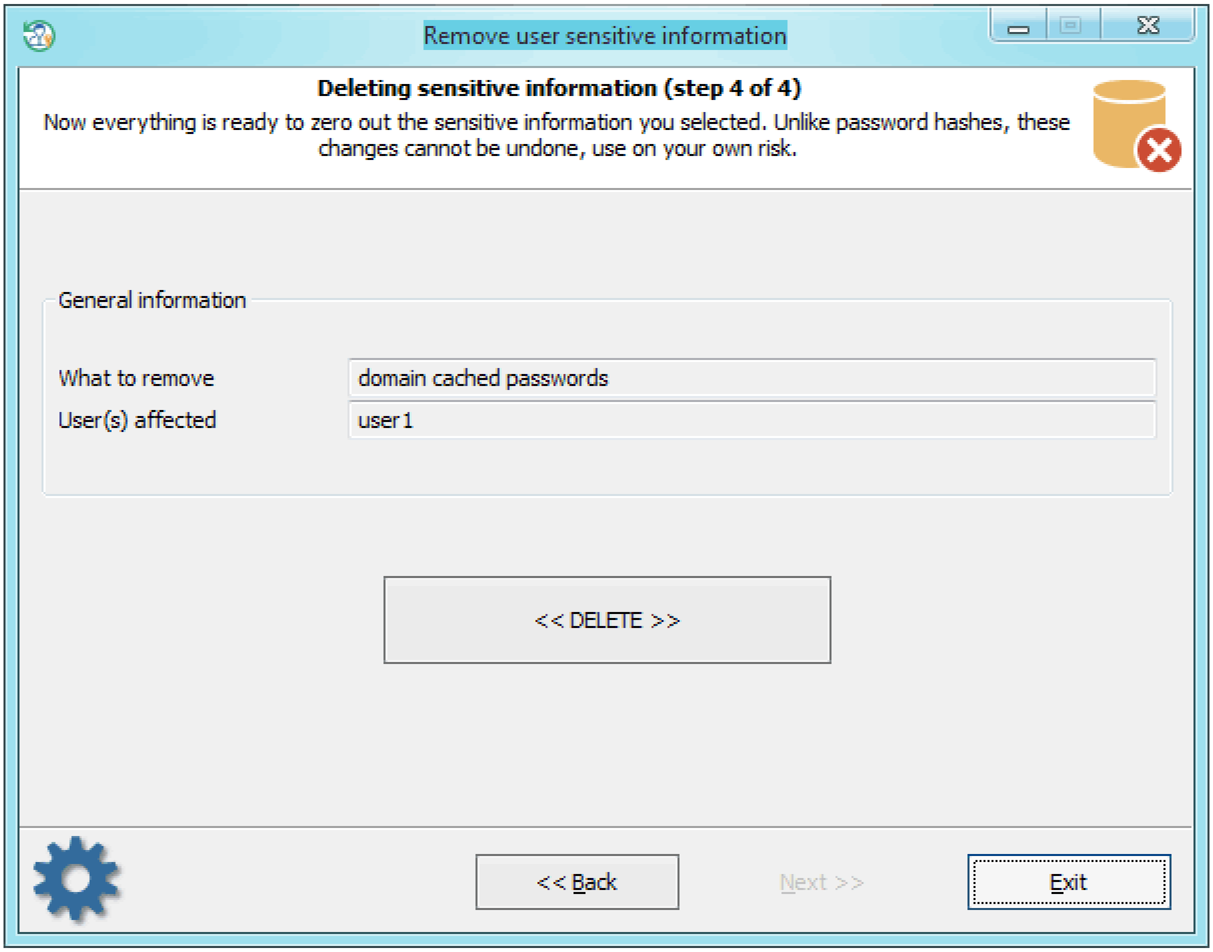
Select a user you want to remove the domain cached passwords for.

User list

	User name	User RID
□	NetShowServices	000003E9
□	Администратор	000001F4
□	IWAM_W2K	000003EC
□	u1	0000045E
☑	user1	00000459

Choosing the account you want to remove the passwords for.

Deleting domain cached passwords



Remove user sensitive information

Deleting sensitive information (step 4 of 4)

Now everything is ready to zero out the sensitive information you selected. Unlike password hashes, these changes cannot be undone, use on your own risk.

General information

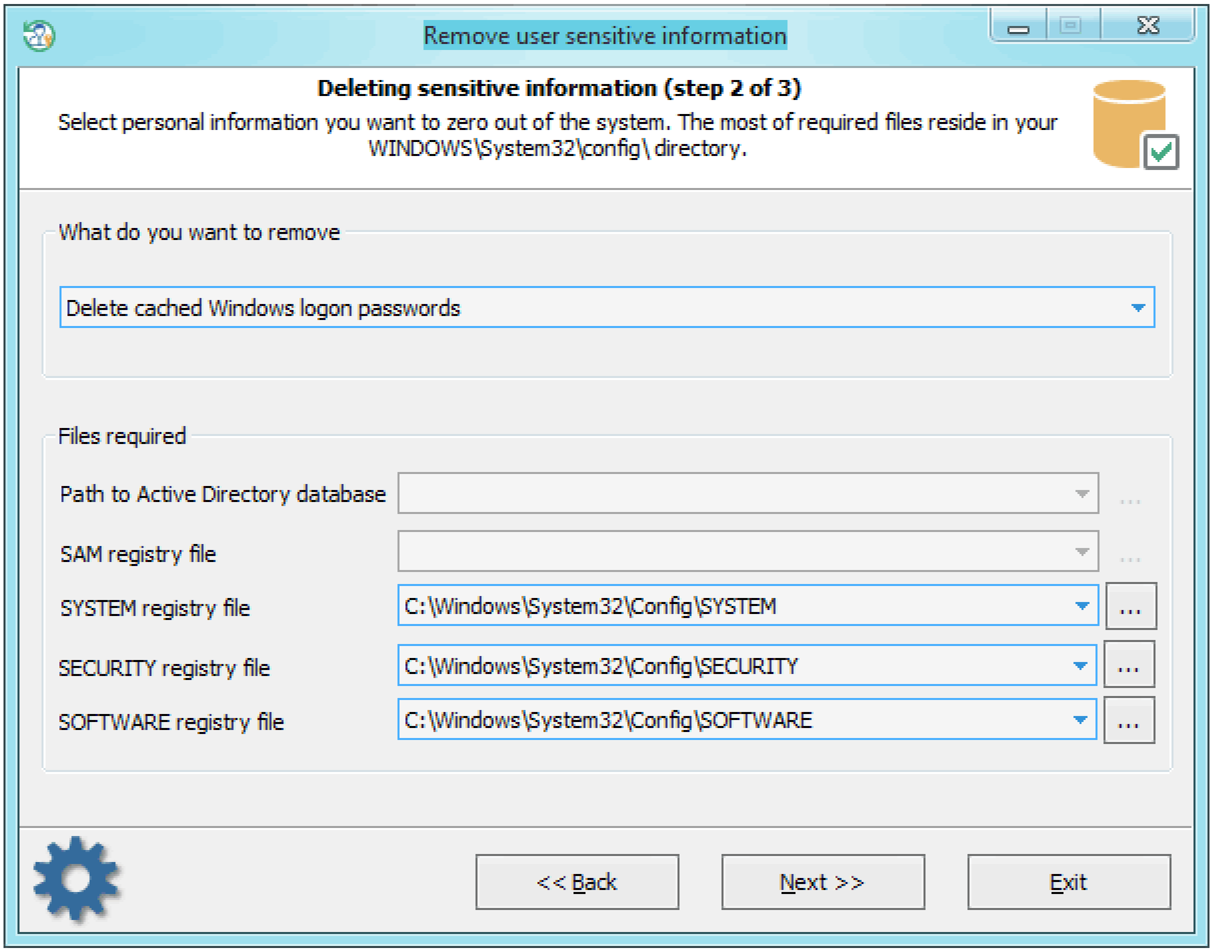
What to remove: domain cached passwords

User(s) affected: user1

Just confirm deleting all domain cached passwords for user1 account.

3.9.3.3 Removing cached logon password

Selecting data source



Remove user sensitive information

Deleting sensitive information (step 2 of 3)

Select personal information you want to zero out of the system. The most of required files reside in your WINDOWS\System32\config\ directory.

What do you want to remove

Delete cached Windows logon passwords

Files required

Path to Active Directory database

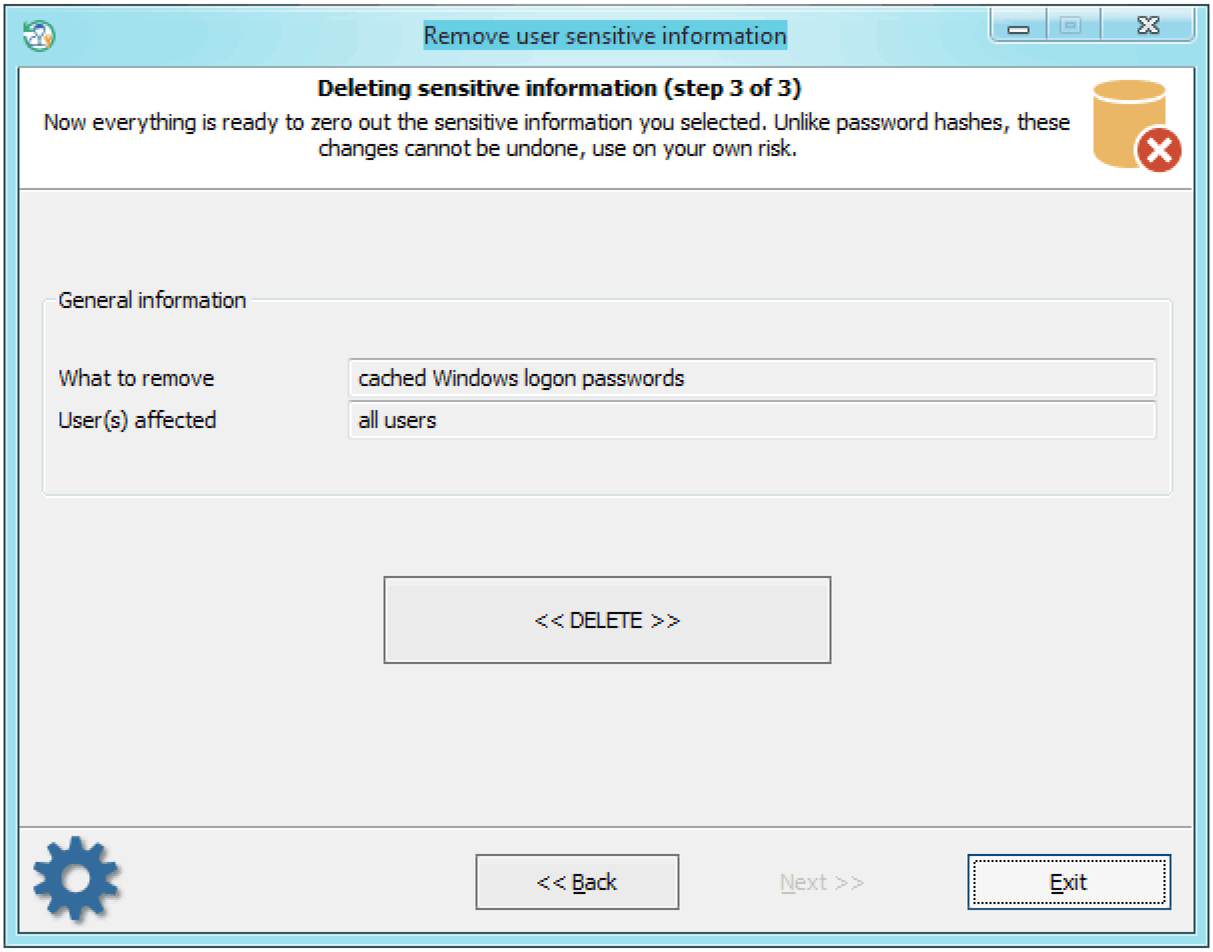
SAM registry file

SYSTEM registry file: C:\Windows\System32\Config\SYSTEM

SECURITY registry file: C:\Windows\System32\Config\SECURITY

SOFTWARE registry file: C:\Windows\System32\Config\SOFTWARE

Deleting Windows cached logon password



Remove user sensitive information

Deleting sensitive information (step 3 of 3)

Now everything is ready to zero out the sensitive information you selected. Unlike password hashes, these changes cannot be undone, use on your own risk.

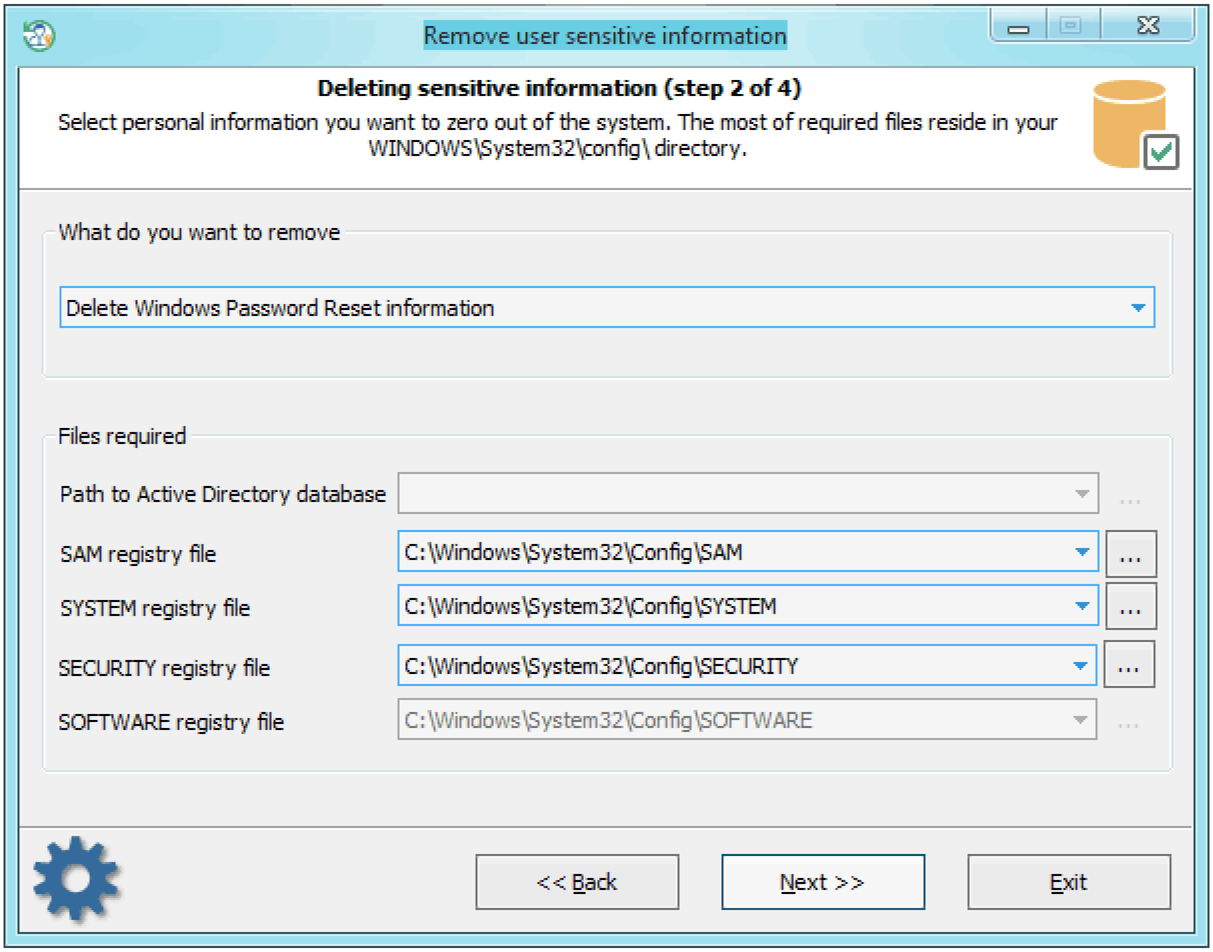
General information

What to remove	cached Windows logon passwords
User(s) affected	all users

And confirm the permanent removal of cached logon passwords.

3.9.3.4 Removing password reset disk information

Selecting data source



Remove user sensitive information

Deleting sensitive information (step 2 of 4)

Select personal information you want to zero out of the system. The most of required files reside in your WINDOWS\System32\config\ directory.

What do you want to remove

Delete Windows Password Reset information

Files required

Path to Active Directory database

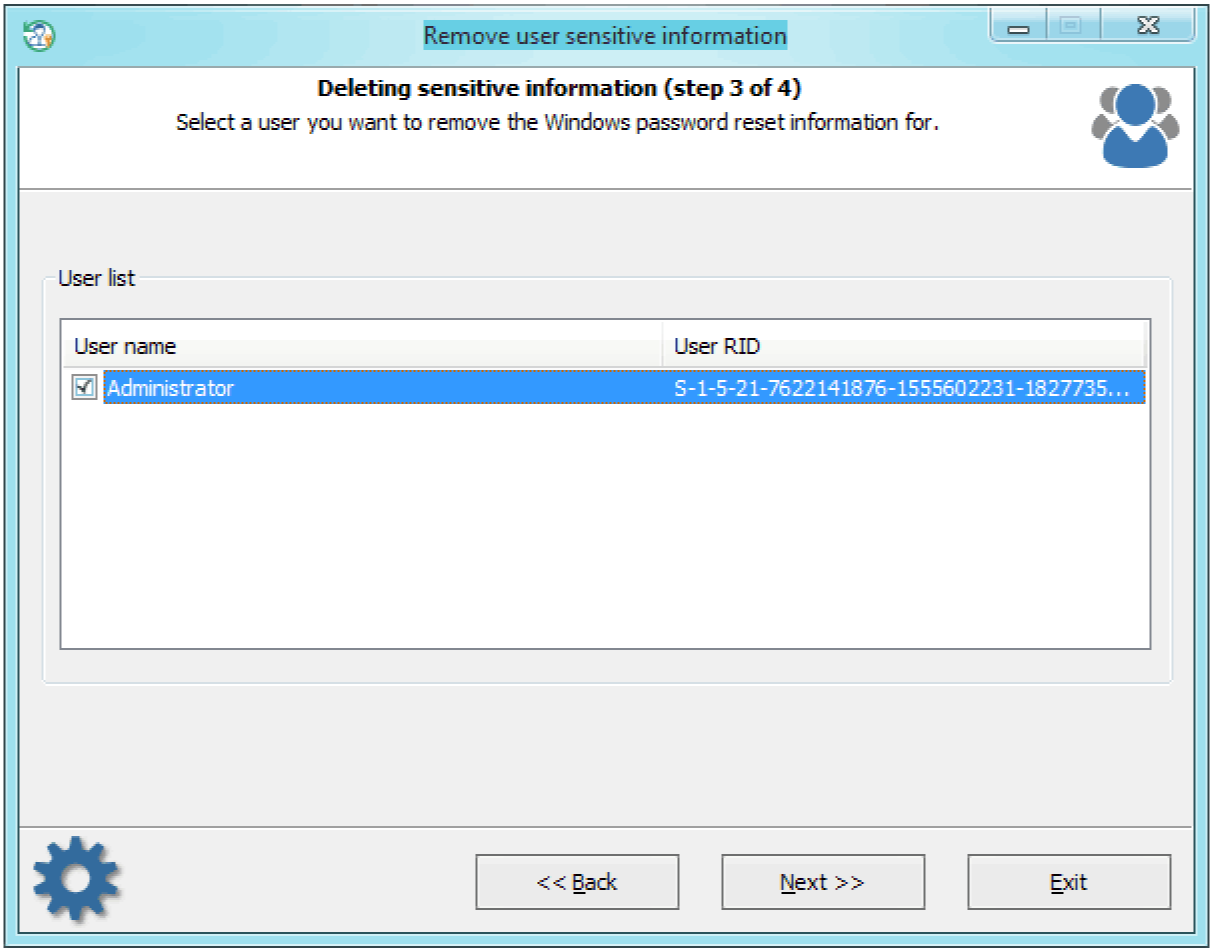
SAM registry file: C:\Windows\System32\Config\SAM

SYSTEM registry file: C:\Windows\System32\Config\SYSTEM

SECURITY registry file: C:\Windows\System32\Config\SECURITY

SOFTWARE registry file: C:\Windows\System32\Config\SOFTWARE

Selecting user account



Remove user sensitive information

Deleting sensitive information (step 3 of 4)

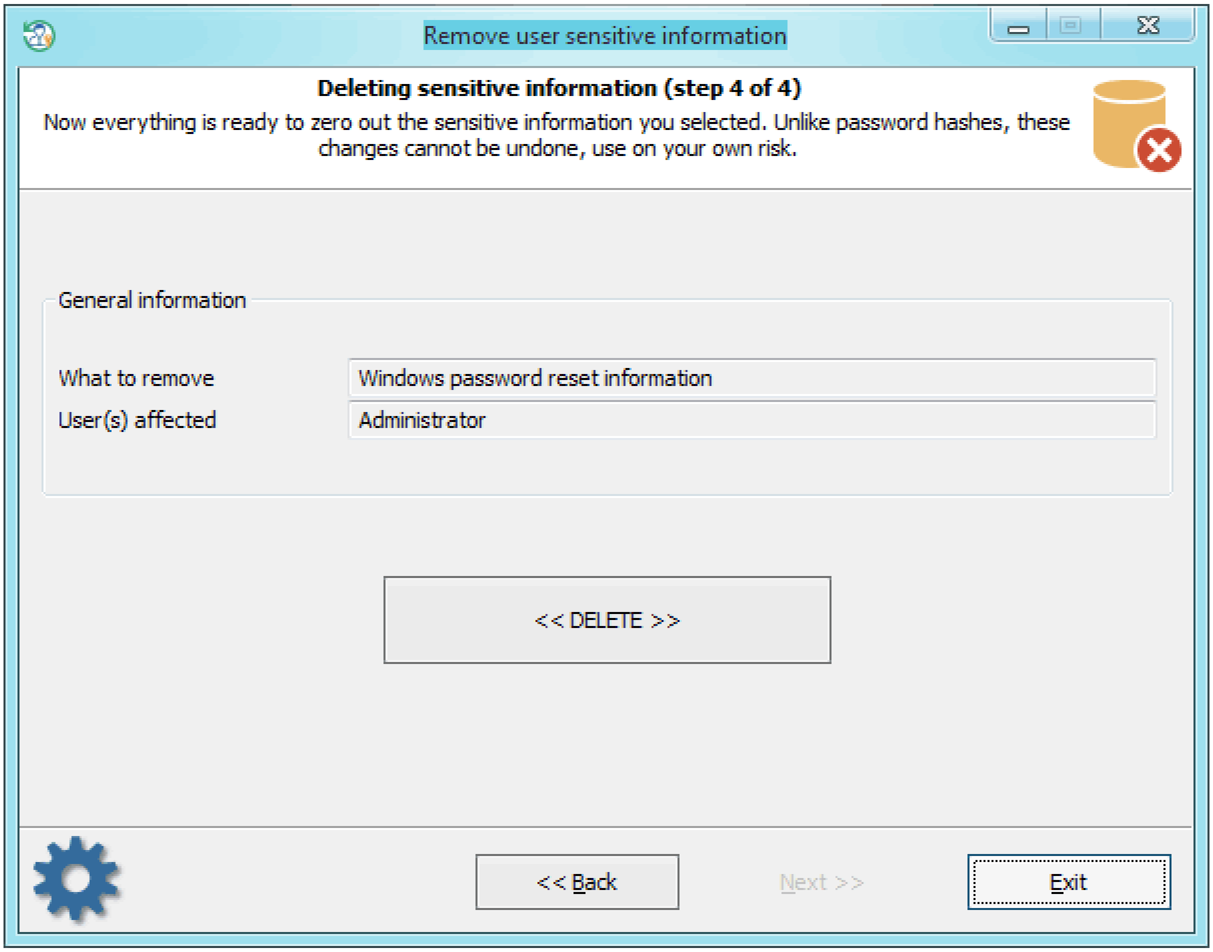
Select a user you want to remove the Windows password reset information for.

User list

User name	User RID
☑ Administrator	S-1-5-21-7622141876-1555602231-1827735...

Check the user whose information we want to delete. When creating a password reset disk, the user's encrypted password is stored in the registry. While the diskette stores the encryption key. Deleting the encrypted password from the registry makes the further existence of the reset password diskette useless.

[Deleting password reset diskette information]



Remove user sensitive information

Deleting sensitive information (step 4 of 4)

Now everything is ready to zero out the sensitive information you selected. Unlike password hashes, these changes cannot be undone, use on your own risk.

General information

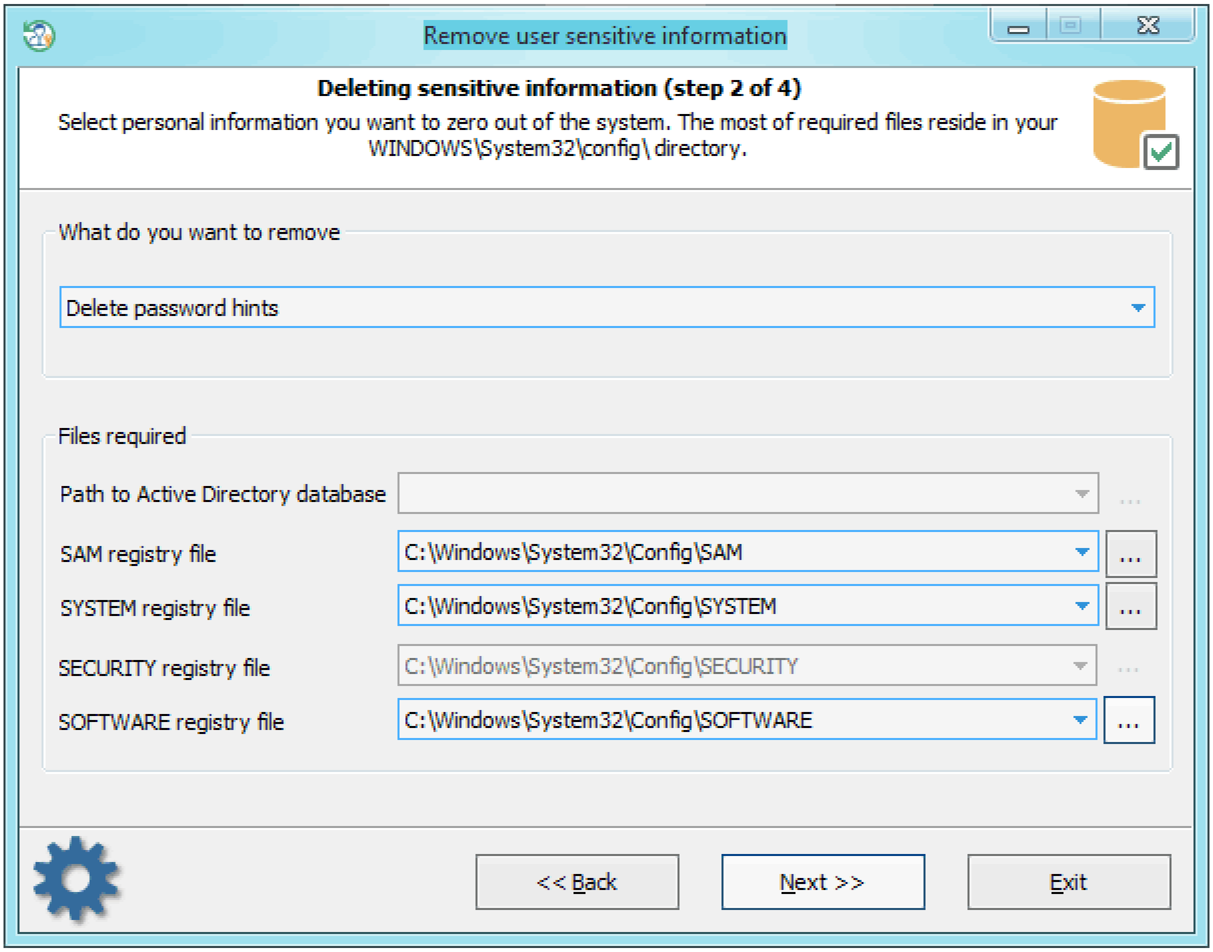
What to remove: Windows password reset information

User(s) affected: Administrator

Confirm deletion.

3.9.3.5 Removing password hints

Selecting data source



Remove user sensitive information

Deleting sensitive information (step 2 of 4)

Select personal information you want to zero out of the system. The most of required files reside in your WINDOWS\System32\config\ directory.

What do you want to remove

Delete password hints

Files required

Path to Active Directory database:

SAM registry file: C:\Windows\System32\Config\SAM

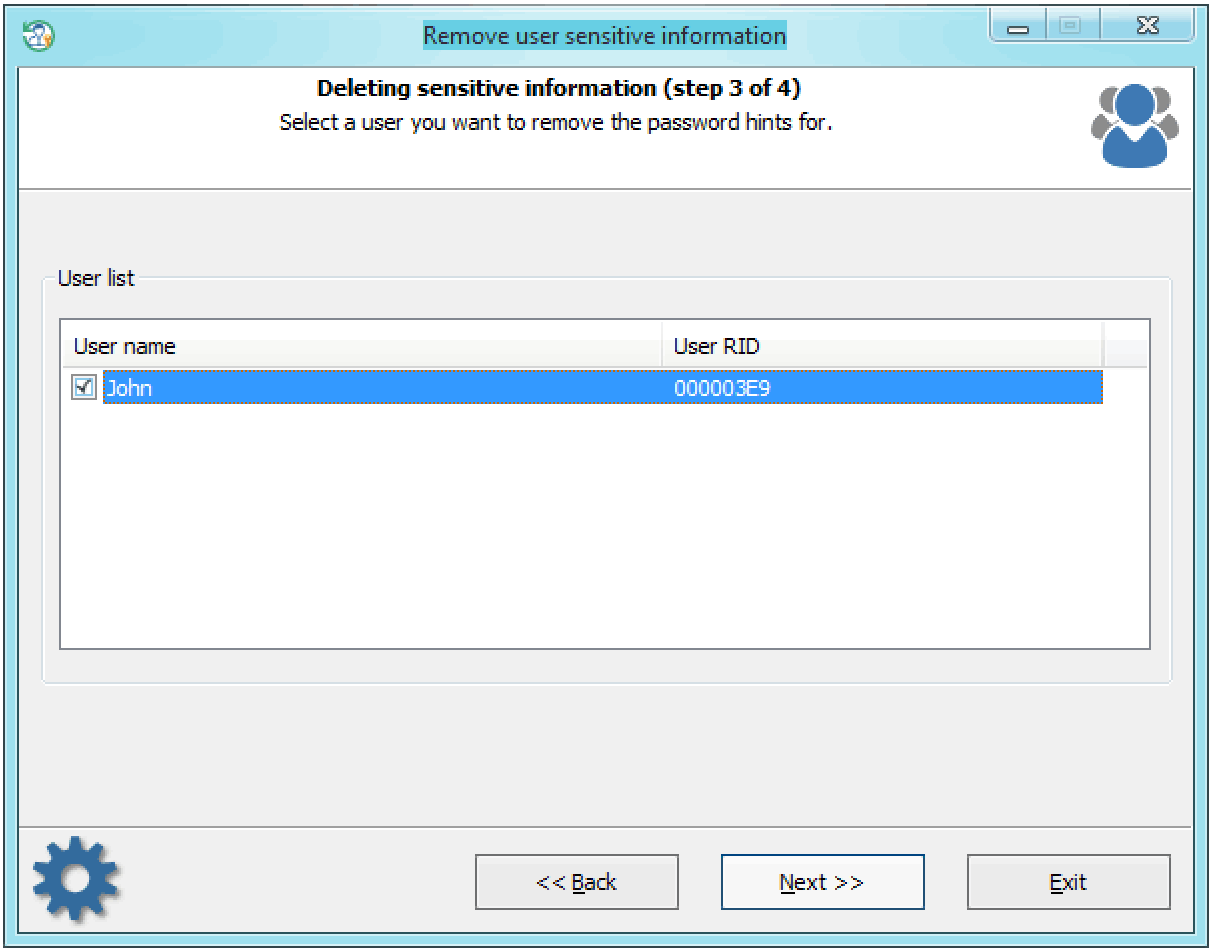
SYSTEM registry file: C:\Windows\System32\Config\SYSTEM

SECURITY registry file: C:\Windows\System32\Config\SECURITY

SOFTWARE registry file: C:\Windows\System32\Config\SOFTWARE

Password hints are stored either in the SOFTWARE registry (Windows XP, Windows 2003) or in the SAM file (Windows Vista and higher OS). The decryption will also require the SYSTEM file.

[Selecting user account](#)



Remove user sensitive information

Deleting sensitive information (step 3 of 4)

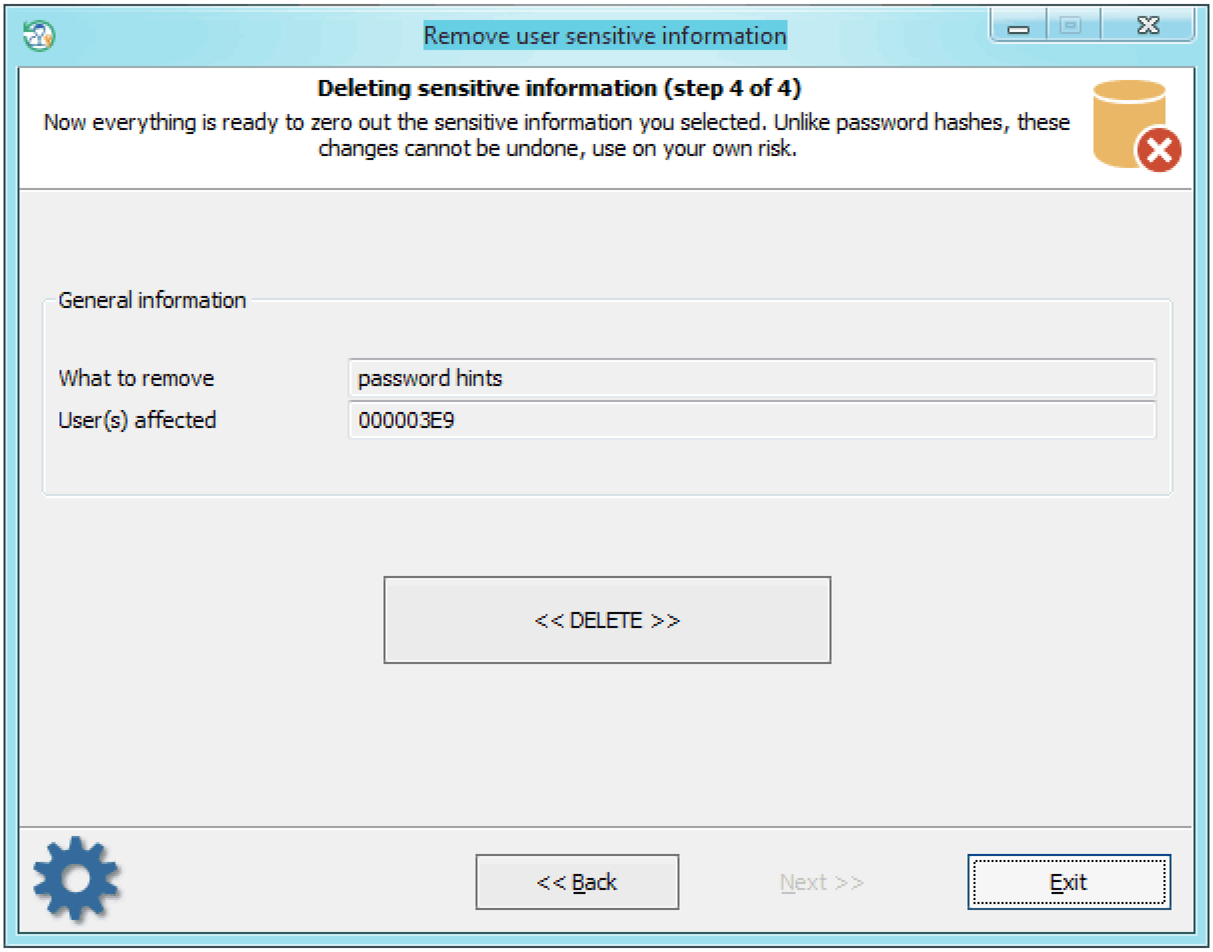
Select a user you want to remove the password hints for.

User list

User name	User RID
☑ John	000003E9

Select the user whose hint is to be cleared from the system and then follow the final removal dialog.

Removing hints



Remove user sensitive information

Deleting sensitive information (step 4 of 4)

Now everything is ready to zero out the sensitive information you selected. Unlike password hashes, these changes cannot be undone, use on your own risk.

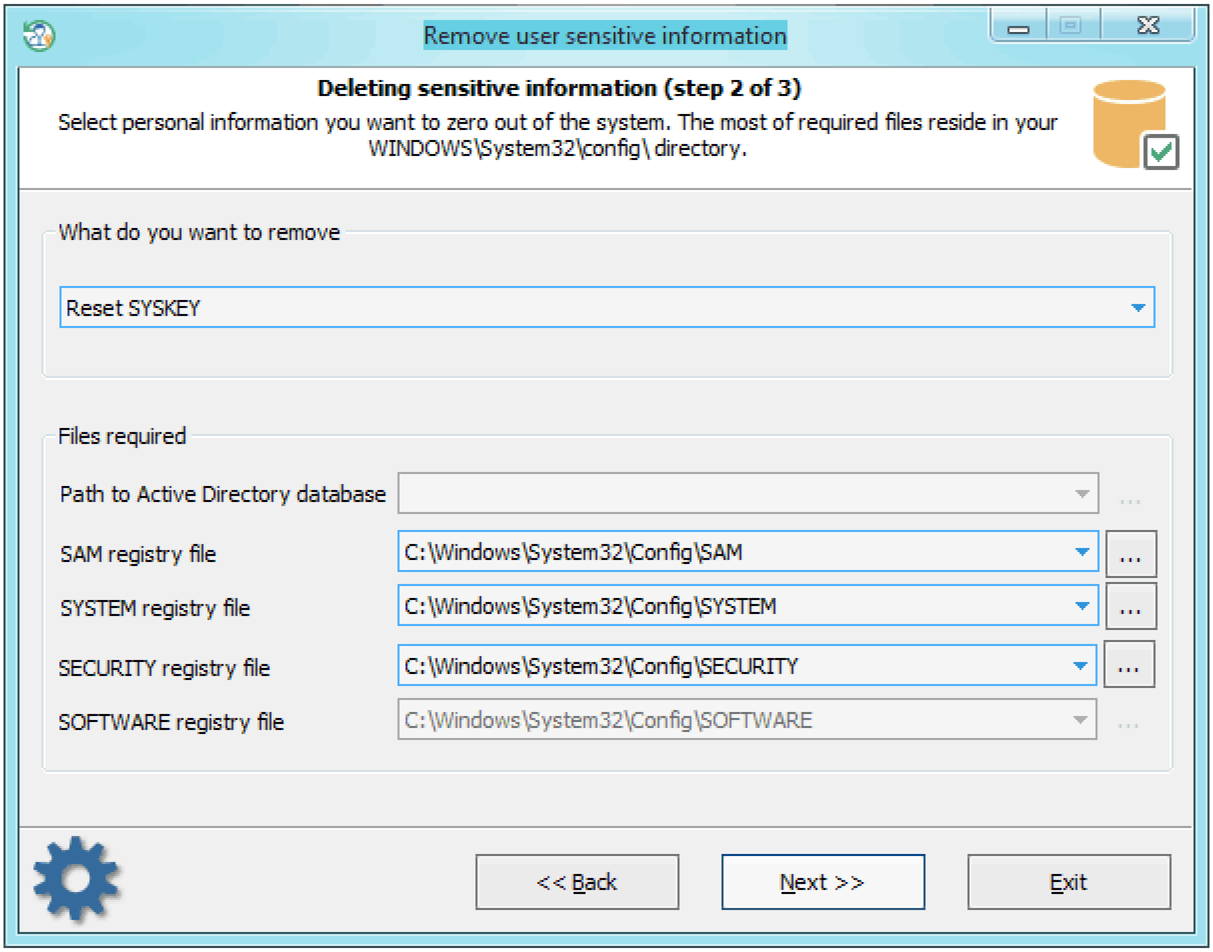
General information

What to remove: password hints

User(s) affected: 000003E9

3.9.3.6 Resetting SYSKEY

Selecting data source



Remove user sensitive information

Deleting sensitive information (step 2 of 3)

Select personal information you want to zero out of the system. The most of required files reside in your WINDOWS\System32\config\ directory.

What do you want to remove

Reset SYSKEY

Files required

Path to Active Directory database:

SAM registry file: C:\Windows\System32\Config\SAM

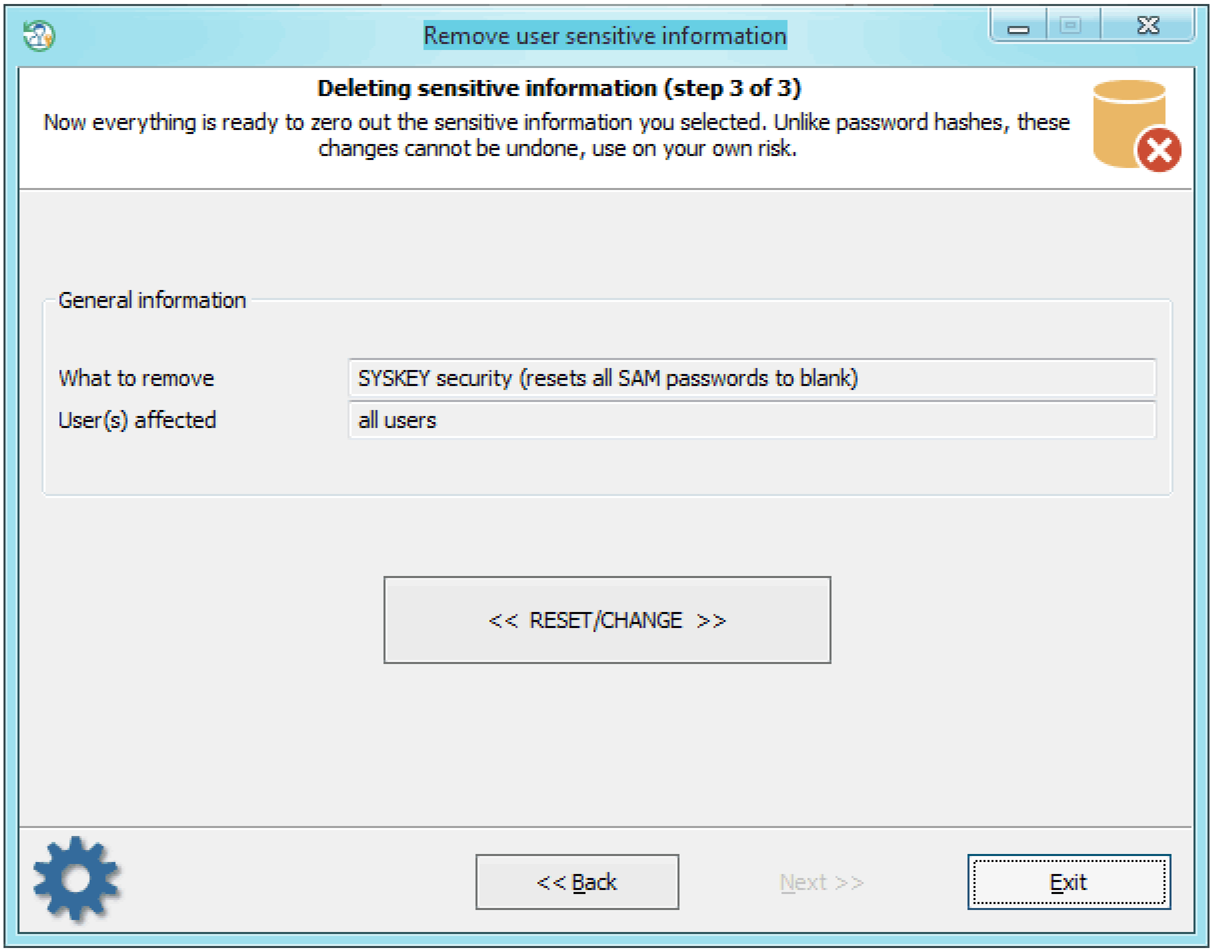
SYSTEM registry file: C:\Windows\System32\Config\SYSTEM

SECURITY registry file: C:\Windows\System32\Config\SECURITY

SOFTWARE registry file: C:\Windows\System32\Config\SOFTWARE

First you need to point to 3 registry hives: **SAM**, **SYSTEM** and **SECURITY**. Usually SYSKEY resides in your SYSTEM registry under **HKLM\CurrentControlSet\Control\Lsa** key. But once you set your SYSKEY for example to require a boot startup password and forgot it, there's no chance to boot up your system. Needless to say that SYSKEY is extremely effective tool in the hands of a guru. Setting your SYSKEY option to require a startup password or boot diskette is very effective against ANY(!) Windows password breaker. In that case a password extractor program can not decrypt your password hashes even if it get a full access to your system.

Resetting SYSKEY



Deleting sensitive information (step 3 of 3)

Now everything is ready to zero out the sensitive information you selected. Unlike password hashes, these changes cannot be undone, use on your own risk.

General information

What to remove	SYSKEY security (resets all SAM passwords to blank)
User(s) affected	all users

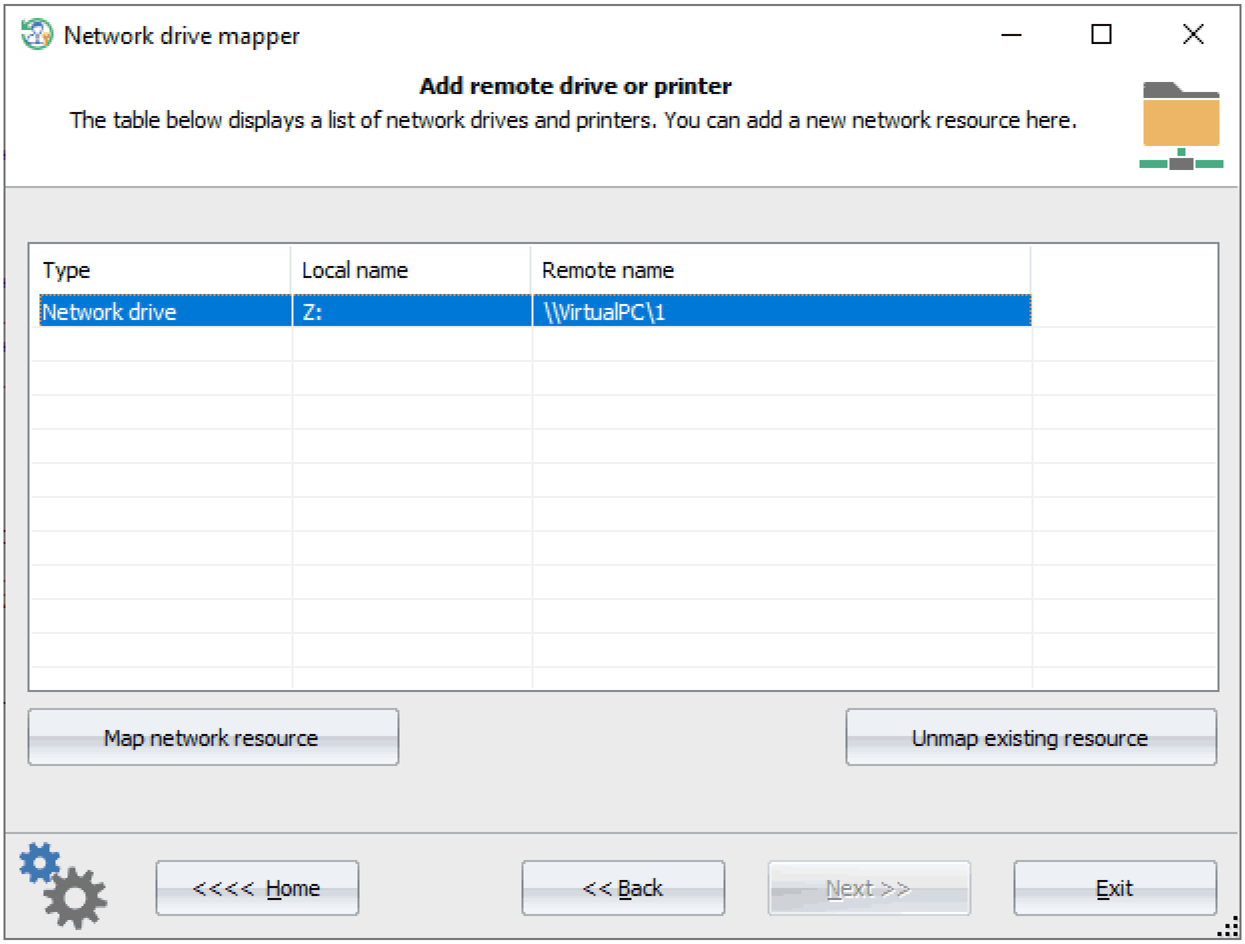
Note! SYSKEY resetting is an unsafe operation that affects the whole system security. For example after SYSKEY is reset, even if you can log on your system, you will not be able to decrypt your EFS protected files, all DPAPI-protected passwords (eg. Outlook saved passwords) will be discarded as well.

There are a number of programs in the Net that proclaim they can reset SYSKEY. But none of them works correctly at the moment. The reason is that SYSKEY resetting requires a lot of additional operations for your system to prevent it from being broken. For example you need also to zero out SAM domain session key(s), re-encrypt and reset local user hashes, LSA secrets, etc. **Reset Windows Password** has 2 algorithms for resetting SYSKEY. Once the primary one fails, another one runs. After SYSKEY is reset, all local user passwords will be set to blank automatically.

Note! After resetting SYSKEY on a Windows 8 and later OSes, you should change password for every LiveID/Microsoft account to a non-empty one. Otherwise you will not be able to log on the system with empty password.

3.9.4 Network drive mapper

This tool is designed to connect to remote resources of the local network. For example, to network drives or printers.



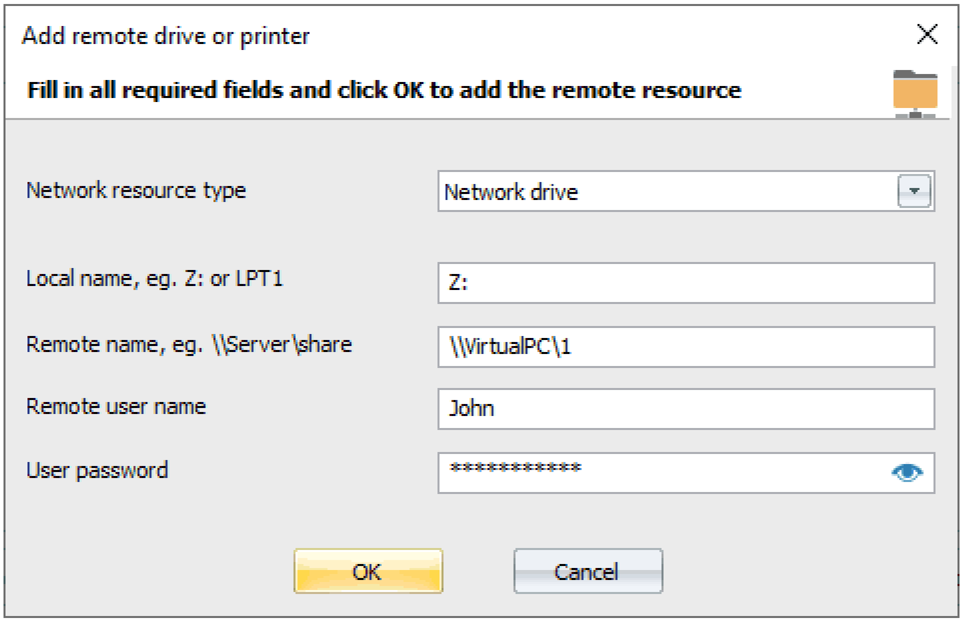
Add remote drive or printer

The table below displays a list of network drives and printers. You can add a new network resource here.

Type	Local name	Remote name
Network drive	Z:	\\VirtualPC\1

In order to create a new network drive, click the *'Map Network resource'* button. A network connection dialog should appear. Type in the name of the remote PC, including the shared resource (i.e. **\\SERVER\SHARE**), the name of the remote user, and his password.
where **SERVER** is a remote PC or its IP address
and **SHARE** is the shared resource

For example,
\\WIN-C2KSHD76D\forall
\\VPC\1
\\COMP2\C$



Add remote drive or printer

Fill in all required fields and click OK to add the remote resource

Network resource type: Network drive

Local name, eg. Z: or LPT1: Z:

Remote name, eg. \\Server\share: \\VirtualPC\1

Remote user name: John

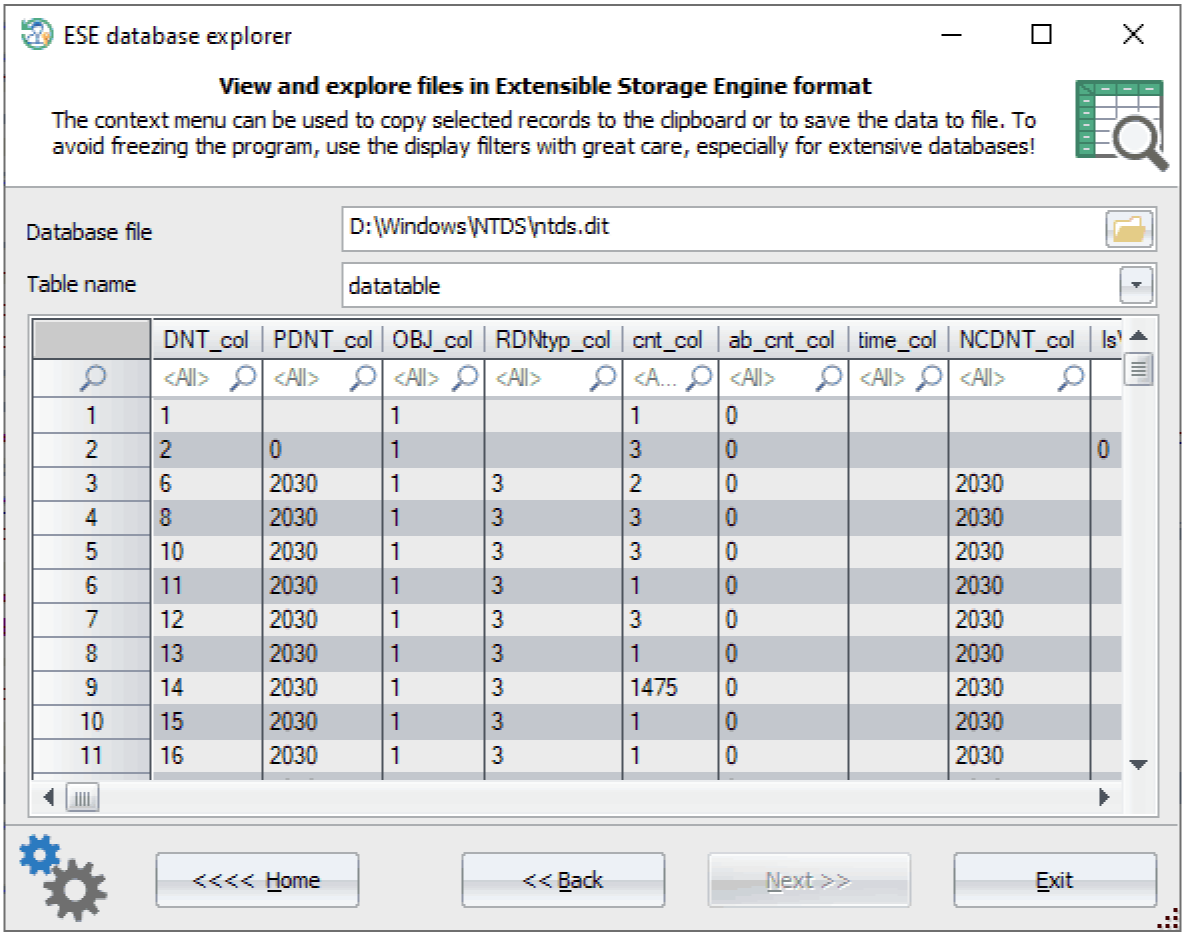
User password: ************

3.9.5 ESE database explorer

Extensible Storage Engine (formerly called as **Jet Blue** in some Microsoft docs) is a non-SQL storage engine developed by Microsoft. It perfectly handles a huge amount of data and is the core of Active Directory, Microsoft Exchange Server, Windows Search, Windows Update, System Resource Usage Monitor, Web cache, and other Windows components.

ESE has a long development story and its format was closed initially. That's why parsing an ESE file was a non-trivial task for quite a long time. Recently, Microsoft opened the format specification.

Unlike some freeware tools that parse ESE format incorrectly (for example, NirSoft's ESEDatabaseView), the RWP applies a bit more reliable way to handle ESE databases exactly in the way they are used by MS applications (using MS documented APIs). The ESE explorer's functionality is poor though, and it is good only for some initial database analysis in most cases.



View and explore files in Extensible Storage Engine format

The context menu can be used to copy selected records to the clipboard or to save the data to file. To avoid freezing the program, use the display filters with great care, especially for extensive databases!

Database file: D:\Windows\NTDS\ntds.dit

Table name: datatable

	DNT_col	PDNT_col	OBJ_col	RDNtyp_col	cnt_col	ab_cnt_col	time_col	NCDNT_col	Is\
	<All>	<All>	<All>	<All>	<A...	<All>	<All>	<All>	
1	1		1		1	0			
2	2	0	1		3	0			0
3	6	2030	1	3	2	0		2030	
4	8	2030	1	3	3	0		2030	
5	10	2030	1	3	3	0		2030	
6	11	2030	1	3	1	0		2030	
7	12	2030	1	3	3	0		2030	
8	13	2030	1	3	1	0		2030	
9	14	2030	1	3	1475	0		2030	
10	15	2030	1	3	1	0		2030	
11	16	2030	1	3	1	0		2030	

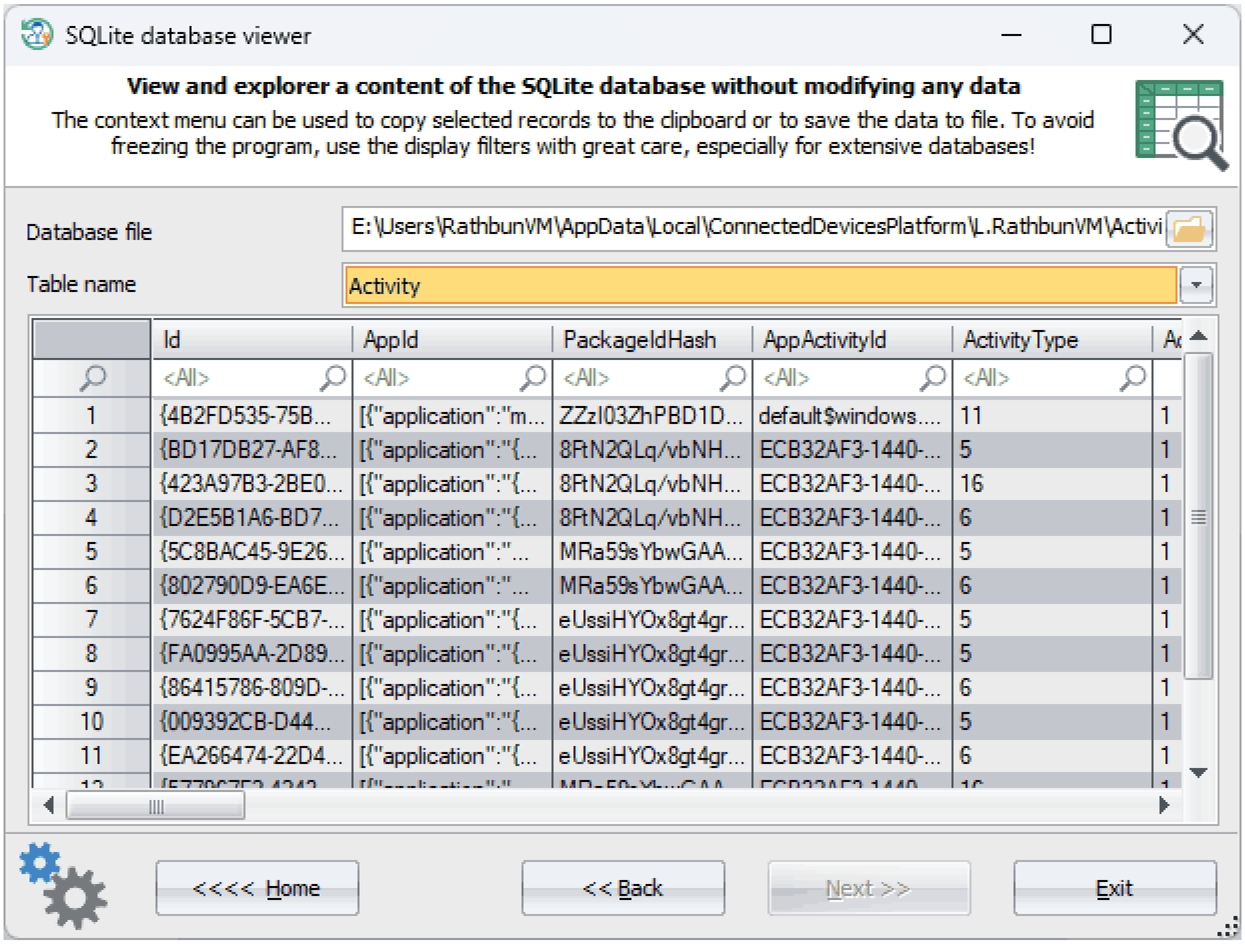
The tool's interface is an extremely simple. After you provide a path to the database file, you're free to select one of the table found there. Next, using a context menu, you can, for example, export the table to a CSV file for further investigation using a 3d-party application.

The program has a higher-level parsers for some Windows ESE databases. For example, the Windows Search database (Windows 7 - 10 only) is an Extensible Storage Engine file located at
%SYSTEMDRIVE%\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

Even though you can view the file in ESE explorer tool, the smarter way to analyze it would be using the Windows Search explorer instead.

3.9.6 SQLite database viewer

The SQLite database viewer is an extremely simple tool for viewing and analyzing databases in **SQLite** format.



View and explorer a content of the SQLite database without modifying any data

The context menu can be used to copy selected records to the clipboard or to save the data to file. To avoid freezing the program, use the display filters with great care, especially for extensive databases!

Database file: E:\Users\RathbunVM\AppData\Local\ConnectedDevicesPlatform\L.RathbunVM\Activi

Table name: Activity

	Id	AppId	PackageIdHash	AppActivityId	ActivityType	Ac
	<All>	<All>	<All>	<All>	<All>	
1	{4B2FD535-75B...	[{"application":"m...	ZZzI03ZhPBD1D...	default$windows....	11	1
2	{BD17DB27-AF8...	[{"application":"{...	8RtN2QLq/vbNH...	ECB32AF3-1440-...	5	1
3	{423A97B3-2BE0...	[{"application":"{...	8RtN2QLq/vbNH...	ECB32AF3-1440-...	16	1
4	{D2E5B1A6-BD7...	[{"application":"{...	8RtN2QLq/vbNH...	ECB32AF3-1440-...	6	1
5	{5C8BAC45-9E26...	[{"application":"...	MRa59sYbwGAA...	ECB32AF3-1440-...	5	1
6	{802790D9-EA6E...	[{"application":"...	MRa59sYbwGAA...	ECB32AF3-1440-...	6	1
7	{7624F86F-5CB7-...	[{"application":"{...	eUssiHYOx8gt4gr...	ECB32AF3-1440-...	5	1
8	{FA0995AA-2D89...	[{"application":"{...	eUssiHYOx8gt4gr...	ECB32AF3-1440-...	5	1
9	{86415786-809D-...	[{"application":"{...	eUssiHYOx8gt4gr...	ECB32AF3-1440-...	6	1
10	{009392CB-D44...	[{"application":"{...	eUssiHYOx8gt4gr...	ECB32AF3-1440-...	5	1
11	{EA266474-22D4...	[{"application":"{...	eUssiHYOx8gt4gr...	ECB32AF3-1440-...	6	1

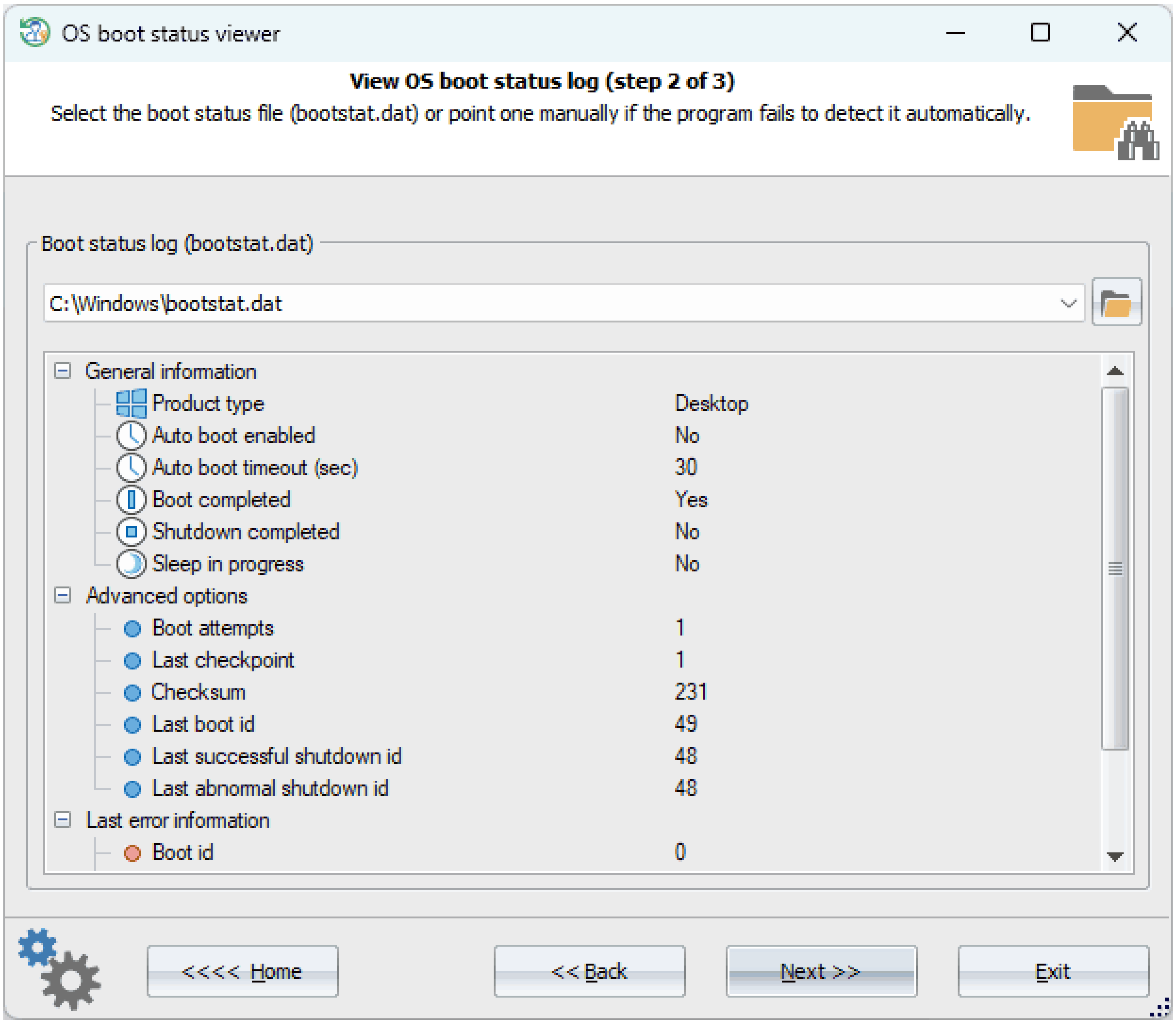
After you provide a path to the SQLite file, select for viewing one of the table this database consists of. Next, using the context menu, you can, for example, save any cell's data or export the entire table to a CSV file for further investigation using 3d-party applications.

3.9.7 Boot status explorer

The boot status explorer tool keeps track of the boot process and identifies any issues that may occur during boot. The tool parses the **bootstat.dat** file and extracts boot information stored by **Windows Boot Manager**, including but not limited to the previous boot sequence, the last successful boot and any previous failed attempts.

This can be vital when you need to determine the cause of any boot failures, such as a crash or unexpected shutdown. If Windows fails to start up properly, the Boot status explorer can be used to determine the cause of the failure and provide guidance on how to resolve the problem.

Selecting the bootstat.dat file



View OS boot status log (step 2 of 3)

Select the boot status file (bootstat.dat) or point one manually if the program fails to detect it automatically.

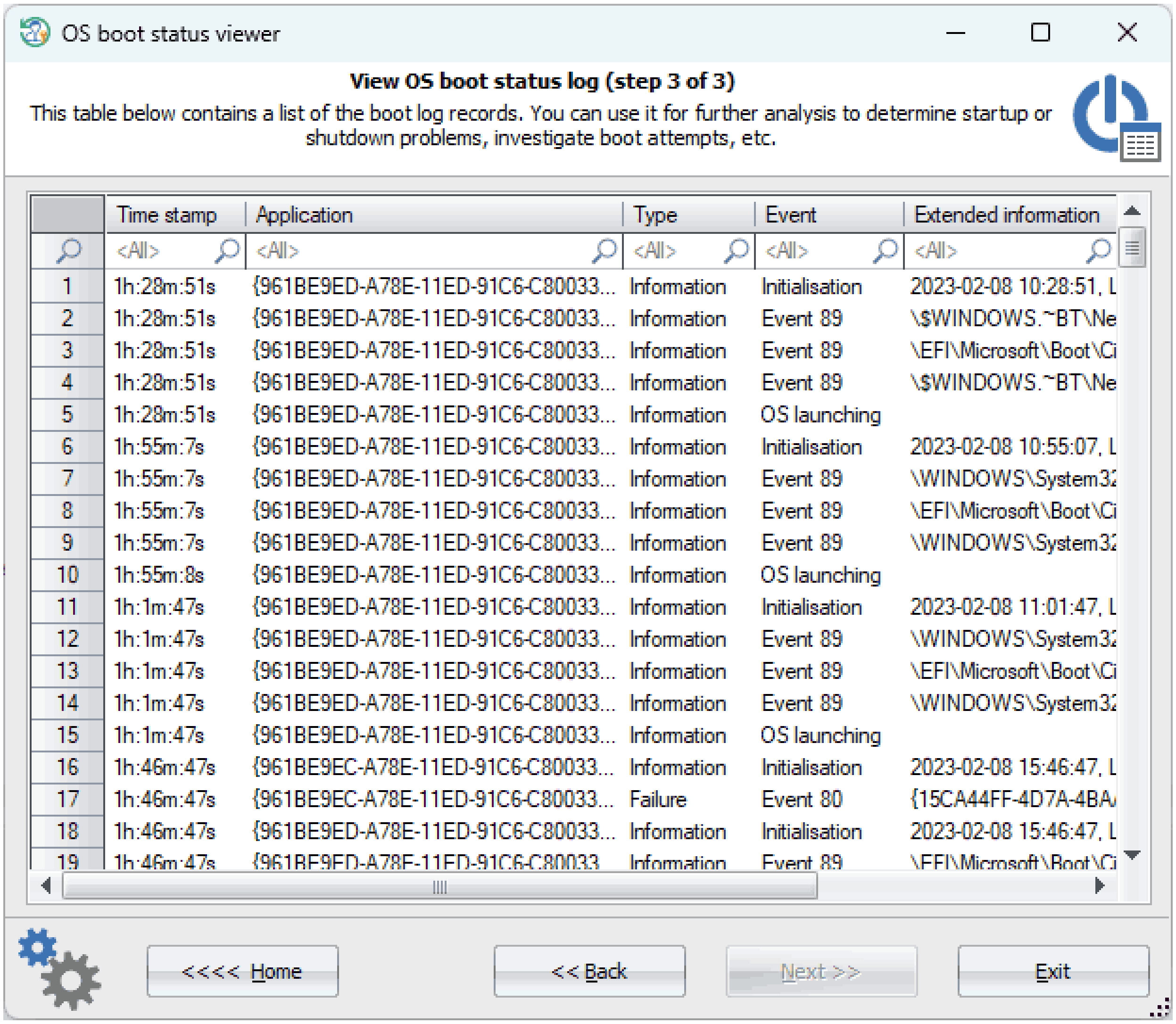
Boot status log (bootstat.dat)

C:\Windows\bootstat.dat

```
⊟ General information
    Product type                      Desktop
    Auto boot enabled                 No
    Auto boot timeout (sec)           30
    Boot completed                    Yes
    Shutdown completed                No
    Sleep in progress                 No
⊟ Advanced options
    Boot attempts                     1
    Last checkpoint                   1
    Checksum                          231
    Last boot id                      49
    Last successful shutdown id       48
    Last abnormal shutdown id         48
⊟ Last error information
    Boot id                           0
```

The bootstat.dat file resides either in Windows directory or in EFI boot partition, normally hidden in Windows. If any hidden partition is found, the program prompts to scan these partitions for the bootstat.dat.

View boot status



OS boot status viewer

View OS boot status log (step 3 of 3)

This table below contains a list of the boot log records. You can use it for further analysis to determine startup or shutdown problems, investigate boot attempts, etc.

	Time stamp	Application	Type	Event	Extended information
	<All>	<All>	<All>	<All>	<All>
1	1h:28m:51s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Initialisation	2023-02-08 10:28:51, L
2	1h:28m:51s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Event 89	\$WINDOWS.~BT\Ne
3	1h:28m:51s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Event 89	\EFI\Microsoft\Boot\Ci
4	1h:28m:51s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Event 89	\$WINDOWS.~BT\Ne
5	1h:28m:51s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	OS launching	
6	1h:55m:7s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Initialisation	2023-02-08 10:55:07, L
7	1h:55m:7s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Event 89	\WINDOWS\System32
8	1h:55m:7s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Event 89	\EFI\Microsoft\Boot\Ci
9	1h:55m:7s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Event 89	\WINDOWS\System32
10	1h:55m:8s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	OS launching	
11	1h:1m:47s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Initialisation	2023-02-08 11:01:47, L
12	1h:1m:47s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Event 89	\WINDOWS\System32
13	1h:1m:47s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Event 89	\EFI\Microsoft\Boot\Ci
14	1h:1m:47s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Event 89	\WINDOWS\System32
15	1h:1m:47s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	OS launching	
16	1h:46m:47s	{961BE9EC-A78E-11ED-91C6-C80033...	Information	Initialisation	2023-02-08 15:46:47, L
17	1h:46m:47s	{961BE9EC-A78E-11ED-91C6-C80033...	Failure	Event 80	{15CA44FF-4D7A-4BA
18	1h:46m:47s	{961BE9ED-A78E-11ED-91C6-C80033...	Information	Initialisation	2023-02-08 15:46:47, L
19	1h:46m:47s	{961BE9ED-A78E-11ED-91C6-C80033	Information	Event 89	\EFI\Microsoft\Boot\Ci

The boot status log consists of event records. Every record describes an event related to the boot process in Windows and contains the following fields:

- **Time stamp** - BIOS time (in seconds) from the beginning of the day. In Windows 10 and higher OSes this value may be cropped
- **Application** - GUID of the source application.
- **Type** - record type. For example, error, warning, or information.
- **Event** - event ID. Some event IDs are unknown.
- **Extended info** - additional information about event.

License and registration

4 License and registration

4.1 License Agreement

==
SOFTWARE LICENSE AGREEMENT
==

IMPORTANT-READ CAREFULLY: This is the End User License Agreement (the "Agreement") is a legal agreement between you, the end-user, and Passcape Software, the manufacturer and the copyright owner, for the use of the "Reset Windows Password" software product ("SOFTWARE").

All copyrights to SOFTWARE are exclusively owned by Passcape Software.

The SOFTWARE and any documentation included in the distribution package are protected by national copyright laws and international treaties. Any unauthorized use of the SOFTWARE shall result in immediate and automatic termination of this license and may result in criminal and/or civil prosecution.

You are granted a non-exclusive license to use the SOFTWARE as set forth herein.

You can use trial version of SOFTWARE as long as you want, but to access all functions you must purchase the fully functional version. Upon payment we provide to you the download link and the registration code to the SOFTWARE .

Once registered, the user is granted a non-exclusive license to use the SOFTWARE on one computer at a time for every single-user license purchased.

With the personal license, you can use the SOFTWARE as set forth in this Agreement for non-commercial purposes in non-business, non-commercial environment. To use the SOFTWARE in a corporate, government or business environment, you should purchase a business license. With the business license you can run the SOFTWARE on multiple computers within a single organization.

The registered SOFTWARE may not be rented or leased, but may be permanently transferred together with the accompanying documentation, if the person receiving it agrees to terms of this license. If the software is an update, the transfer must include the update and all previous versions.

The SOFTWARE unregistered (trial) version may be freely distributed, provided that the distribution package is not modified. No person or company may charge a fee for the distribution of the SOFTWARE without written permission from the copyright holder.

You may not create any copy of the SOFTWARE. You can make one (1) copy the SOFTWARE for backup and archival purposes, provided, however, that the original and each copy is kept in your possession or control, and that your use of the SOFTWARE does not exceed that which is allowed in this Agreement.

You agree not modify, decompile, disassemble, otherwise reverse engineer the SOFTWARE, unless such activity is expressly permitted by applicable law.

Passcape Software does not warrant that the software is fit for any particular purpose. Passcape Software disclaims all other warranties with respect to the SOFTWARE, either express or implied. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, do the above limitations or exclusions may not apply to you.

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our SOFTWARE or have permission from the legitimate owner to perform these acts. Any illegal use of our SOFTWARE will be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

You further attest that the recovered data, passwords and/or files will not be used for any illegal purpose. Be aware password recovery and the subsequencial data decryption of unauthorized or otherwise illegally obtained files may constitute theft or another wrongful action and may result in your civil and (or) criminal prosecution.

All rights not expressly granted here are reserved by Passcape Software.

4.2 Registration

The software is available in three editions: Light, Standard and Advanced. The detailed list of features is shown here. You can order fully registered version of Reset Windows Password at a cost of $45 for Light Edition (personal usage), $145 for Standard Edition (personal usage) or $345 for Advanced Edition (business license).

Detailed instructions for all kinds of orders are available online at the program's order page. Online orders are fulfilled in just a few minutes 24 hours a day 7 days a week. The ordering pages are on a secure server, ensuring that your confidential information remains confidential.

As soon as your order is processed, you will be provided with the link to the fully-featured version of the program. If you've made a payment, but haven't received a confirmation letter with the link within a reasonable amount of time, please notify us!

Important: when completing the order form, please double-check that your e-mail address is correct. If it will not, we'll be unable to send you the registration code.

To complete the registration process, you should download the program using the link that was sent to you in your registration e-mail and follow the instructions to create a bootable disk.

4.3 Limitation of unregistered version

An unregistered version of the **Reset Windows Password** shows only first 3 characters of recovered passwords and has some functional limitations. In particular, only hashes dump and password backup features are working without any limitations. Registered version eliminates all restrictions.

4.4 Program editions

Reset Windows Password comes in three editions: Light, Standard and Advanced. The detailed list of features is shown below.

FEATURE	Light	Stan-dard	Advan-ced
Support for Windows NT/2000/XP/Vista/7/8/10/11 workstations	+	+	+
Support for NT/2000/2003/2008/2012/2016/2019/2022 servers	+	+	+
Windows 64-bit support	+	+	+
Non-US Windows support	+	+	+
Multilingual passwords support	+	+	+
Additional mass storage drivers	+	+	+
Detect multiple Operating Systems	+	+	+
Extended download warranty	+	+	+
14-day money back guarantee	+	+	+
Using in a corporate, government or business environment	-	-	+
License	**personal**	**personal**	**business**
Support for all types of Windows accounts, including Live ID, Microsoft account, etc.	+	+	+
Create a bootable password reset CD/DVD	+	+	+
Create a bootable password reset USB	+	+	+
Create a bootable password reset HDD	+	+	+
Support booting on UEFI-based computers	+	+	+
Reset local Administrator password	+	+	+
Change local Administrator password	+	+	+
Unlock disabled, locked or expired local Administrator account (1)	+	+	+
Reset Domain Administrator password	-	-	+
Change Domain Administrator password	-	-	+
Unlock disabled, locked or expired Domain Administrator account (1)	-	-	+
Change a desktop account extended properties and flags	+	+	+
Change extended properties and flags of Active Directory accounts	-	-	+
Reset password to regular (SAM) accounts	+	+	+
Change passwords to regular (SAM) accounts	+	+	+
Unlock disabled, locked or expired SAM account (1)	+	+	+
Decrypt secret questions and answers for Windows 10 OS	+	+	+
Reset password to Active Directory accounts	-	-	+
Change passwords to Active Directory accounts	-	-	+
Unlock disabled, locked or expired Active Directory accounts (1)	-	-	+
Reset/Change password to DSRM (2) account	-	-	+
Reset domain cached password	-	+	+
Change domain cached password	-	+	+
Instant load and install any IDE/SATA/SCSI/RAID driver	+	+	+
Roll back changes (restore previously modified passwords)	+	+	+
Support SYSKEY encryption	+	+	+
Support SYSKEY startup password decryption	+	+	+

FEATURE	Light	Standard	Advanced
Support SYSKEY floppy decryption	+	+	+
Show password hints	+	+	+
Dump LM/NTLM password hashes for regular (SAM) accounts	+	+	+
Dump password history hashes	-	+	+
Dump domain cached credentials (MSCACHE)	-	+	+
Dump LM/NTLM password hashes for Active Directory accounts	-	-	+
Dump Windows PIN	+	+	+
Password recovery for Active Directory user accounts [3]	-	-	+
Password recovery for regular (SAM) user accounts	-	+	+
Password recovery for domain cached accounts	-	-	+
Search for simple passwords	-	+	+
Primitive dictionary analysis	-	+	+
Advanced dictionary analysis [4]	-	-	+
Primitive brute-force attack against user passwords	-	+	+
Recover passwords using Artificial Intelligence analysis	-	+	+
Password recovery using custom attacks including dictionary, hybrid and mask attacks	-	+	+
Remove password history hashes out of regular (SAM) accounts	-	+	+
Remove password history hashes out of Active Directory accounts	-	+	+
Remove domain cached passwords	-	+	+
Remove cached logon passwords	-	+	+
Remove password reset information	-	+	+
Remove password hints	-	+	+
Reset SYSKEY security (with user passwords re-encryption)	-	+	+
Lookup SYSKEY startup password	-	+	+
Instant plaintext password recovery for accounts with Picture password	-	+	+
Instant plaintext password recovery for accounts with Biometric logon [5]	-	+	+
PIN recovery	-	+	+
Decrypt PIN history [8]	-	+	+
Mount virtual drives	+	+	+
Network drive mapper	+	+	+
ESE database explorer [6]	+	+	+
Automatic detection and mounting virtual OSes	+	+	+
Search for virtual machines passwords	-	+	+
Search for lost product keys and serial numbers	-	+	+
Convert Microsoft Live ID to local user account	+	+	+
Backup passwords, registry and Active Directory	+	+	+
Search for password-protected documents	+	+	+
Search for recently opened documents [7]	+	+	+

FEATURE	Light	Stan-dard	Advan-ced
Password recovery for MS Office, OpenOffice, LibreOffice, MyOffice, and PDF documents	-	+	+
Password lookup and recovery for Indian Aadhaar and e-pan cards	-	+	+
Search and decrypt Internet browser passwords	-	+	+
Search and decrypt passwords for popular e-mail clients	-	+	+
Search and decrypt different network passwords	-	+	+
Create new SAM accounts	-	+	+
Unlock BitLocker drives	+	+	+
Volume explorer	+	+	+
Extract BitLocker recovery passwords from Active Directory	-	-	+
Windows logon options	-	+	+
Local password policy editor	-	+	+
Domain password policy editor	-	-	+
Logon policy editor	-	+	+
Interface and system restriction policy editor	-	+	+
Support for passwordless sign-in option	+	+	+
Decrypt Windows Hello credentials (8)	-	+	+
Logon history and statistics (6)	-	-	+
Hardware history (7)	-	+	+
Software history (7)	-	+	+
Network history (7)	-	+	+
Recent user activity (6)	-	-	+
Search for recently opened documents (7)	-	+	+
View program execution timeline (7)	-	+	+
Windows activity timeline (6)	-	-	+
Windows Sticky Notes (6)	-	-	+
Camera and microphone access tracking (6)	-	-	+
Clipboard history (6)	-	-	+
USB history (6)	-	-	+
Recycle Bin history (6)	-	-	+
History of the Remote Desktop (6)	-	-	+
System resource usage monitor (6)	-	-	+
Windows Search database explorer (6)	-	-	+
SQLite database viewer (6)	-	-	+
OS boot status viewer (6)	-	-	+
Windows Media forensics: image analysis	-	-	+
Windows Media forensics: video analysis	-	-	+
Windows Media forensics: user actions	-	-	+

FEATURE	Light	Stan-dard	Advan-ced
Photo library analysis	-	-	+
Photo library actions	-	-	+
Media Player analysis	-	-	+
Media Player actions	-	-	+
System events (6)	-	-	+
View Telegram downloads (6)	-	-	+
Recover Telegram passcode	-	-	+
Decrypt Telegram files (6)	-	-	+
Web history (6)	-	-	+
User IP address history (6)	-	-	+
Last modified files	-	+	+
Last modified directories	-	+	+
File checksum calculator (7)	-	+	+
Duplicate file finder (7)	-	+	+
Disk space analyzer (6)	-	-	+
File statistics (6)	-	-	+
Fast disk search (7)	-	+	+
Junk file remover and registry cleaner	-	+	+
Create disk images in raw format	+	+	+
Create disk images in *.E01 format	-	+	+
Program's access password	+	+	+
Price	**$45**	**$145**	**$345**

Notes:
(1) If the account is locked, disabled or expired
(2) Directory Services Restore Mode
(3) If Reversible Encryption is set. You can find this option in your domain password policy.
(4) Using Arabian, Chinese, English, French, German, Portuguese, Russian, Spanish dictionaries.
(5) Not for all accounts
(6) Data export feature is available in Advanced edition only
(7) Data export feature is available in Standard and Advanced editions only
(8) If not protected with TPM

Technical support

5 Technical support

5.1 Reporting problems

If you have a problem, please contact us at support@passcape.com. Please inform us about the following:

- Windows version including service packs and other fixes installed
- Program full version (see **About** dialog)
- Program registration information if any
- Detailed description of your problem (as much information as possible)

If you're reporting an error, please attach **RWPCrash.log** file(s) that was saved during an unhandled exception.

5.2 Suggesting features

If you have any questions, comments or suggestions about the program or would like more information, email us at info@passcape.com. Please don't forget to mention the program name and version. Also make sure you have the latest program version installed. Your feedback helps us to improve our products and work more effective.

5.3 Contacts

Please don't hesitate to send your questions regarding our products to e-mail support@passcape.com.
You will get reply during one or two days. Note, that registered users have priority in technical support.

If you experience any problems during registration process, please send a letter to sales@passcape.com
We will be happy to assist you with the registration.

Please write in English!

You can find other password recovery utilities at https://www.passcape.com.