

Reset Windows Password

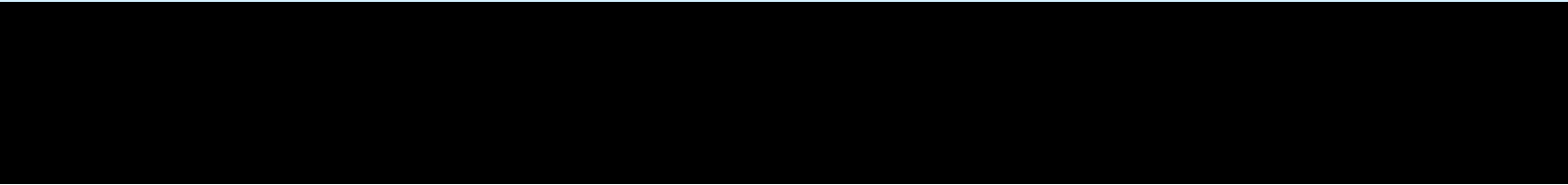
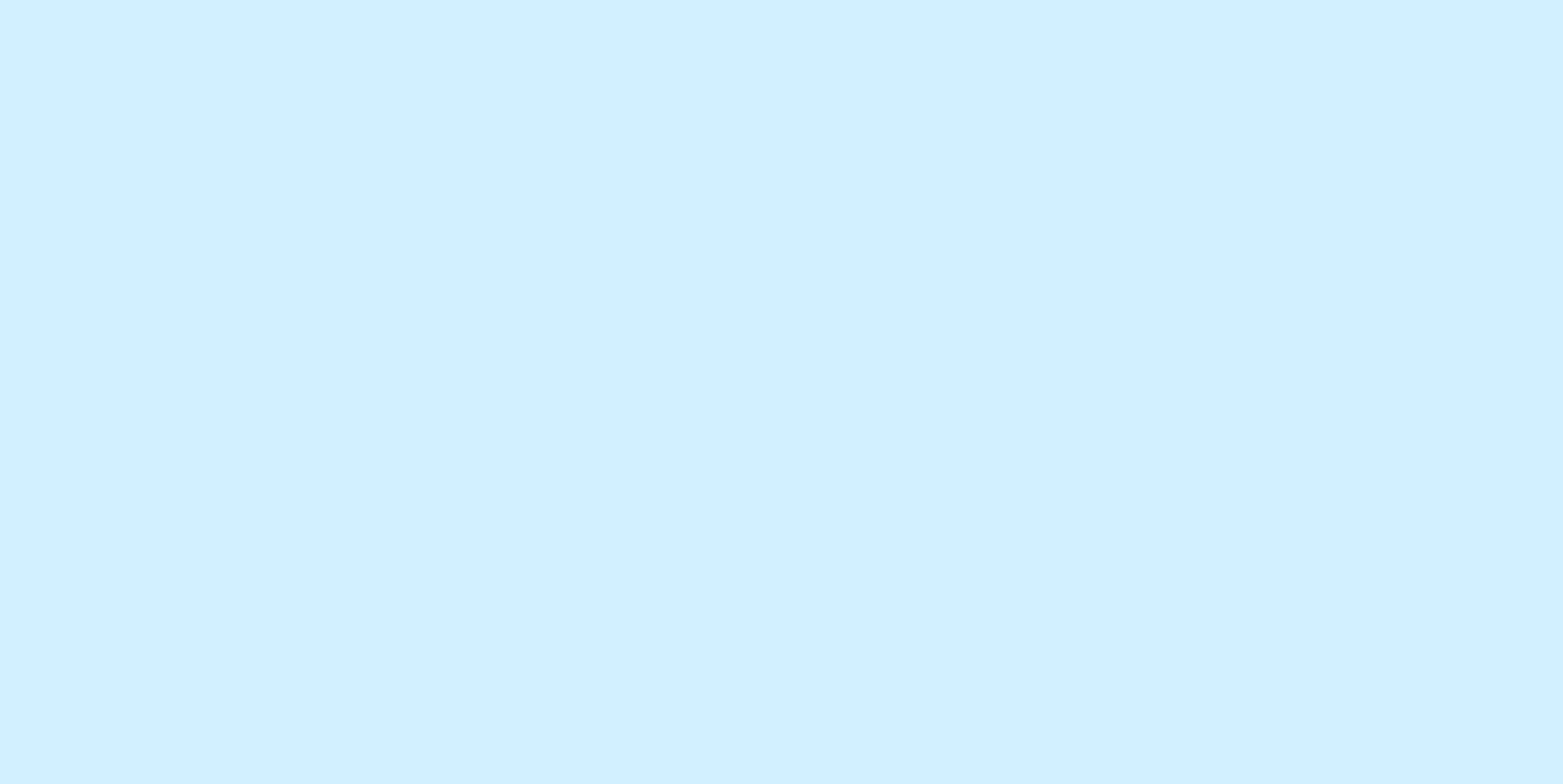
Copyright (c) 2024 Passcape Software. All rights reserved.
Passcape Software

1.		6
1.1	7
1.2	7
1.3	8
2.		10
2.1	3	11
2.2	RWP	11
2.3	BIOS/UEFI	15
2.4	CD/DVD/USB BIOS-	19
2.5	22
3.		24
3.1	25
3.2	28
3.2.1	28
3.2.2	32
3.2.3	34
3.2.4	37
3.2.5	55
3.2.6	69
3.2.7	()	71
3.2.8	() PIN	73
3.2.9	75
3.3	Active Directory	78
3.3.1	DSRM	78
3.3.2	BitLocker	80
3.4	82
3.4.1	82
3.4.2	()	86
3.5	87
3.5.1	88
3.5.1.1	91
3.5.2	94
3.5.2.1	97
3.5.3	Windows Hello	100
3.5.4	PIN	102
3.5.4.1	106
3.5.5	SYSKEY	108

3.5.5.1		114
3.5.6		117
3.5.7		120
3.5.8		125
3.5.8.1		127
3.5.8.2	e-mail	128
3.5.8.3	LAN/WAN/RAS/DSL/VPN/WiFi	129
3.5.8.4		131
3.5.9		131
3.6		133
3.6.1		133
3.6.2	C	137
3.6.3		140
3.6.4		143
3.6.5		146
3.6.6		149
3.6.7		151
3.6.8	IP	158
3.7		160
3.7.1		160
3.7.2		164
3.7.3	Windows	166
3.7.4	Windows Media	170
3.7.4.1		171
3.7.4.1.1		172
3.7.4.1.2		173
3.7.4.1.3		174
3.7.4.1.4		175
3.7.4.1.5		176
3.7.4.1.6		177
3.7.4.1.7		178
3.7.4.1.8		179
3.7.4.1.9		180
3.7.4.1.10		181
3.7.4.1.11		182
3.7.4.2		182
3.7.4.2.1		183
3.7.4.2.2		184
3.7.4.2.3		185
3.7.4.2.4		186
3.7.4.2.5		187
3.7.4.2.6		188
3.7.4.3		188
3.7.4.3.1		189

3.7.4.3.2		190
3.7.4.3.3		191
3.7.4.3.4		192
3.7.4.3.5		193
3.7.4.3.6		194
3.7.4.4		194
3.7.4.4.1		195
3.7.4.4.2		196
3.7.4.4.3		197
3.7.4.4.4		198
3.7.4.5		198
3.7.4.5.1		199
3.7.4.6		199
3.7.4.6.1		200
3.7.4.6.2		201
3.7.4.6.3		202
3.7.4.6.4		203
3.7.4.6.5		204
3.7.4.6.6		205
3.7.4.7		205
3.7.4.7.1		206
3.7.5	Windows	206
3.7.6		209
3.7.7		212
3.7.8	USB	216
3.7.9		217
3.7.10	Windows Search	222
3.7.11		224
3.7.12		224
3.7.12.1		225
3.7.12.2		227
3.7.12.3		229
3.7.13		231
3.7.14	Telegram	234
3.7.14.1	Telegram	238
3.7.14.2	Telegram	238
3.7.14.3	Telegram	242
3.8		243
3.8.1		243
3.8.2		245
3.8.3	Bitlocker	246
3.8.4		247
3.8.5		248
3.8.6		250

3.8.7	253
3.8.8	253
3.8.9	255
3.8.10	258
3.8.11	260
3.8.12	262
3.8.13	264
3.9	268
3.9.1	268
3.9.2	271
3.9.3	274
3.9.3.1	276
3.9.3.2	278
3.9.3.3	281
3.9.3.4	283
3.9.3.5	286
3.9.3.6	SYSKEY	289
3.9.4	292
3.9.5	ESE (Extensible Storage Engine)	293
3.9.6	SQLite	294
3.9.7	295
4.		298
4.1	299
4.2	300
4.3	300
4.4	300
5.		306
5.1	307
5.2	307
5.3	307



1

1.1

Reset Windows Password

Windows. Reset Windows Password

Windows (Windows NT), Active Directory

Windows.

1. SAM SYSTEM ()
- 2.
- 3.

CD, DVD USB (Compact Flash,
 SmartMedia, SONY Memory Stick, Secure Digital, ZIP drives, USB Hard Disk drives .). Reset Windows
 Password IDE, SATA, SCSI, RAID, FAT,
 FAT32, NTFS, NTFS5,
 Highpoint, Intel, Jmicron, Marvell, Nvidia, Silicion Image, Sis, Uli, Via, Vmware

1.2

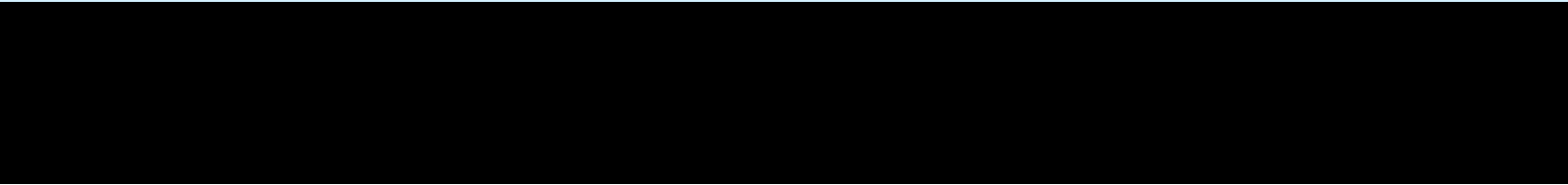
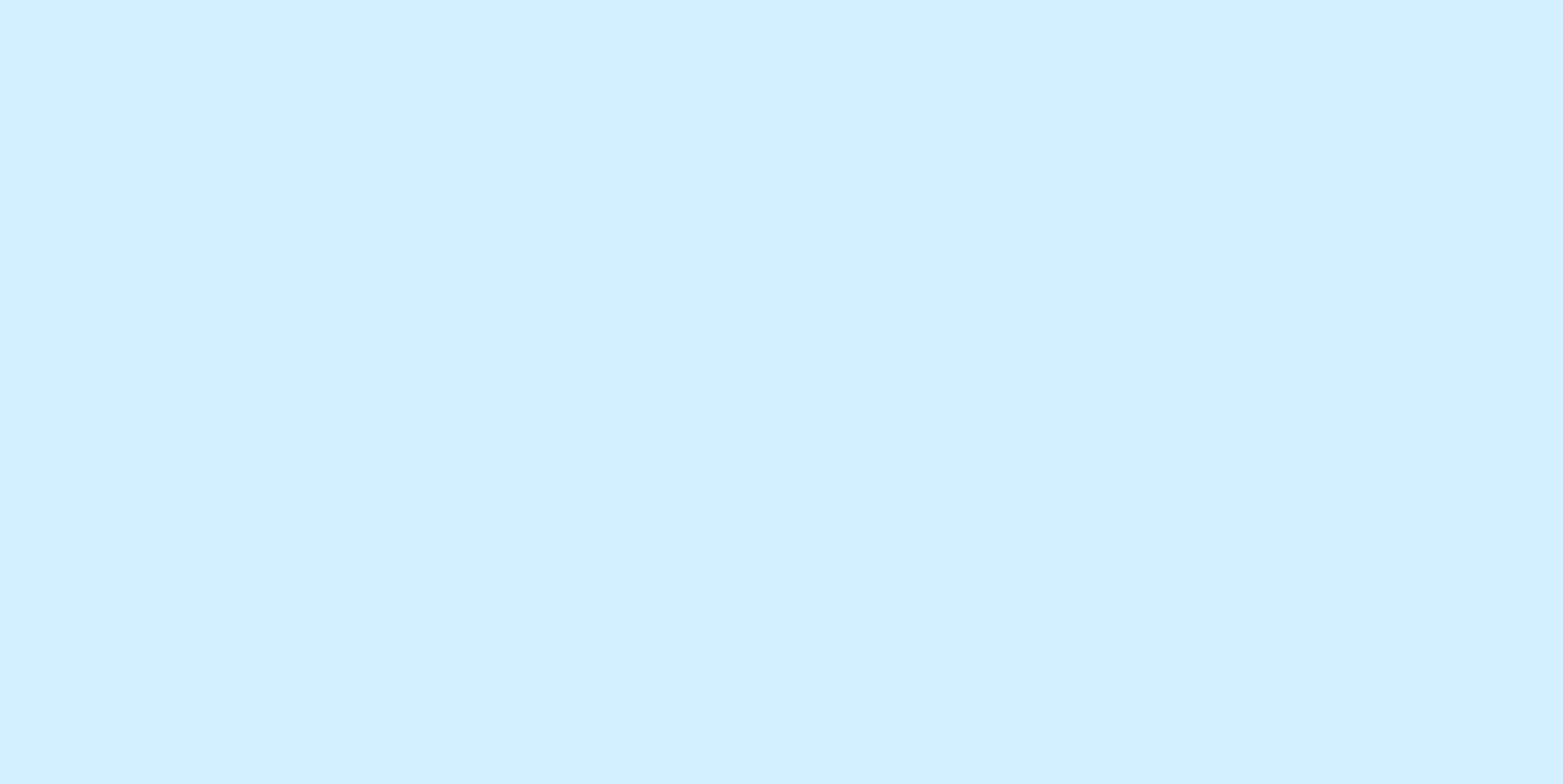
- Windows Windows NT.
- 32/64- Windows.
-

Active Directory.

- Windows
- SAM
- Active Directory.

Active Directory.

- Active Directory
- RODC.
- Microsoft,



2

2.1 3



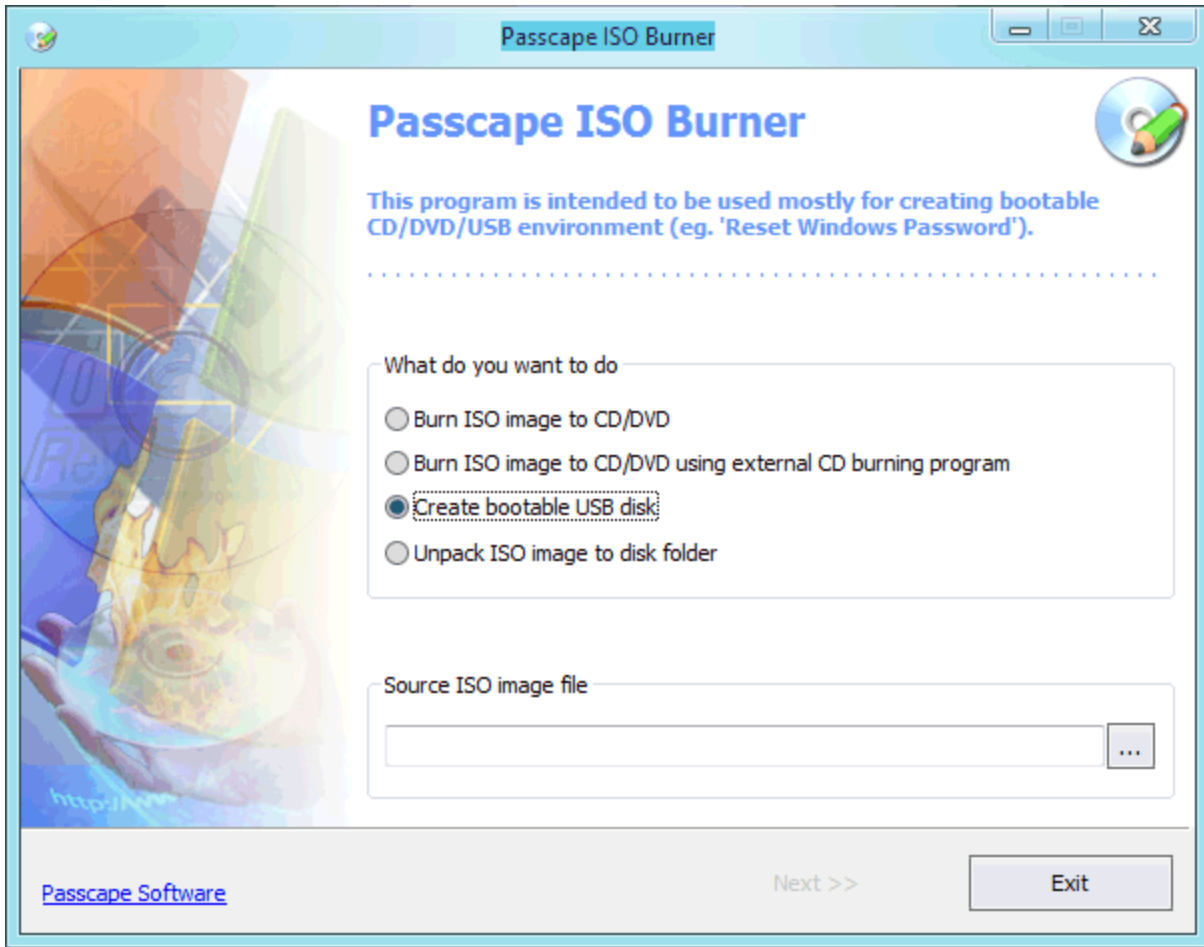
1. <https://www.passcape.com/download/rwp.zip> (Reset Windows Password)
2. [RWP:](#) RWP.ZIP, IsoBurner.exe, CD/DVD/USB, ISO
3. [BIOS/UEFI](#) (CD-ROM, DVD-ROM USB) BIOS/UEFI (CD, DVD USB F8),

2.2

RWP



[Passcape ISO Burner](#)

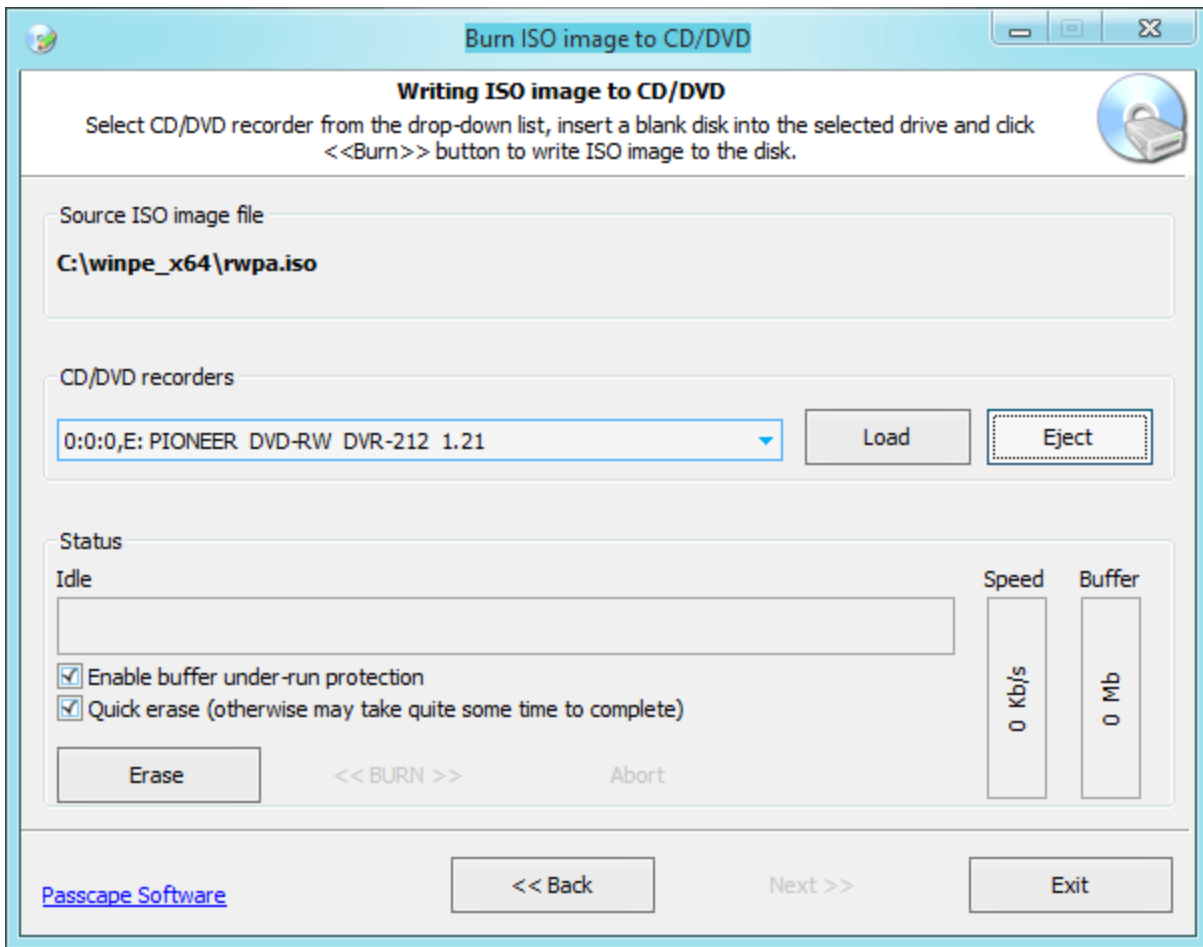


Passcape ISO Burner CD, DVD USB ISO-9660

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

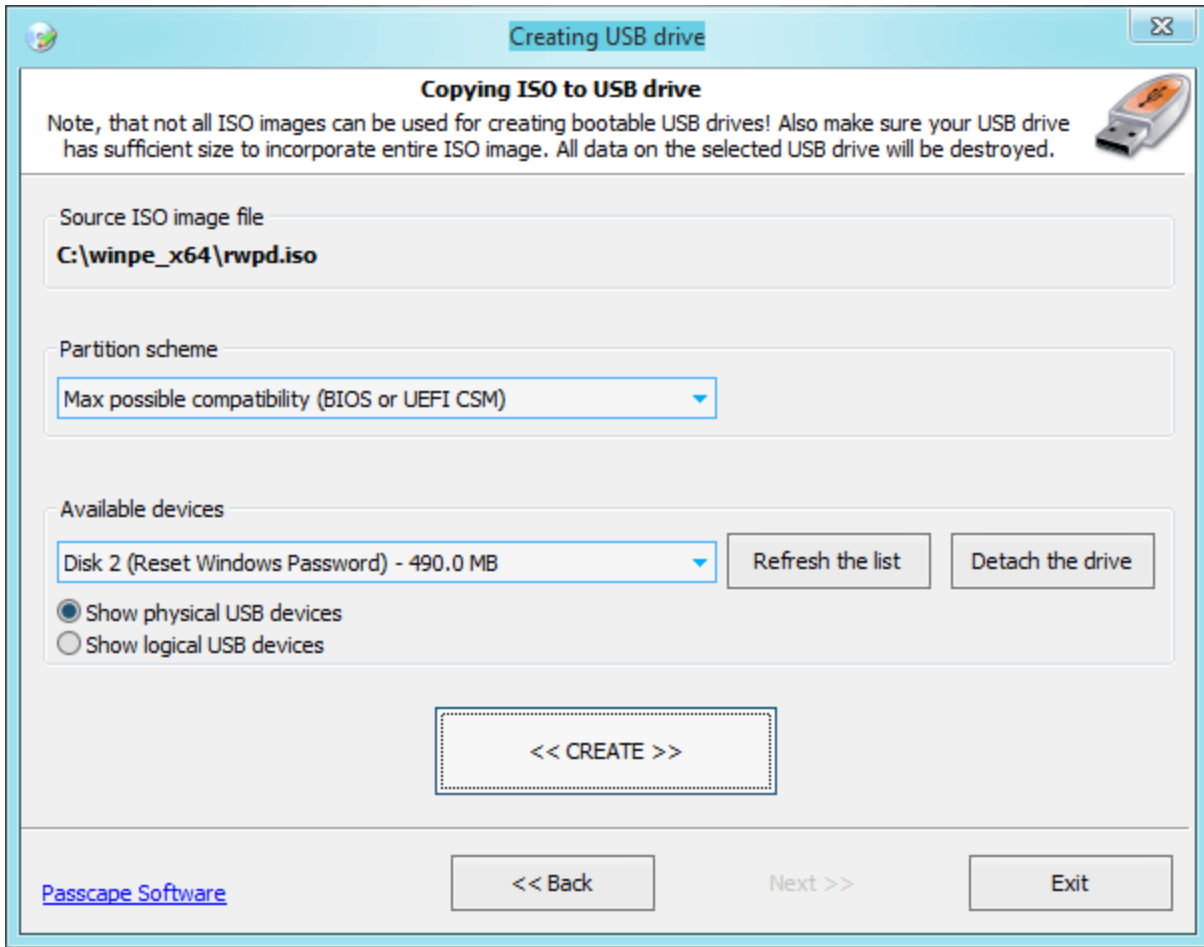
- ISO CD/DVD
- ISO CD/DVD, Nero, ImgBurn.
- ISO- USB
- ISO (,)

CD Reset Windows Password



ISO : 'Burn ISO image to CD/DVD',
 'Next',
 CD/DVD
 <<Burn>> ISO

USB c Reset Windows Password



- ISO (USB- (<< CREATE >> USB-))
 - USB- ()
 - MBR for UEFI). UEFI, 'Max compatibility with new PCs (FAT32 UEFI USB-)
 - BIOS, USB, 'Max compatibility with old PCs (FAT32 MBR for BIOS). USB
 - ('Max possible compatibility'). BIOS UEFI (**USB Compatibility Support Mode).** **Legacy Boot Mode.**
- UEFI (Unified Extensible Firmware Interface) — BIOS. BIOS 2010
- UEFI.

Q: CD USB ; ,

A: , . 2 .

Q: BIOS,

A: BIOS. , BIOS. , BIOS. , BIOS. ; BIOS

Ins. AMI BIOS Ctrl+Alt+Del+Ins. ; BIOS

Award, , ,

BIOS. BIOS

CMOS , CMOS Dallas BIOS CMOS Odin; BIOS BIOS

killcmos. BIOS , cmospwd

Q: 64- 64- 32- 32- , 32-

A: Reset Windows Password

Q: BIOS- CD/USB UEFI?

A: UEFI. ESC, F2 DEL 'Boot' 'Launch CSM'. 'Security' 'Secure Boot UEFI Control'. DVD/USB UEFI (F8),

Q: USB , BIOS, UEFI?

A: IsoBurner (Max possible compatibility') USB. BIOS, UEFI (). 'Legacy Boot Mode'.

Q: USB UEFI. ?

A: , USB BIOS UEFI CSM, UEFI
 UEFI
 UEFI 'Boot - Fast Boot' 'Security - Secure Boot',
 ('Compatibility Support Mode').
 'Max compatibility with new PCs (FAT32 MBR for UEFI Secure Boot).

BIOS

BIOS	
AWARD BIOS 2.50	AWARD_SW, 01322222, j262, TTPTHA, KDD, ZBAAACA, aPAf, lkwpete, 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, lkwpete, Wodj, aPAf, j262, Syxz, ZJAAADC, 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, helga s, 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, xljbj
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

CD/DVD/USB

BIOS-

PhoenixBIOS Setup Utility							
Main	Advanced	Security	Power	Boot	Exit		
+Removable Devices +Hard Drive CD-ROM Drive Network boot from AMD Am79C970A				Item Specific Help Keys used to view or 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

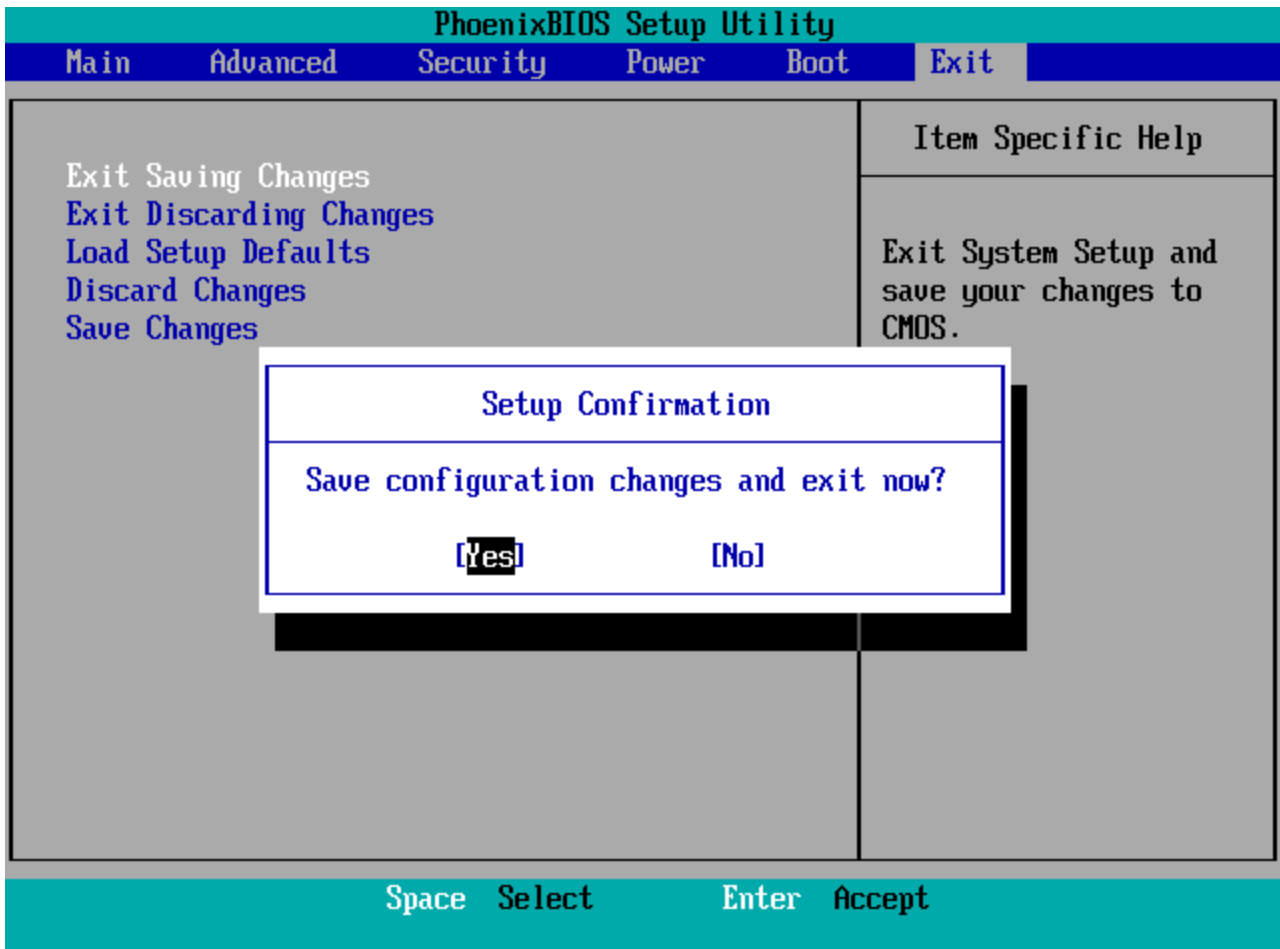
BIOS

 Del
 : F2, F10, F11, ESC . . .

BIOS.

PhoenixBIOS Setup Utility						
Main	Advanced	Security	Power	Boot	Exit	
CD-ROM Drive +Removable Devices +Hard Drive Network boot from AMD Am79C970A					Item Specific Help Keys used to view or 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

BIOS , CD USB Reset Windows Password



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

Reset Windows Password.



RWP

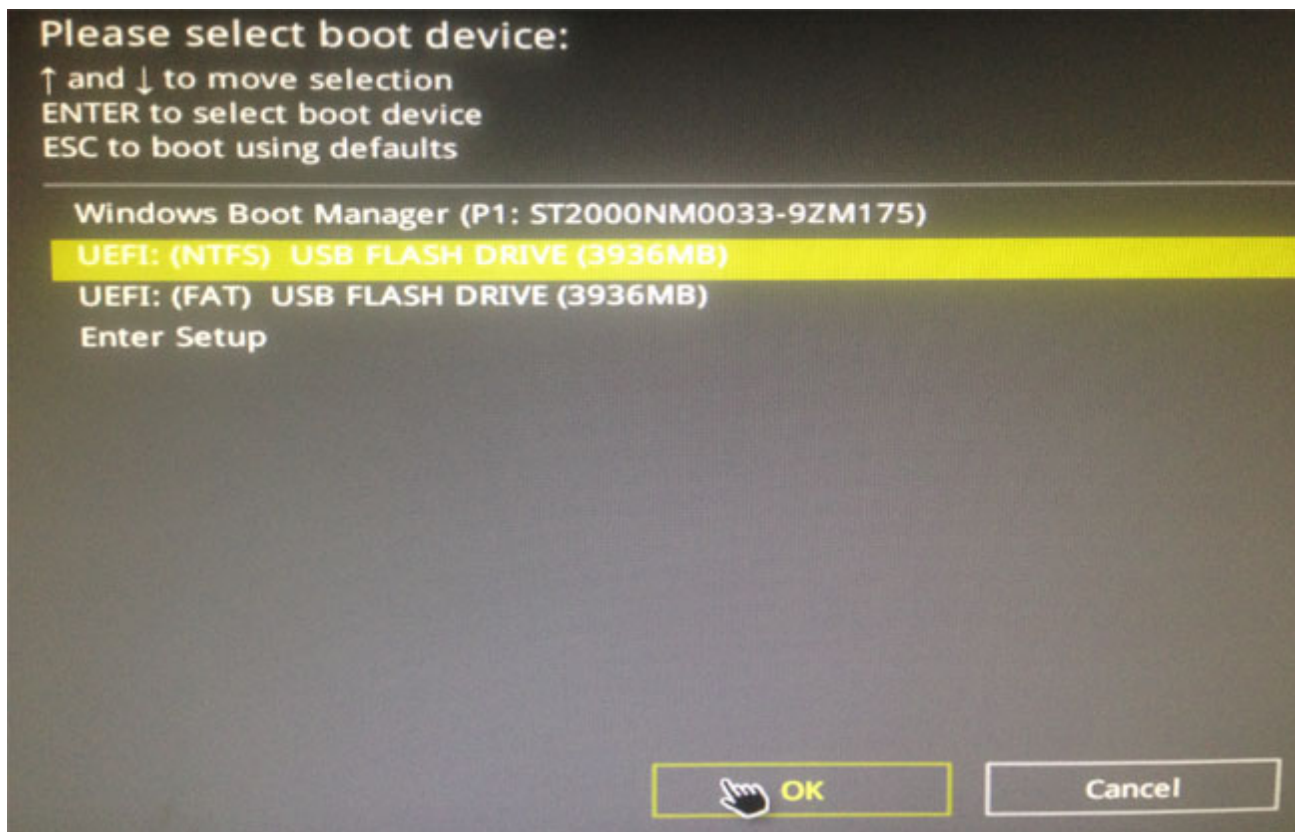
2.5

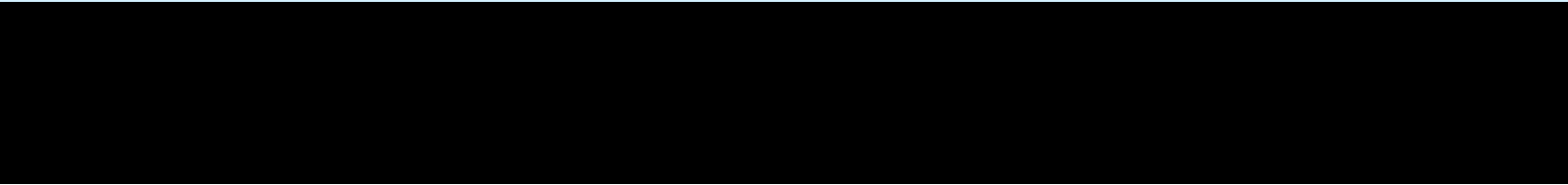
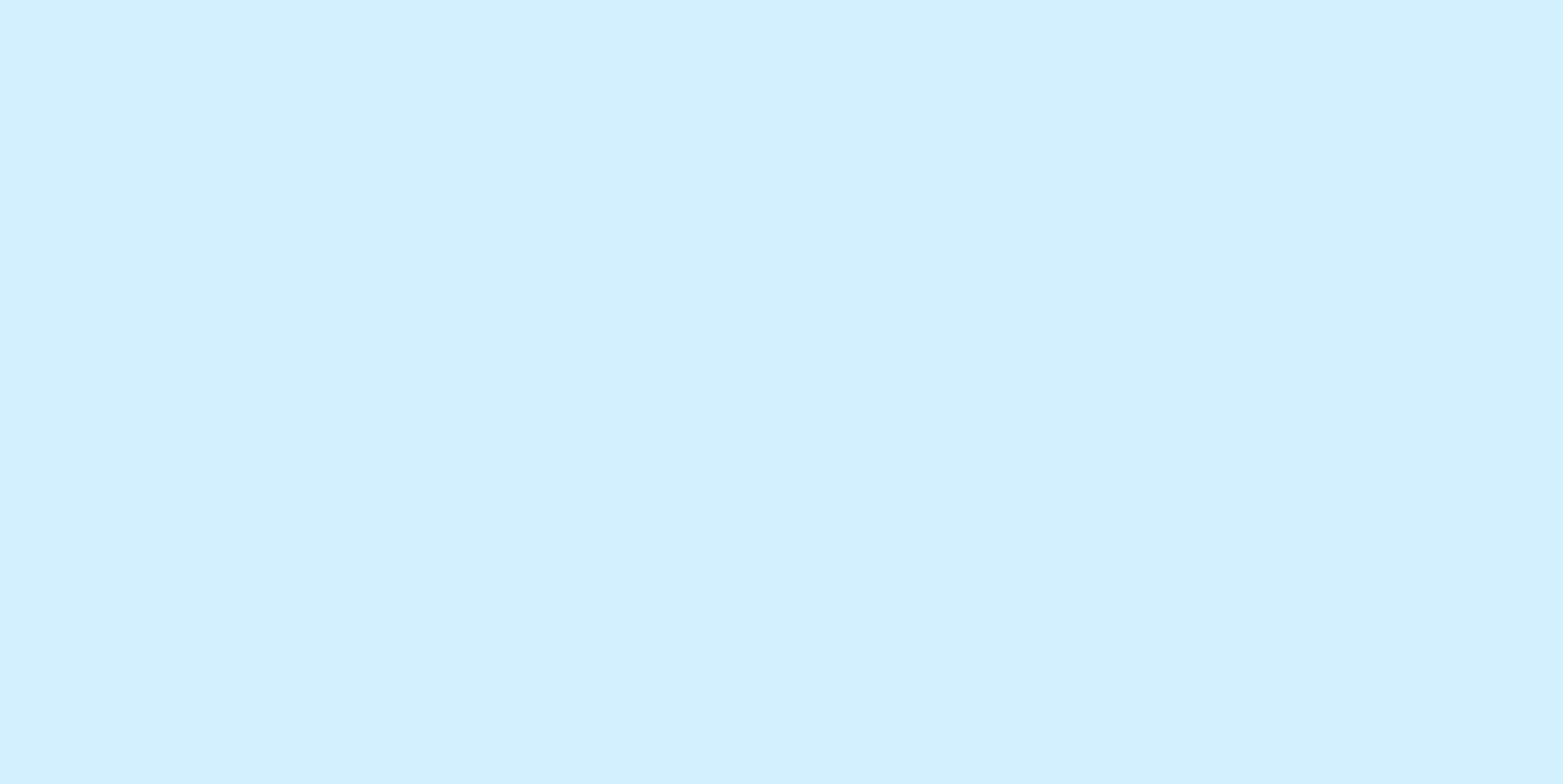
BIOS/UEFI

UEFI.

F8.

UEFI,
UEFI





3
3.1



- : Local accounts -
- SAM, Active Directory -
- NTDS.DIT, Domain accounts -
- SECURITY), Passwords -
- , Forensic tools -
- , Utilities -

- (. .).
- (SAM)
- _____
- _____
- _____
- _____

- _____
- _____
- () _____
- Windows PIN
- _____

Active Directory (AD)

- _____
- / _____ DSRM (Directory Services Restore Mode)
- _____
- _____
- _____ BitLocker
- () _____
- _____

(DCC)

- _____
- () _____
- _____

- _____
- _____
- _____
- _____ Windows Hello
- _____ PIN-
- _____ SYSKEY
- _____
- _____
- _____
- _____

- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____ IP

- _____
- _____
- _____ Windows
- _____ Windows Media
- _____ Windows
- _____
- _____
- _____
- _____ USB
- _____
- _____ Windows Search
- _____
- _____ Windows
- _____ Telegram

- _____
- _____ IDE/SATA/SCSI/RAID
- _____ Bitlocker
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____

- _____
- _____
- _____
- _____
- _____ ESE (Extensible Storage Engine)
- _____ SQLite
- _____

SAM

SAM

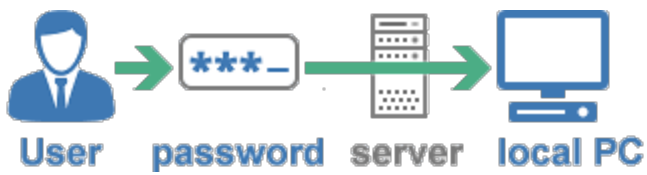
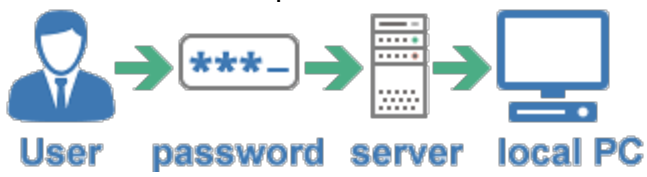


ACTIVE DIRECTORY

NTDS.DIT

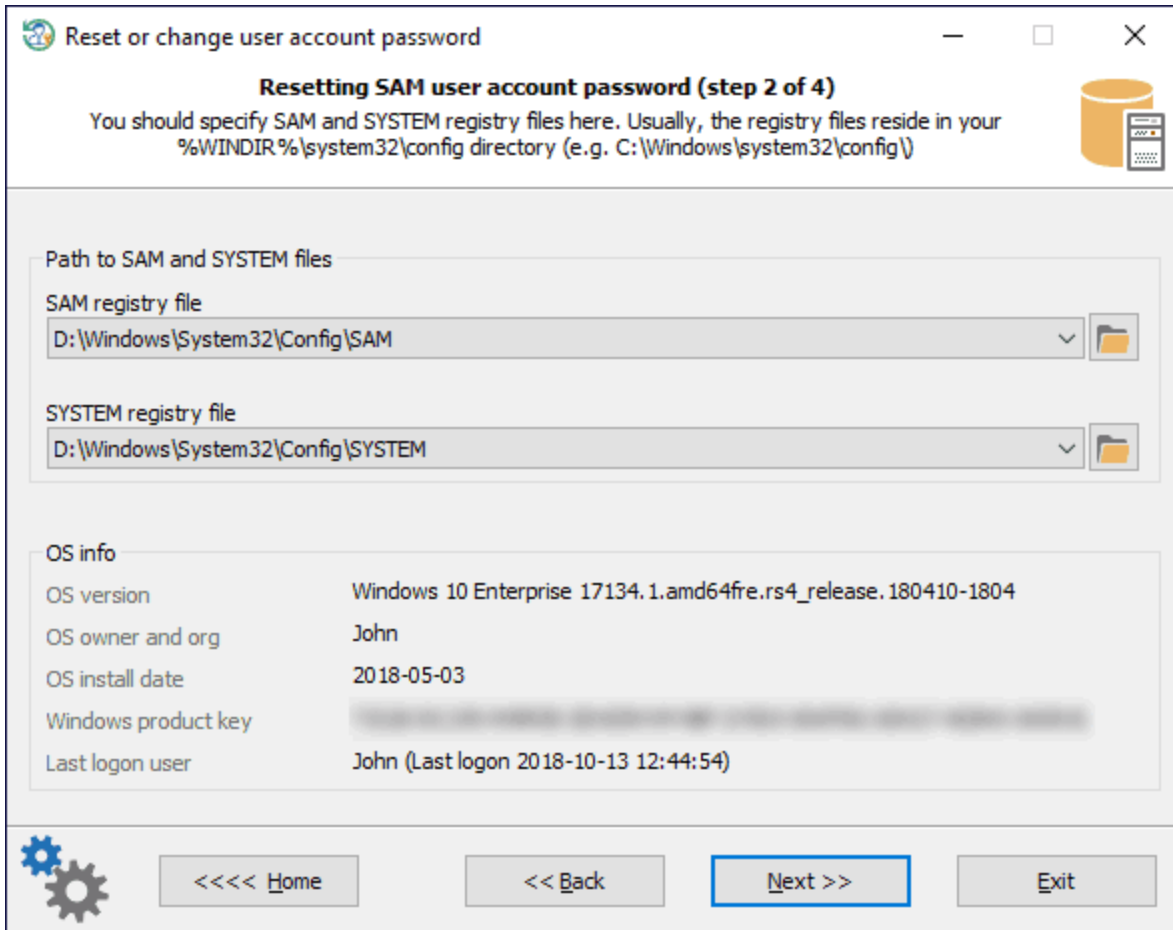


DCC



3.2

3.2.1



: SAM SYSTEM.

%WINDIR%\system32\config. %WINDIR% - Windows.

Active Directory,

SAM

Active Directory.

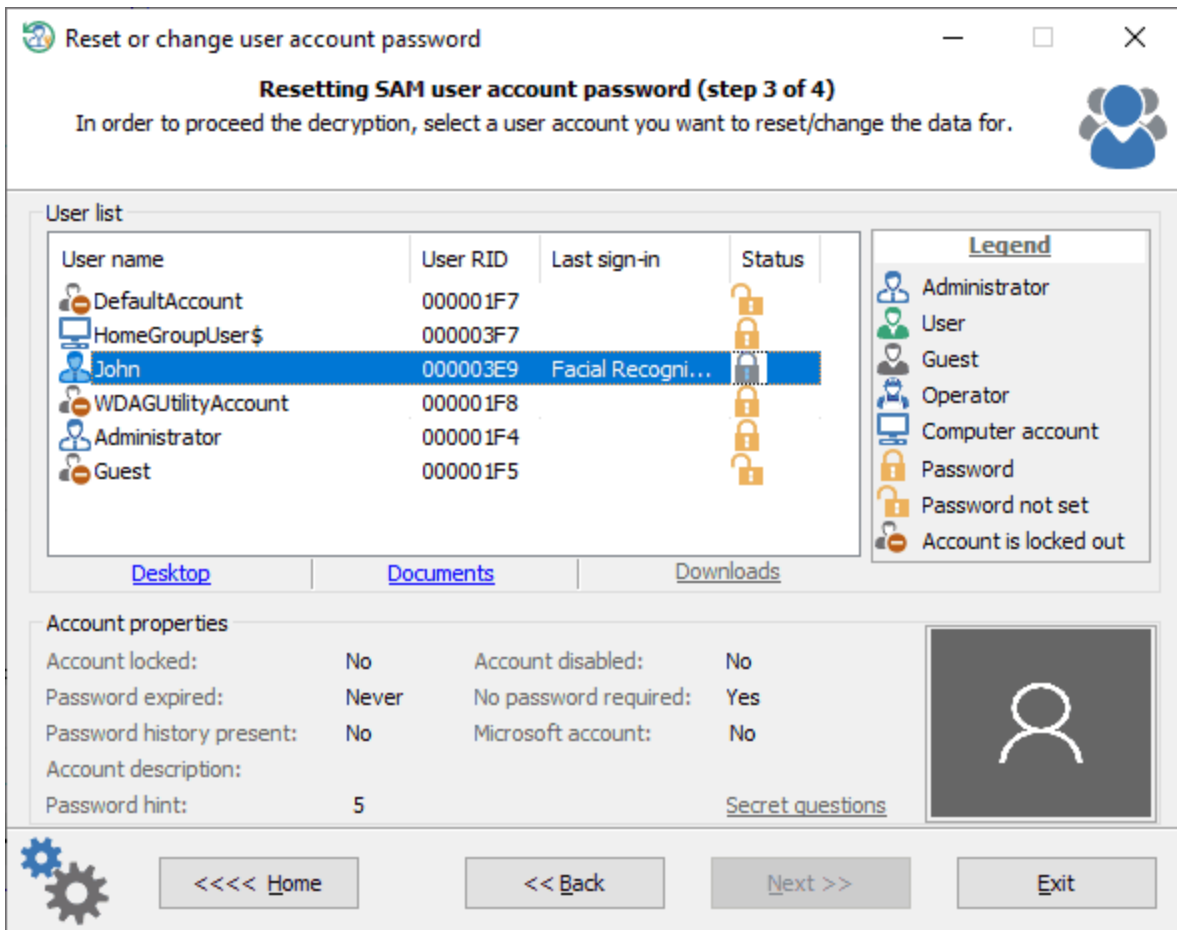
%WINDIR%\NTDS.

Active Directory

: C:\Windows\NTDS\ntds.dit

OS Info

Windows.



Windows 10 v17063

. Reset Windows 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	

<< RESET/CHANGE >>

 <<<< Home << Back Next >> Exit

()

Windows

Windows,

F8

Windows 8

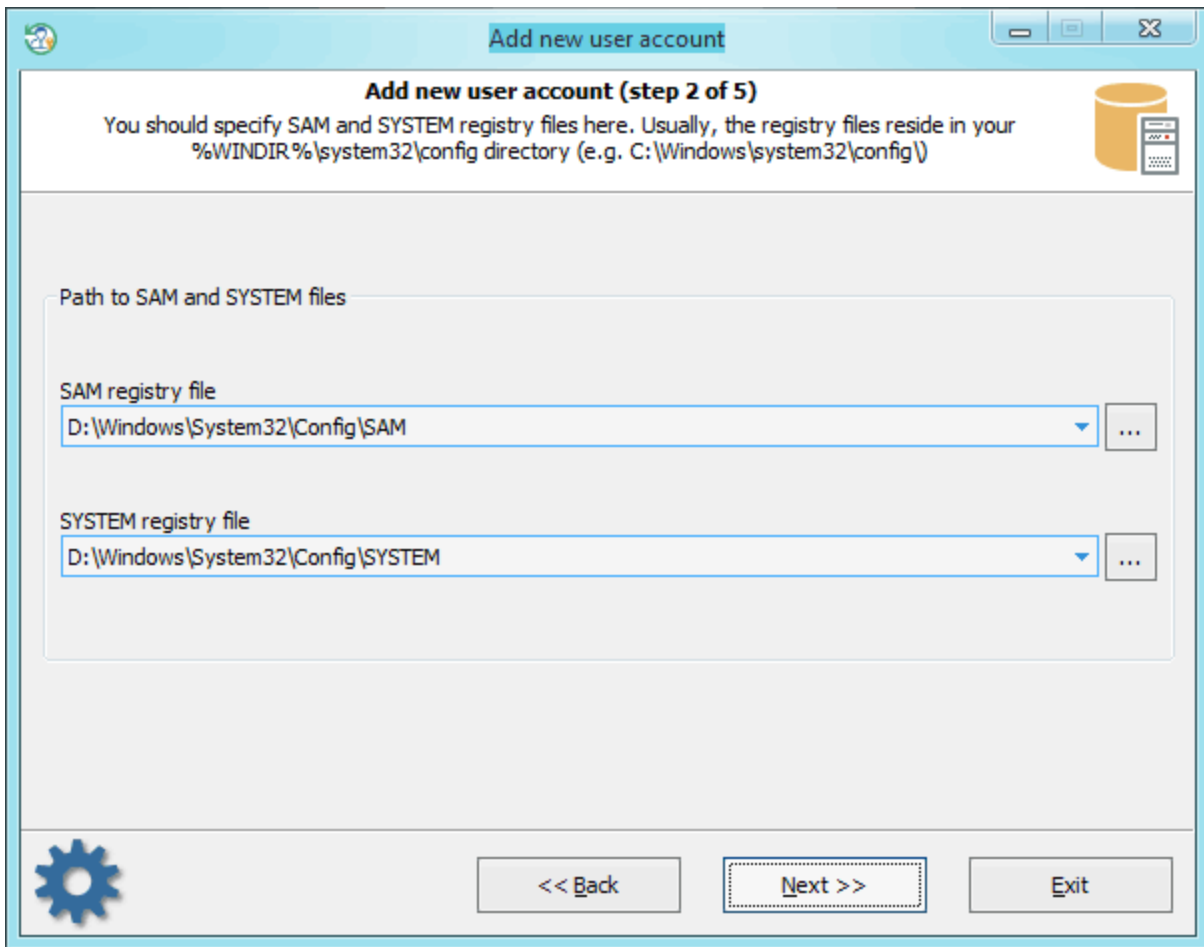
Shift

Microsoft,

3.2.2

3

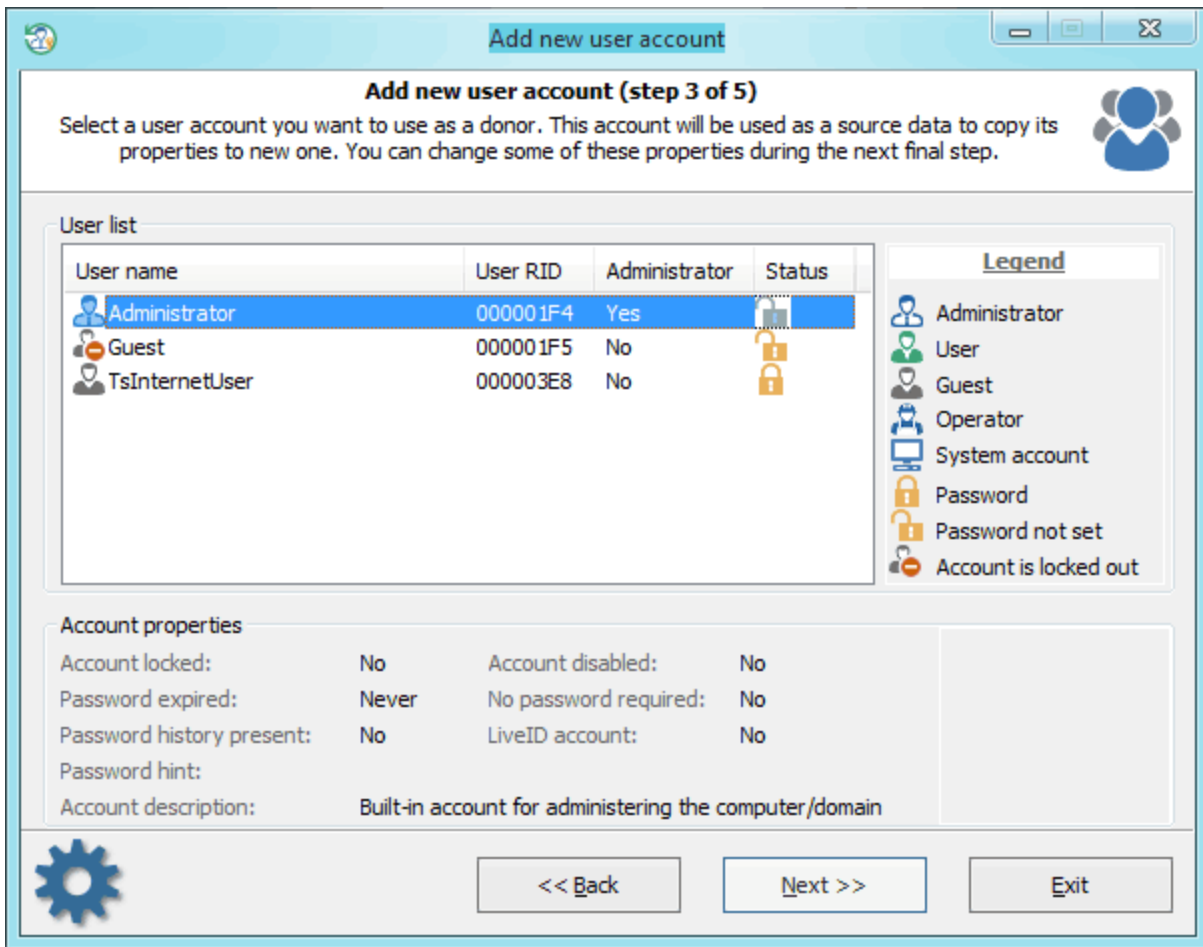
1.



SAM SYSTEM.

%WINDIR%\system32\config.

2.



Windows Password,

, Reset

3.

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

- Administrators
- Power Users
- Replicator
- Users

Not member of

- Backup Operators
- Guests

<< Create >>

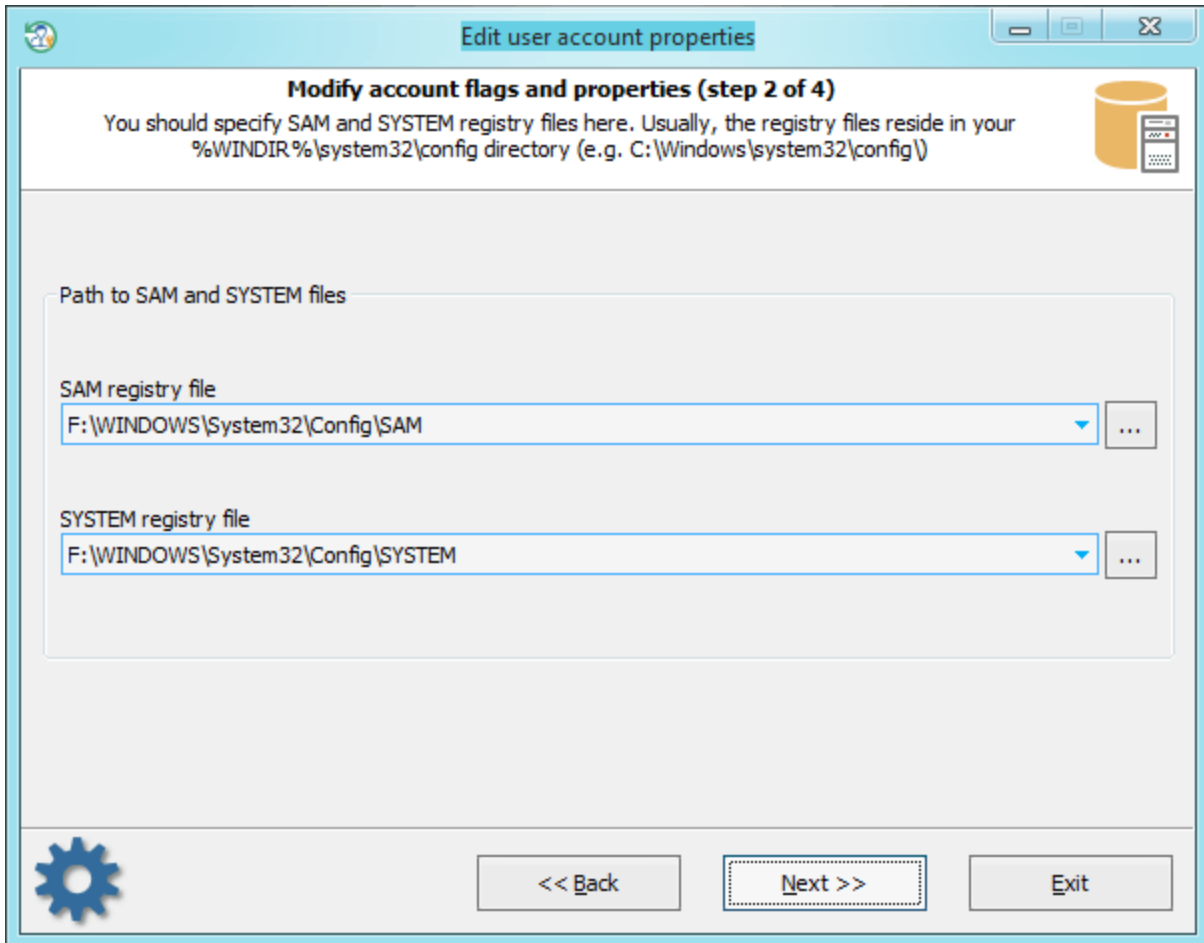
<< Back Next >> Exit

3.2.3

Reset Windows Password

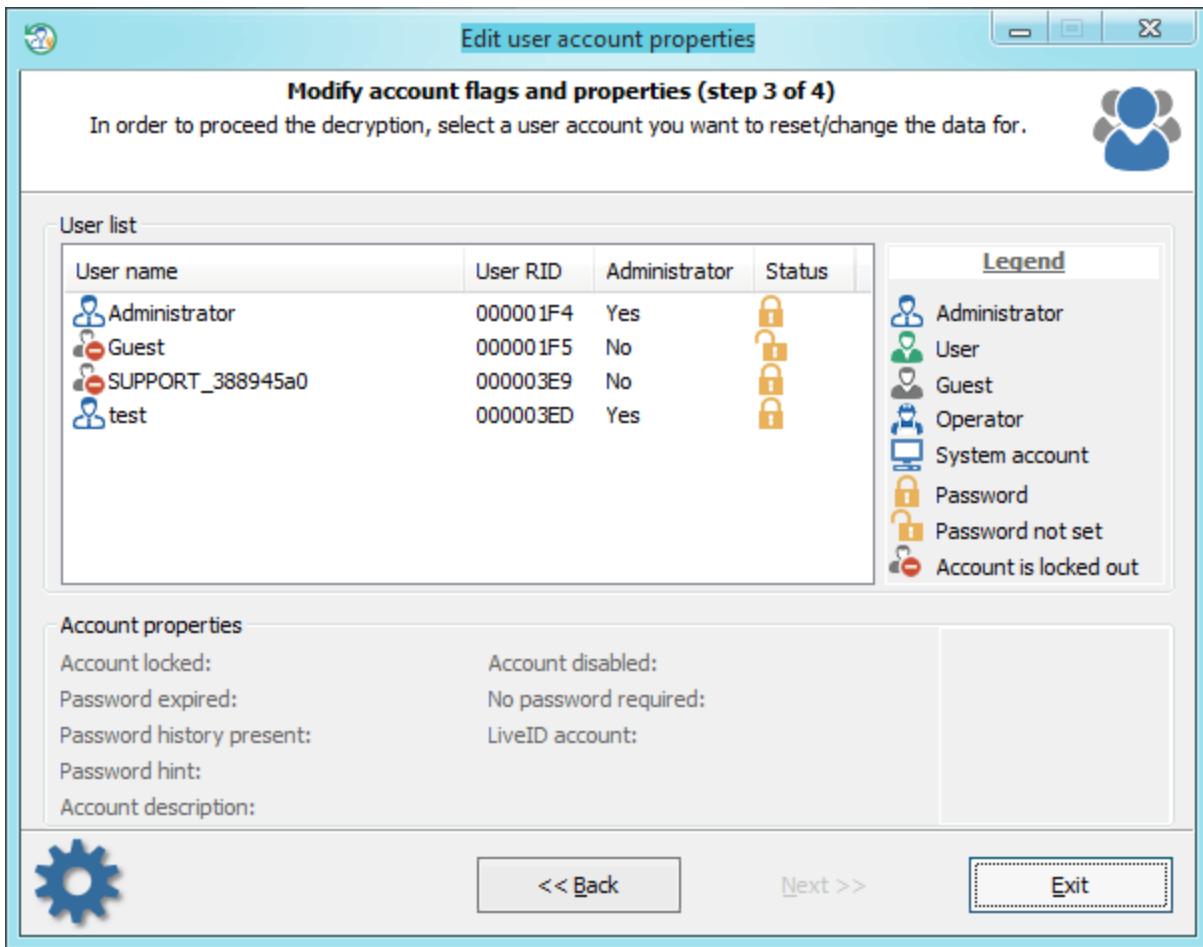
Microsoft
/

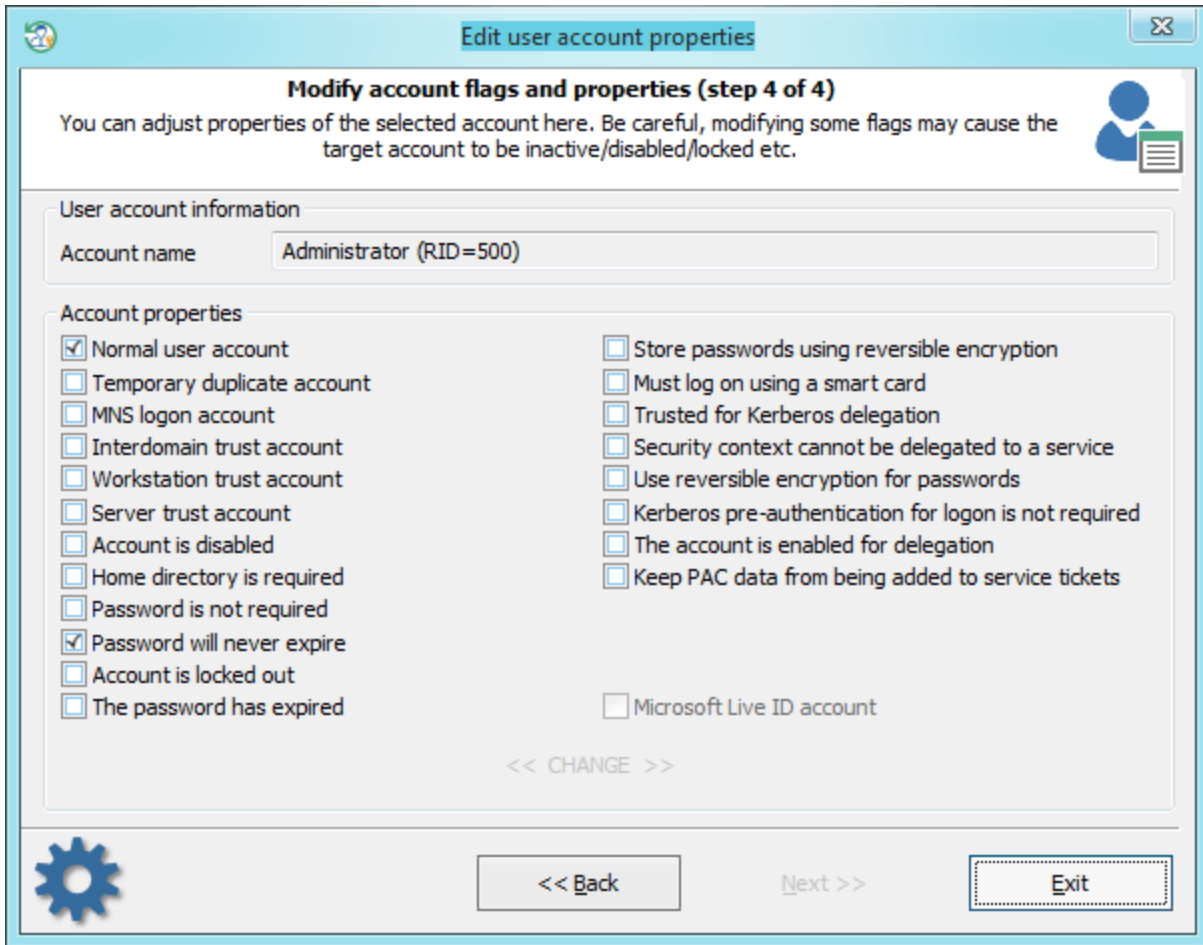
Smart-



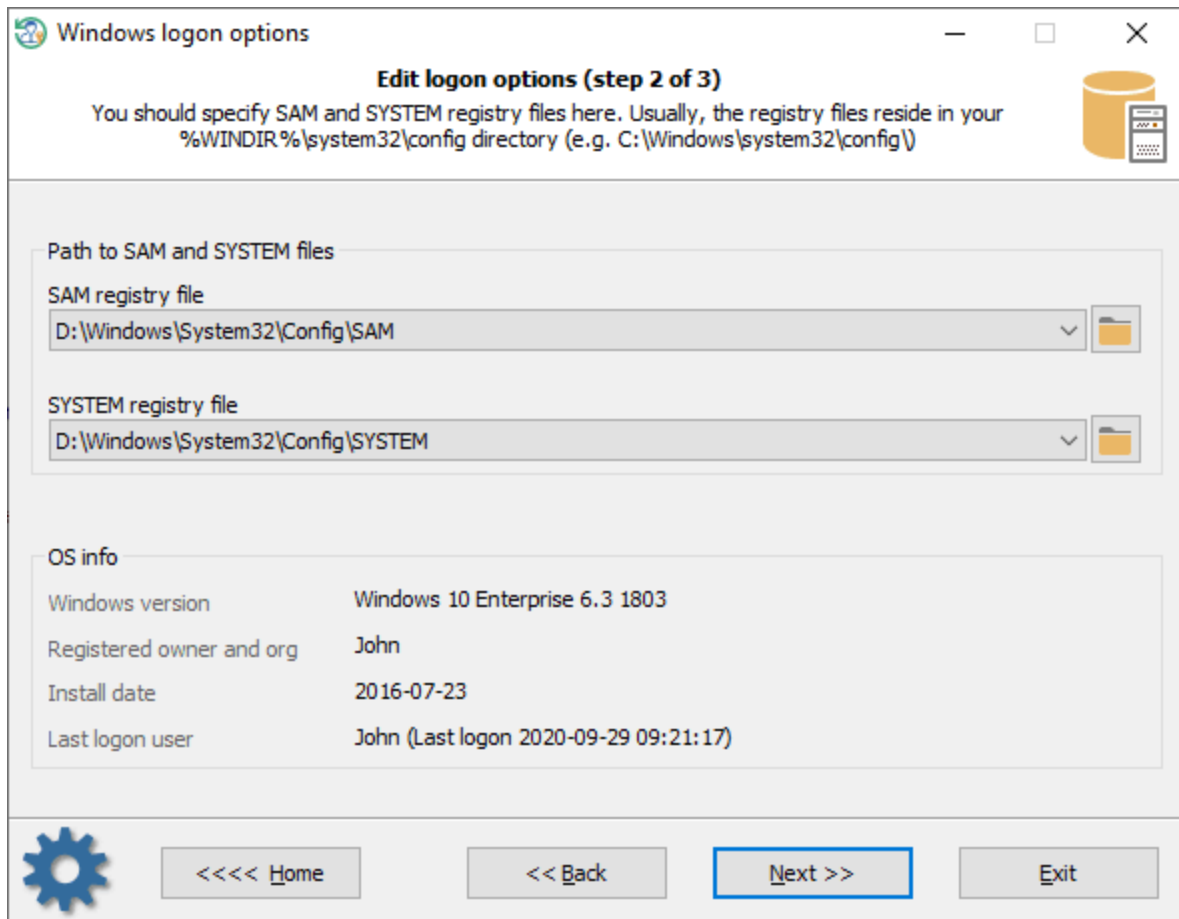
SAM SYSTEM ()
 NTDS.DIT SYSTEM (). RWP
 % WINDIR%\system32\config %WINDIR%\NTDS. %WINDIR% - Windows.
 Active Directory : C:\Windows\NTDS\ntds.dit

Windows

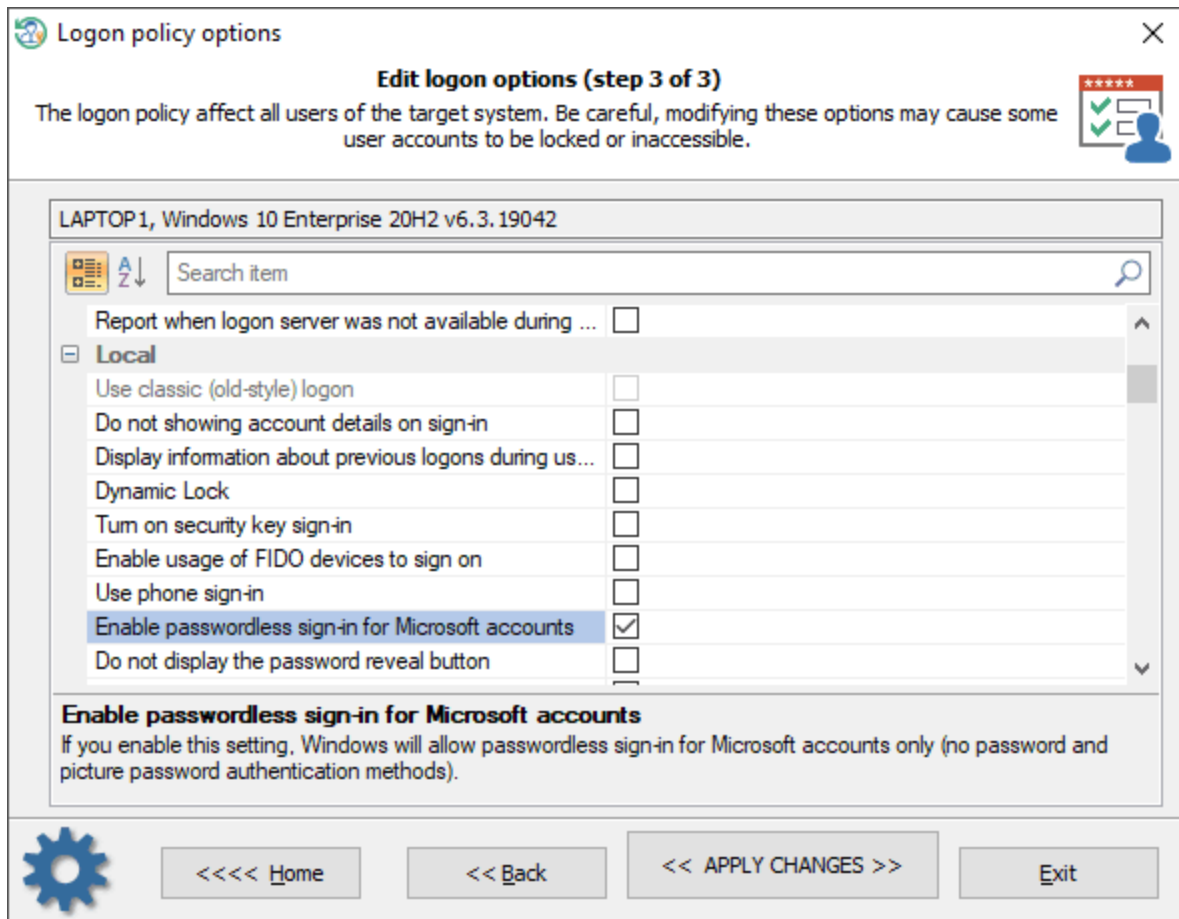




3.2.4



SAM SYSTEM



>>

<<

Domain:

EAS

(, , - Windows 10. IoT)

Windows Hello

(SAS).

Misc:

[Grey bar]

Windows.

» « « » Welcome « ».

Windows Windows

Windows

Vista, Windows XP Professional Windows 2000 Professional.

« » « »

Windows Hello

60

PIN:

PIN

(),

PIN-

1 730,

PIN-

PIN-

0.

PIN

PIN-

0 50 PIN-

PIN-

PIN-

, - 127.

PIN-

PIN-

, - 4.

, Windows

PIN-

, Windows

PIN-

, Windows

PIN-

, Windows

PIN-

Windows Hello:

Windows

Windows Hello

, Windows

Windows Hello

XML-

, Windows Hello

Windows Hello

1.2 2.0.

Windows Hello

: TPM 1.2

TPM1.2

, Windows Hello

Windows Hello

PIN-

Windows Hello
PIN-

Windows Hello

Windows

Hello

Windows

Hello

Windows Hello

Windows Hello

Windows Hello

Windows Hello

Windows Hello

TPM:

TMP,

Windows

TPM, TPM, TPM, TPM, TPM

Windows 10 1607 Windows, 2.0 Windows 10 1607 2.0.

Windows TPM

Windows TPM

(TPM). (TPM) 4.

(TPM),

480 (8).

(TPM).

(TPM)

9.

Directory (1	2)	TPM Active	2 Windows	()	AD DS
--------------	----	------------	-----------	-----	-------

Directory (2	2)	TPM Active	2 Windows	()	AD DS
--------------	----	------------	-----------	-----	-------

Local security:



DOS,

SACL;

(SACL).

SACL.


```

:
,
.
'
. 1- , 2-
:
( API ),
Windows (WHQL).
: 0- , 1-
2 -
:
AT.
LDAP- LDAP. LDAP
:
30
:
( )
:
(
)
:
(
)
:
"
"
30
:
128-
(Windows 2000
)
:
Windows.
:
CTRL+ALT+DEL CTRL+ALT+DEL

```

Microsoft Network: (SMB) SMB

SMB

Microsoft Network: (), SMB (Server Message Block)

SMB.

Microsoft network server: SMB.

: (SMB) Microsoft,

() Windows. "" SMB SMB

"" SMB.

SMB.

Microsoft network server: SMB SMB

: SMB (SMB)

() Microsoft, Windows. "" SMB

"" SMB.

SMB SMB,

SMB SMB,

Microsoft network server: Server Message Block (SMB).

Microsoft network server: (SMB)

SPN Windows. SMB

SPN SMB SMB,

SMB SMB, SMB1, SMB2.

: Windows

SAM

: SAM Windows

SAM

:					.NET
:					
:				()	
:					
:			(ACL)		winreg.
:				(ACL)	winreg.
:					
:				« »	
:				« »	
:	LAN Manager	LM		LAN Manager (LM)	Windows NT.
:	LAN Manager				
:		LDAP			LDAP BIND.
:			128 /		NTLMv2.
(RPC)	NTLMSSP	Manager.			LAN
:			128 /		NTLMv2.
	NTLMSSP	Manager.			LAN

(RPC)	:	:	:	:
NTLM:	NTLM	NTLM	NTLM	Windows 7
NTLM:	NTLM	Windows.	Windows Server 2008 R2	
NTLM:	NTLM	NTLM.		
NTLM:	NTLM	NTLM.		
NTLM:	NTLM			
NTLM:	NTLM			NTLM
NTLM:	NTLM			
NTLM:	NTLM	NTLM,		
NTLM:	NTLM	NTLM,		
NTLM:	NTLM	NTLM		
NTLM:	NTLM	NTLM		
NTLM:	NTLM	NTLM		LocalSystem.
NULL- LocalSystem				
PKU2U	Windows 7.			
Kerberos		Kerberos		
			SET	
	Windows.			

Windows.

:

:

Schannel (SSP)
Secure Sockets Layer (SSL)
Transport Layer Security (TLS)

FIPS ()
Transport Layer Security/Secure Sockets Layer (TLS/SSL)
FIPS 140: 3DES AES

, RSA ECC
TLS, Secure Hashing Algorithm (SHA1,
SHA256, SHA384 SHA512) TLS.

:

:

(SID)

:

Win32

, POSIX.

Windows,
Windows

:

(DACL)

()

:

:

.exe.

Windows

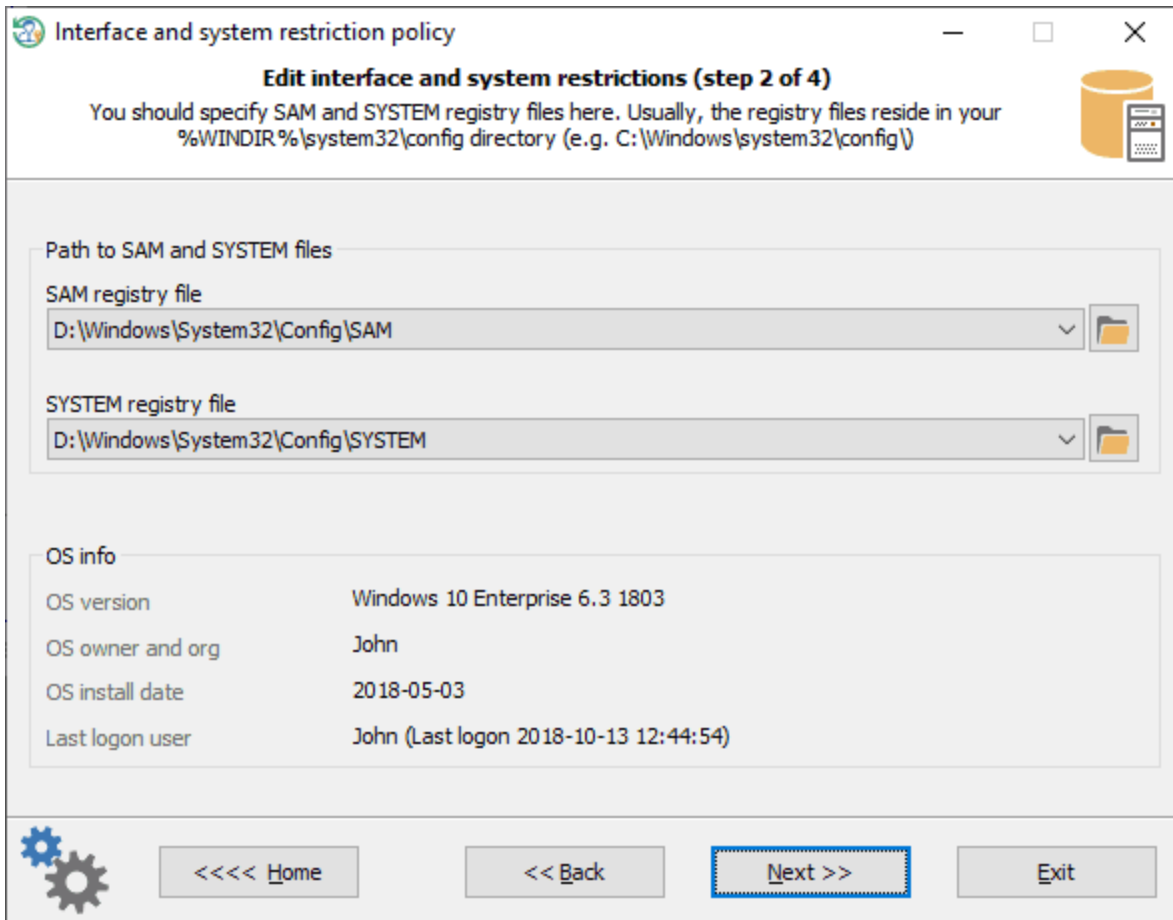
, Authenticode,
,

:

UIA,

Windows,

3.2.5





SAM SYSTEM

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	

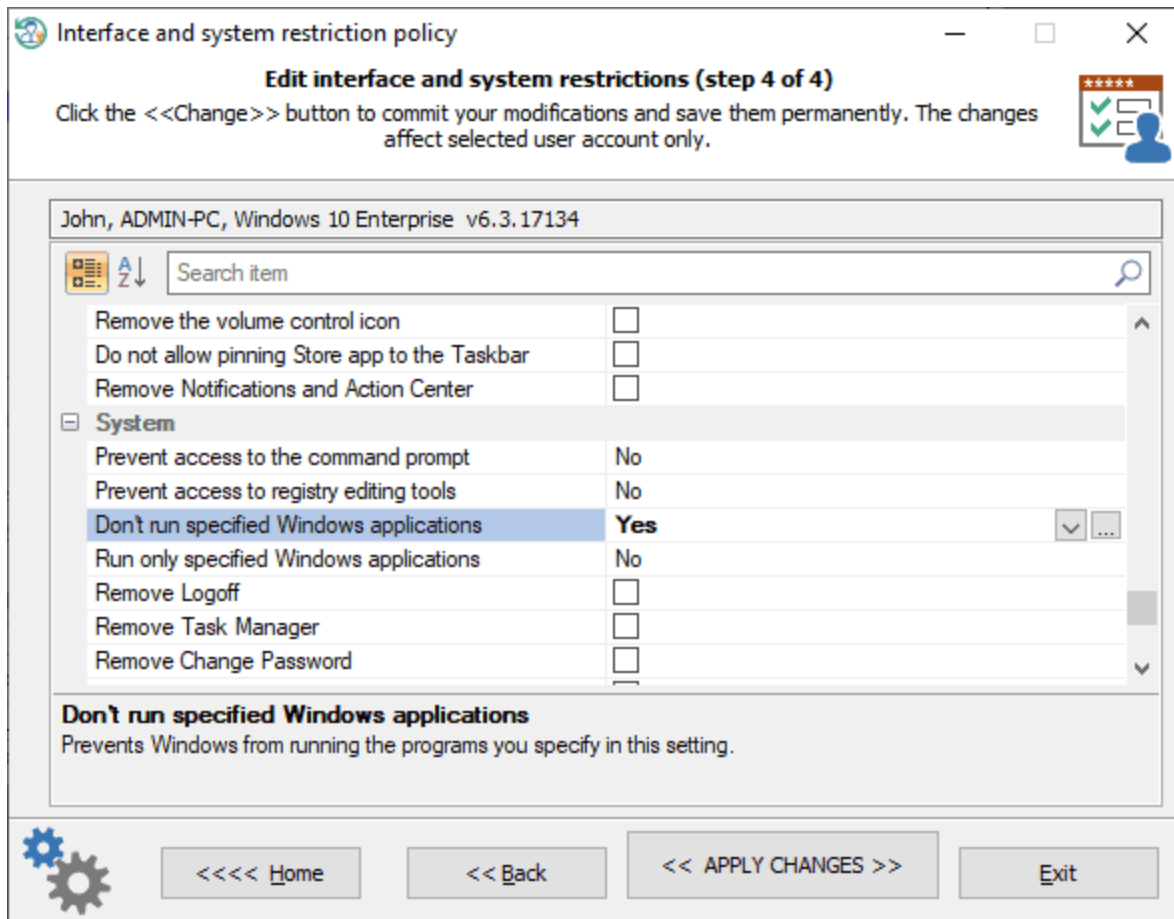
Legend

-  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:			


<<<< Home
<< Back
Next >>
Exit



>>

<<

Control panel:

control.exe.

```

control.exe.
"
"
control.exe.
Control.exe
SystemSettings.exe,
URI-
: showonly:about,bluetooth hide:bluetooth
( Windows 8),
( Windows Vista
Windows 7),

```


" " " " " "

" " " " " "

" " " " " "

Active Directory " "

Directory

" " " " " "

Active Desktop Active Desktop

Active Desktop Active Desktop

Active Desktop

Active Desktop.

Desktop. Active

Active Desktop.

Active Desktop.

Active Desktop.

Active Desktop.

Active Desktop.

Active Desktop Active Desktop

Active Desktop.

Network:

' (")

' (")

' (")

' (")

' (")

' (")

' (")

' (")

' (")

' (")

Windows 2000 Server

Windows 2000

/ ()

/ (

"),

Windows

Windows Connect Now

(WCN).

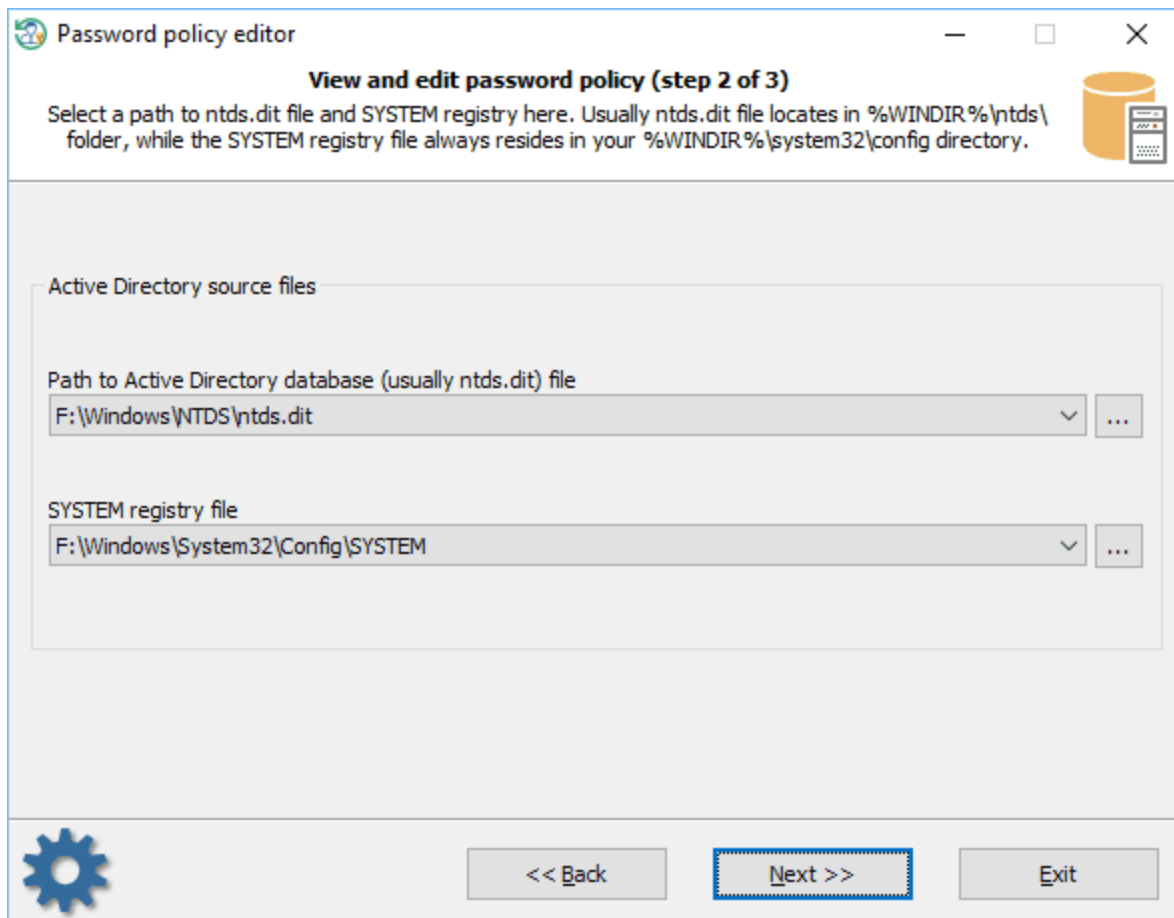
Windows Connect Now

Start menu and taskbar:

:	USB-	,
:	.	.
:	.	.

3.2.6

Windows.



- SAM SYSTEM,
- NTDS.DIT SYSTEM,

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

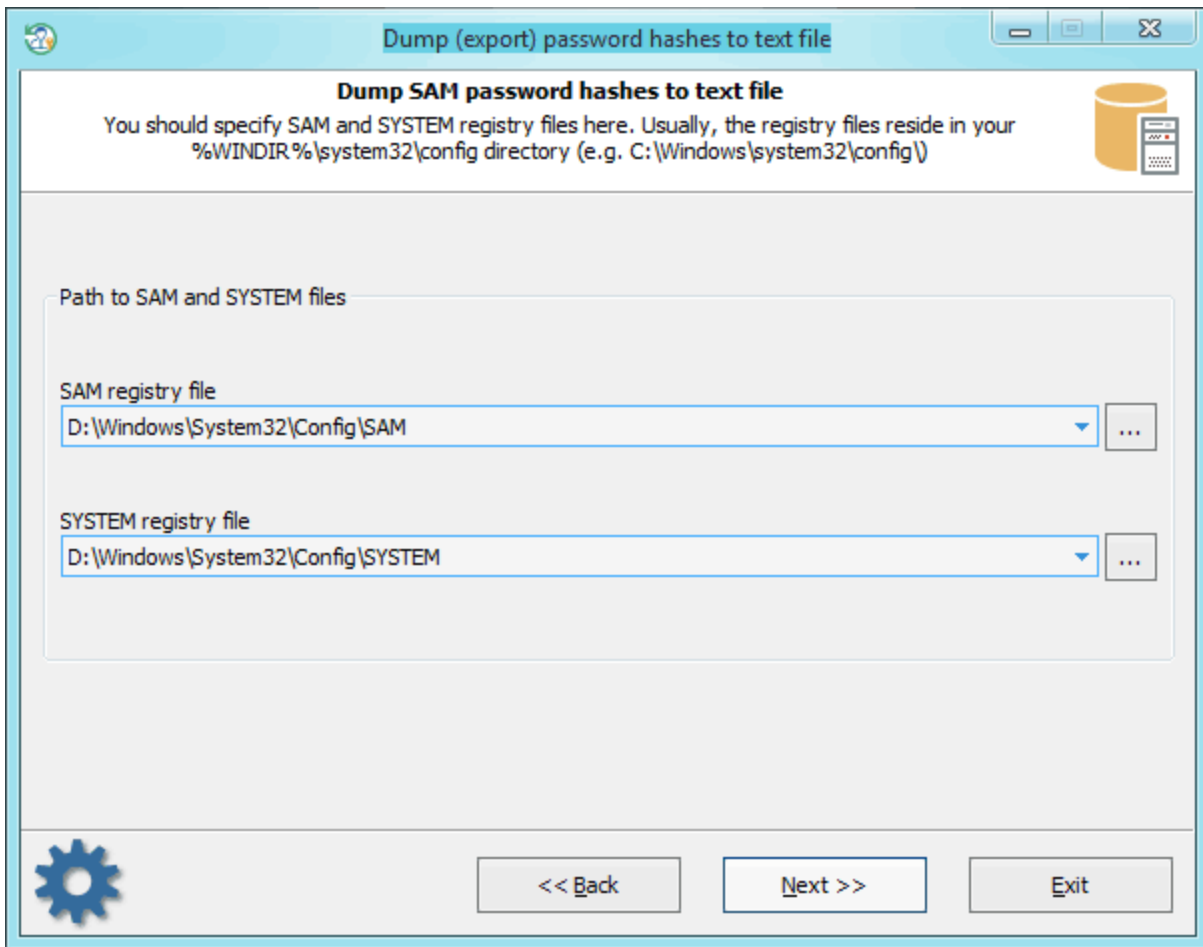
<< APPLY CHANGES >>

Home <<<< << Back Next >> Exit

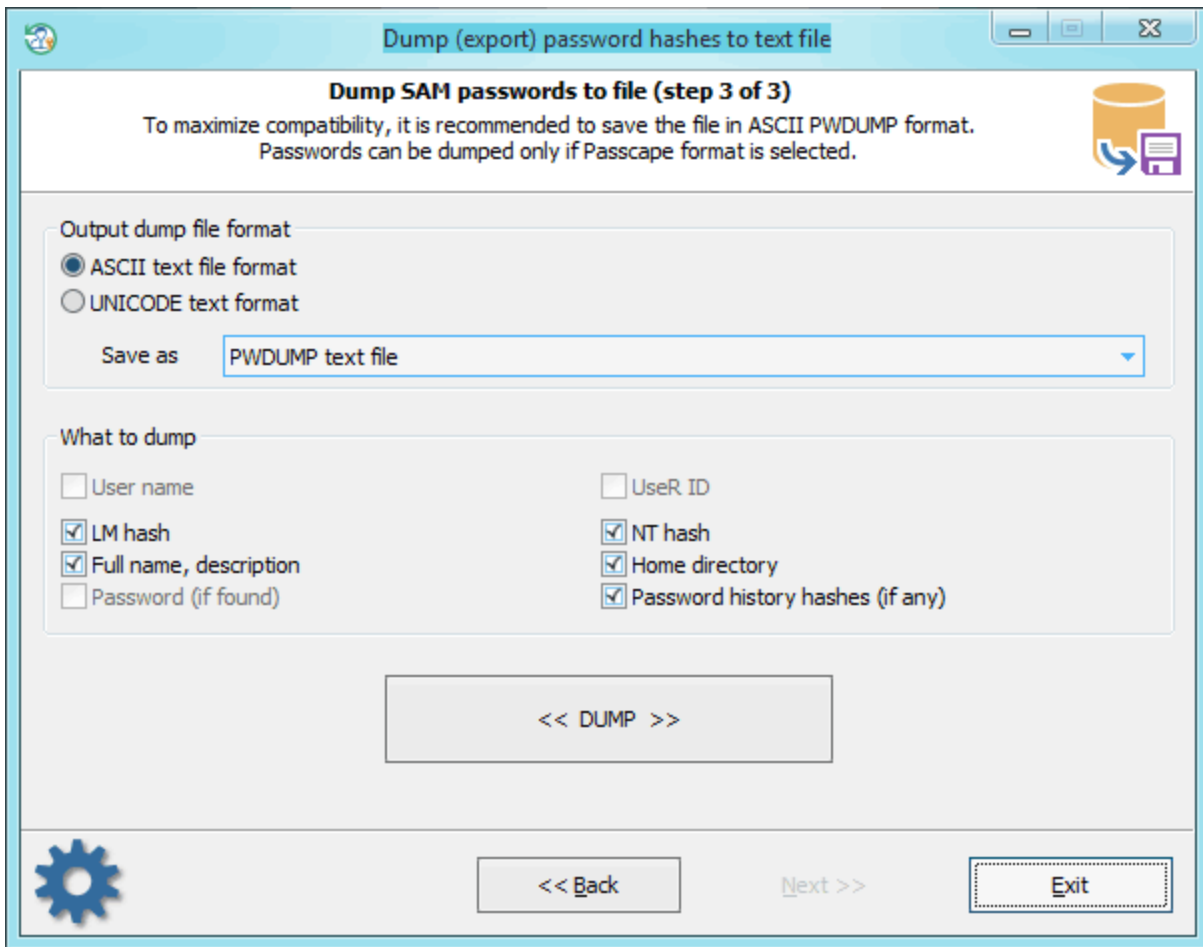
- Minimum password length -
- Password history length -
- Maximum password age - () 0 25.
- Minimum password age - (), 1 999
- Password must meet complexity requirements -

- 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 -
- LM LAN Manager SAM (Windows Vista Active Directory)
- Windows!

3.2.7 ()



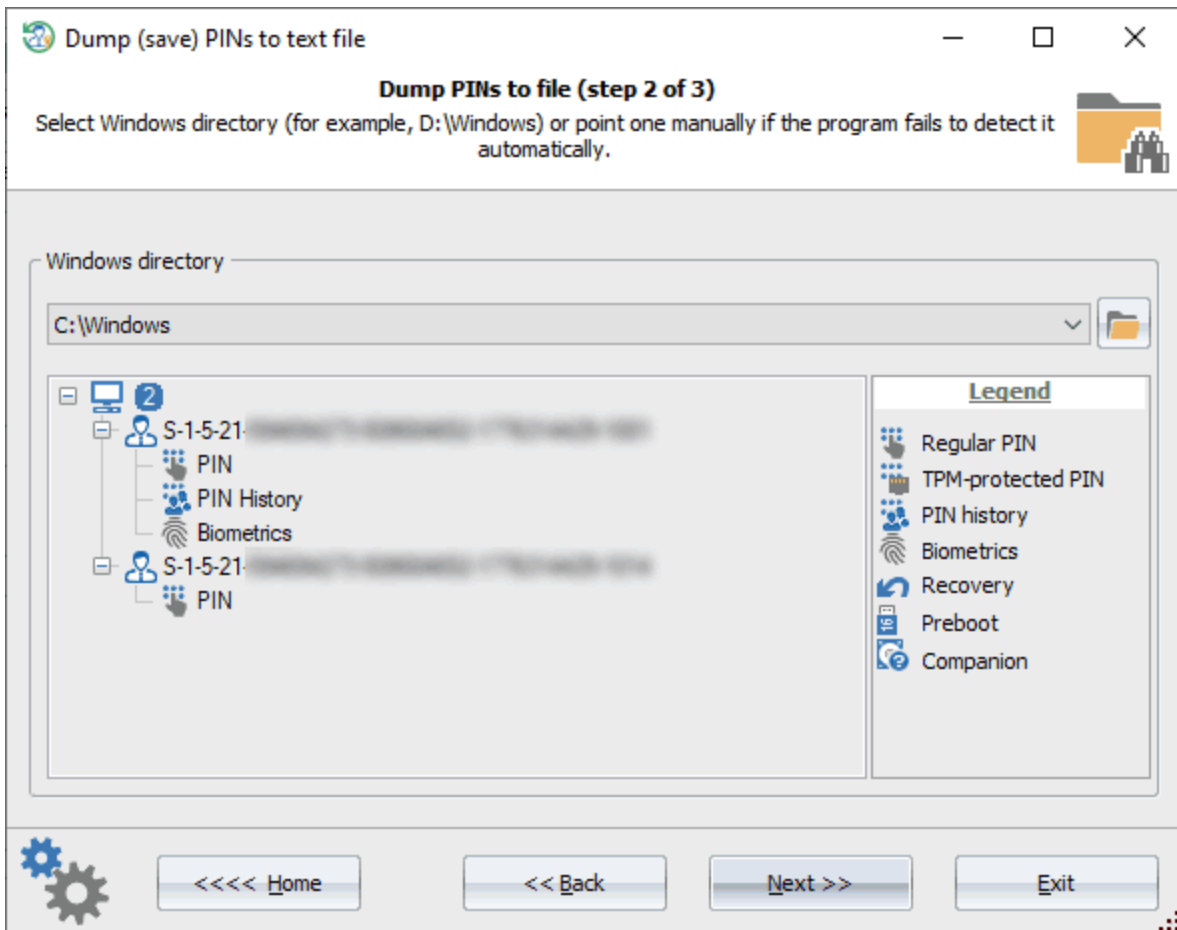
, ntds.dit SYSTEM. SAM SYSTEM . ,



plaintext, Passcape, 'Store passwords using reversible encryption for all users in the domain', Reset Windows Password, AI attack, Passcape Software,

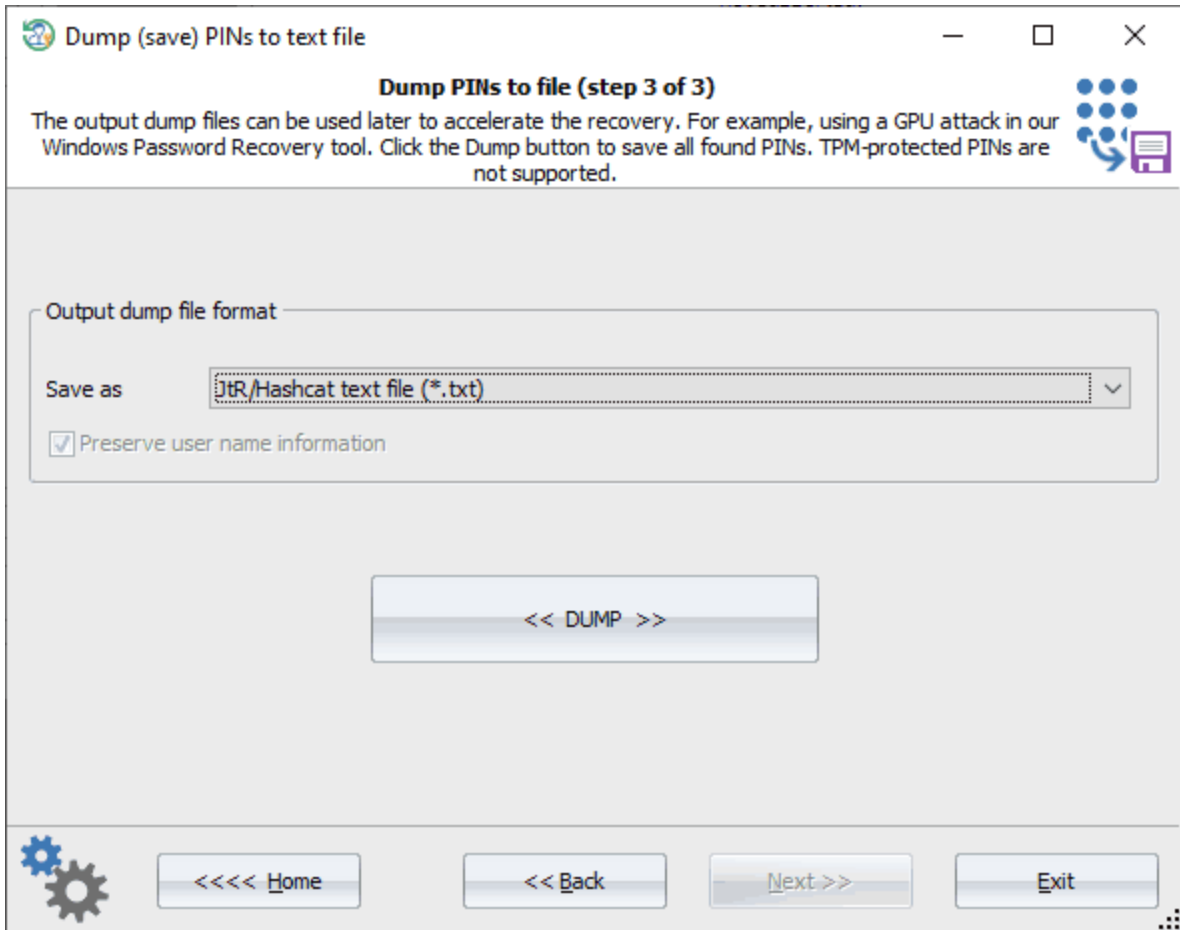
3.2.8 () PIN

Windows



Windows,
PIN-

Windows PIN



PIN

Windows

hashcat (*.txt)

Elcomsoft (*.pin).

GPU

[Windows Password Recovery](#)

3.2.9

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
 Directory Service Restore Mode password
 Active Directory password
 Domain Cached Credentials
 Password policy


[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

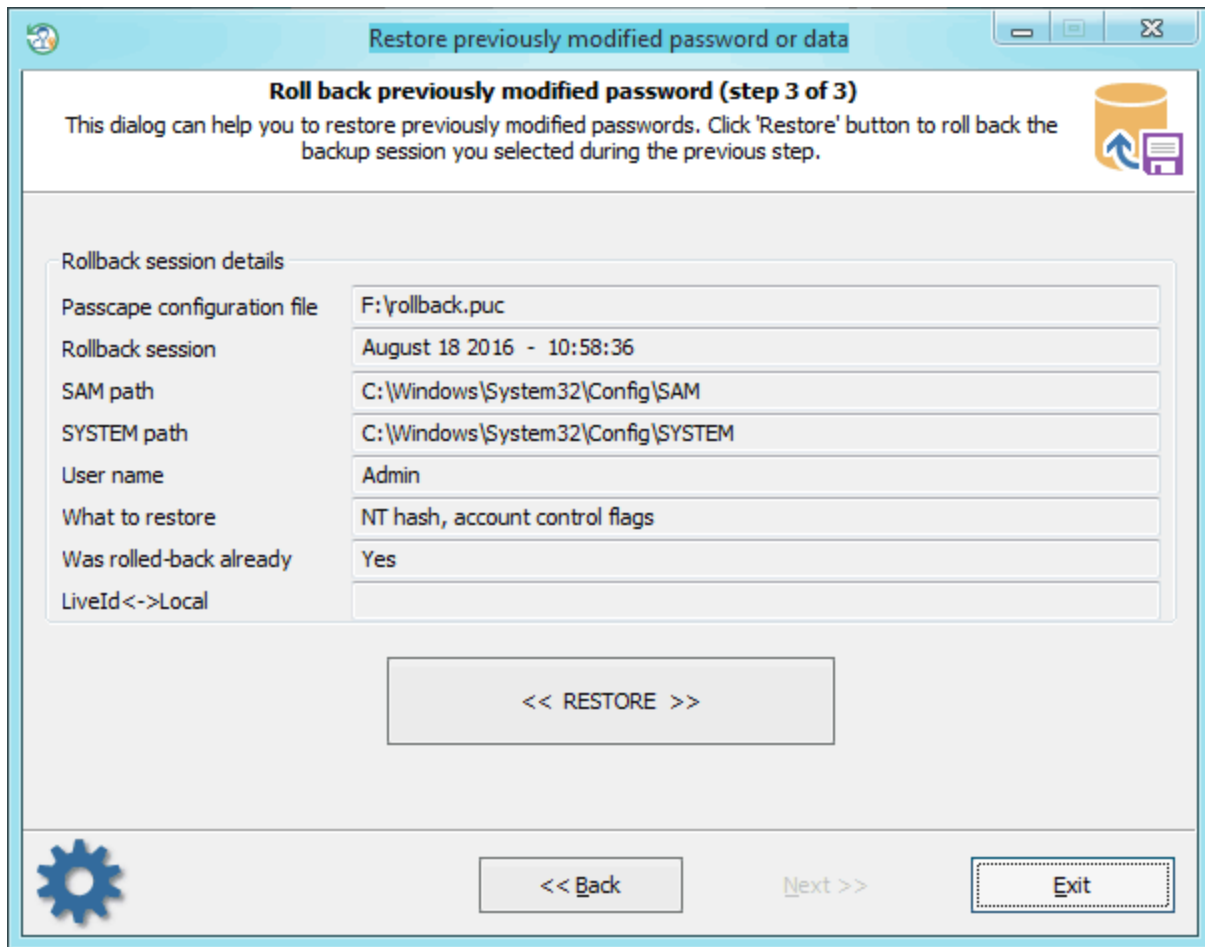


Rollback sessions are stored in *.puc files and ordered by date/time.

Rollback session details

SAM path, SYSTEM path, User name, Rollback data type

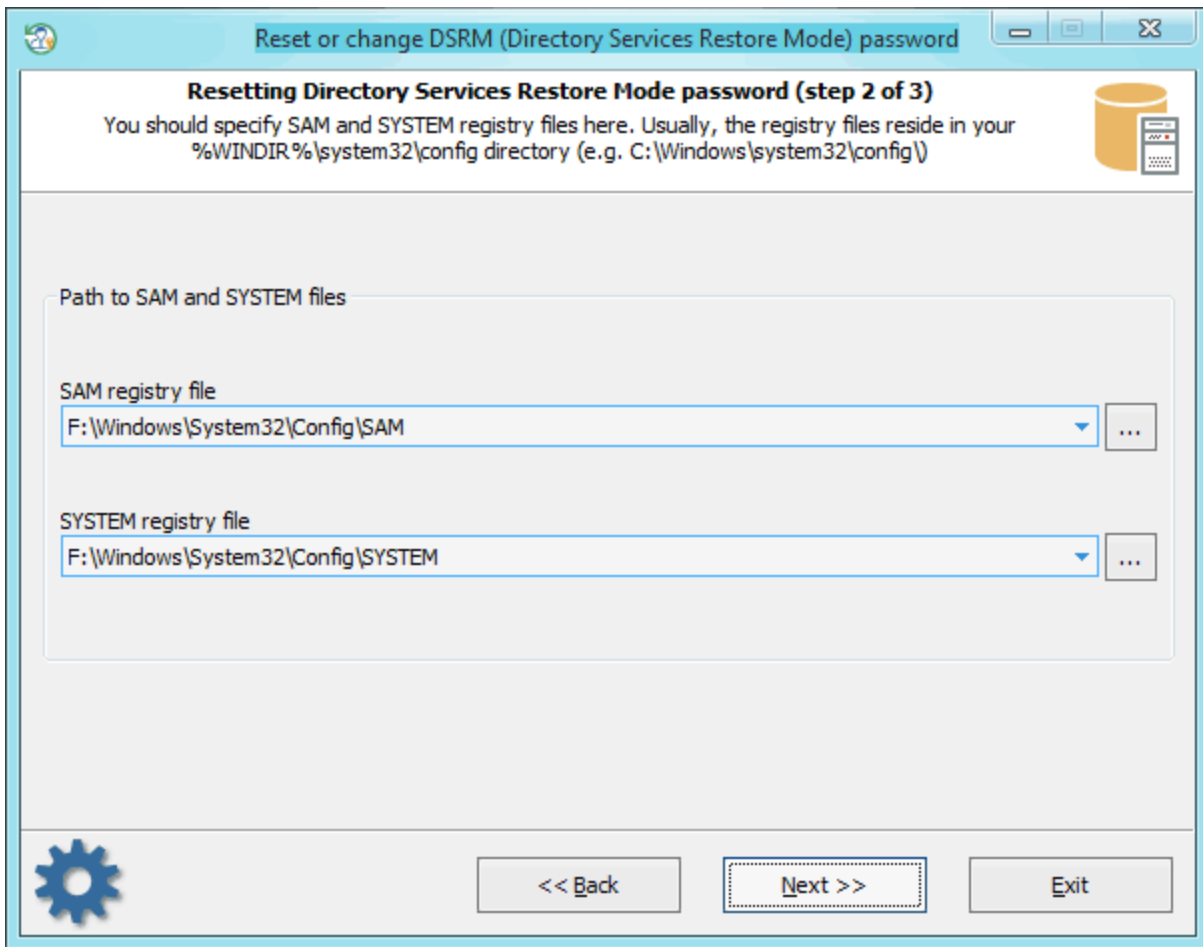
SAM, Active Directory, DSRM



-
-
-

Windows

- Reset Windows Password, *.puc (
- Reset Windows Password Windows.
- Reset Windows Password.

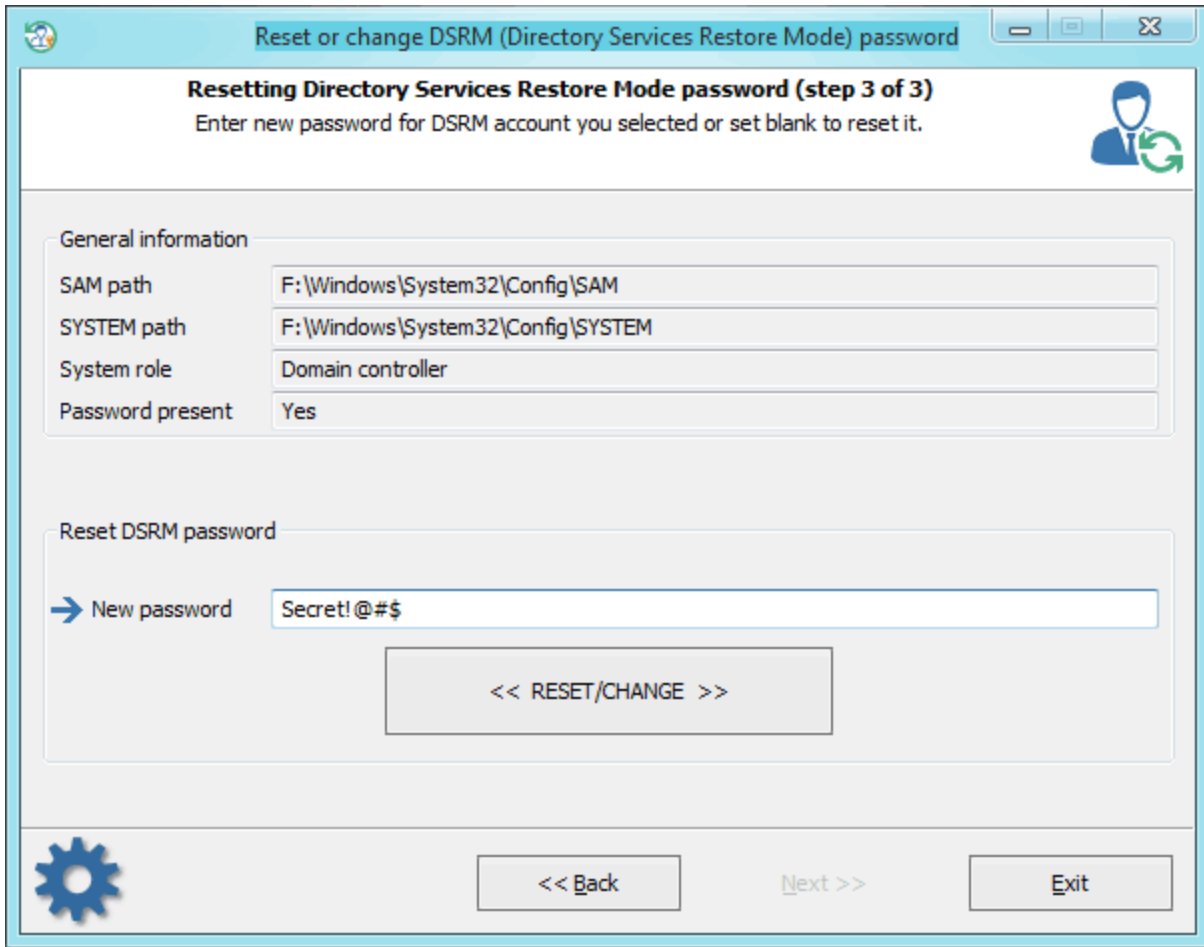


Directory Service Restore Mode

SYSTEM.

C:\Windows\system32\config.

: SAM



'RESET/CHANGE' ()

DSRM.

3.3.2

BitLocker

BitLocker

BitLocker

Active Directory.

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

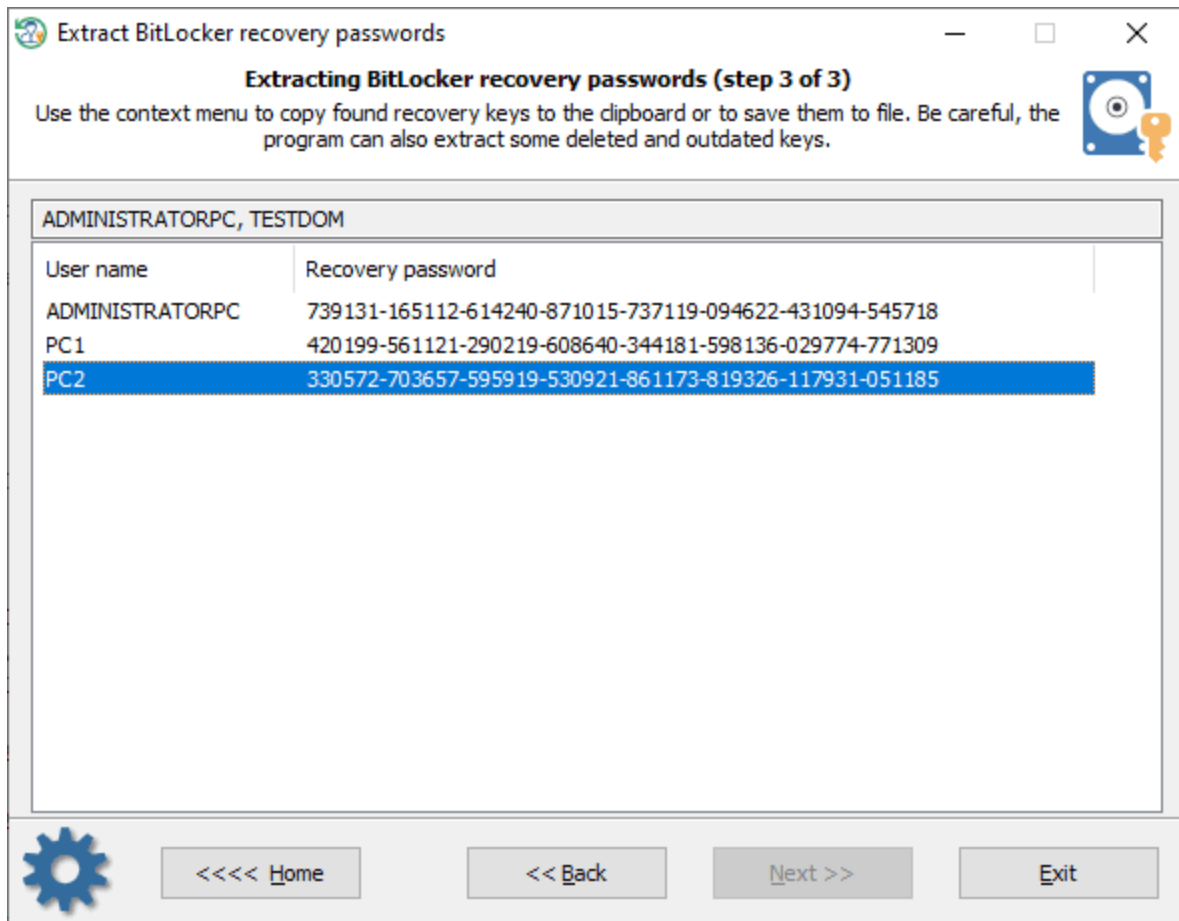
Settings icon:

<<<< Home << Back **Next >>** Exit

SYSTEM

NTDS.DIT.

BitLocker



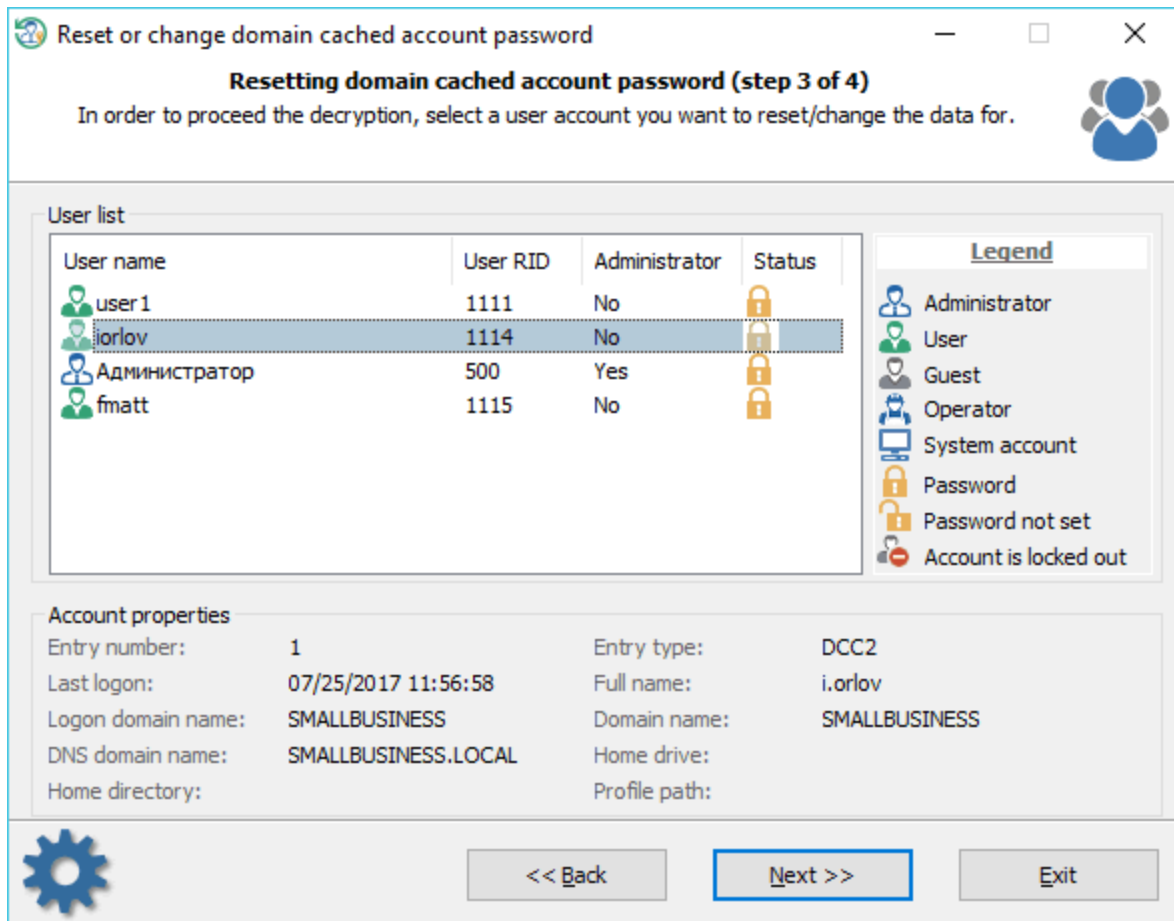
BitLocker.

3.4

3.4.1

Windows,

Reset Windows 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

Change passwords for all cached entries of this user account

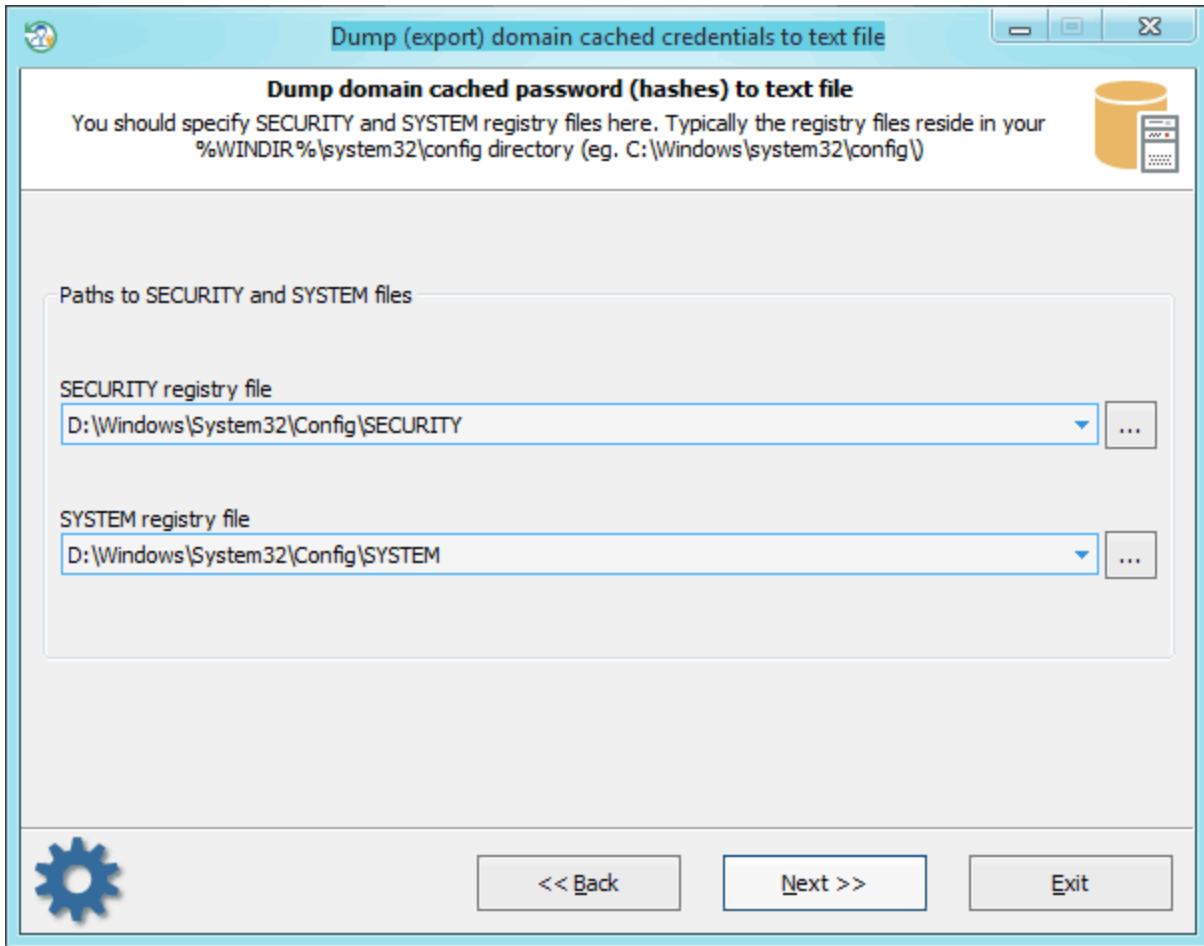
<< RESET/CHANGE >>

<< Back Next >> Exit

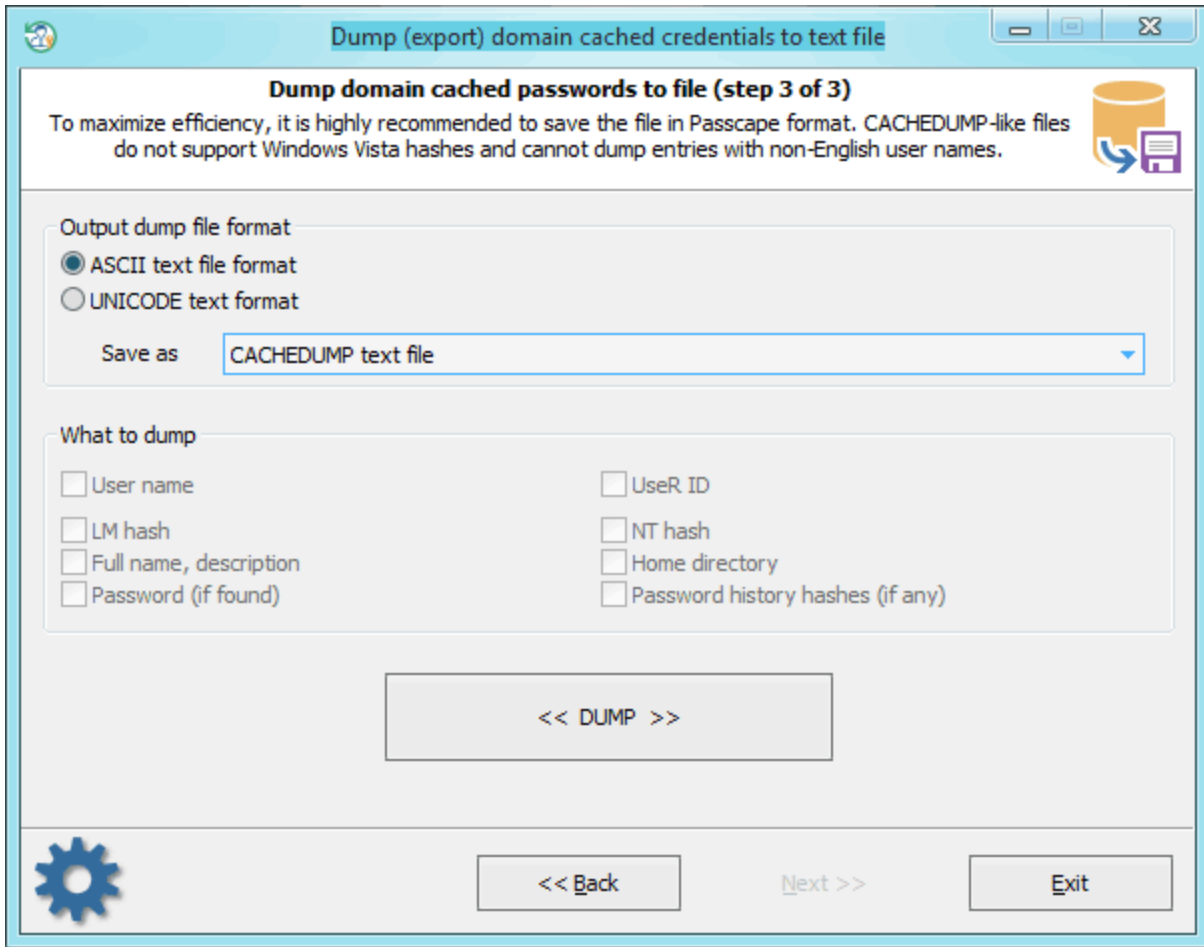
RID.

, Windows

3.4.2 ()

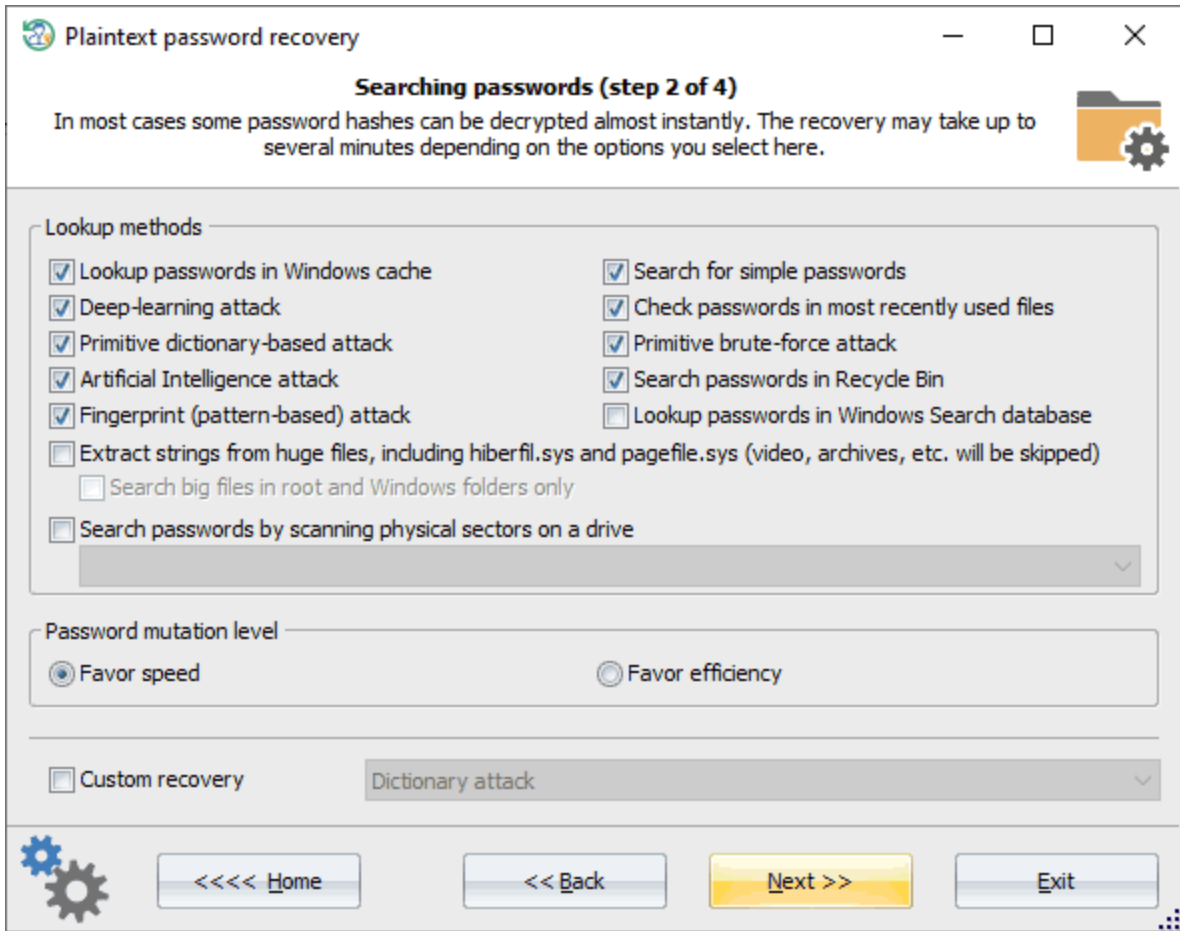


: SECURITY SYSTEM.



. ASCII , . UNICODE
 , ,
 .
 - - CACHEDUMP - , .
 , . , . , .
 CACHEDUMP , . Windows Vista .
 Passcape , . [Network Password Recovery Wizard](#).

3.5.1



11 :

1. Windows.
 DSL, VPN, FTP, IM, sticky notes,
 Windows, Windows Search . . .
 Windows Search, ()
[ESE Explorer](#)
 Windows Search
2. , , . . .
3. , , . . .
4. Passcape, . . .
5. , . . . Light Standard
 (, ,) Advanced Edition.

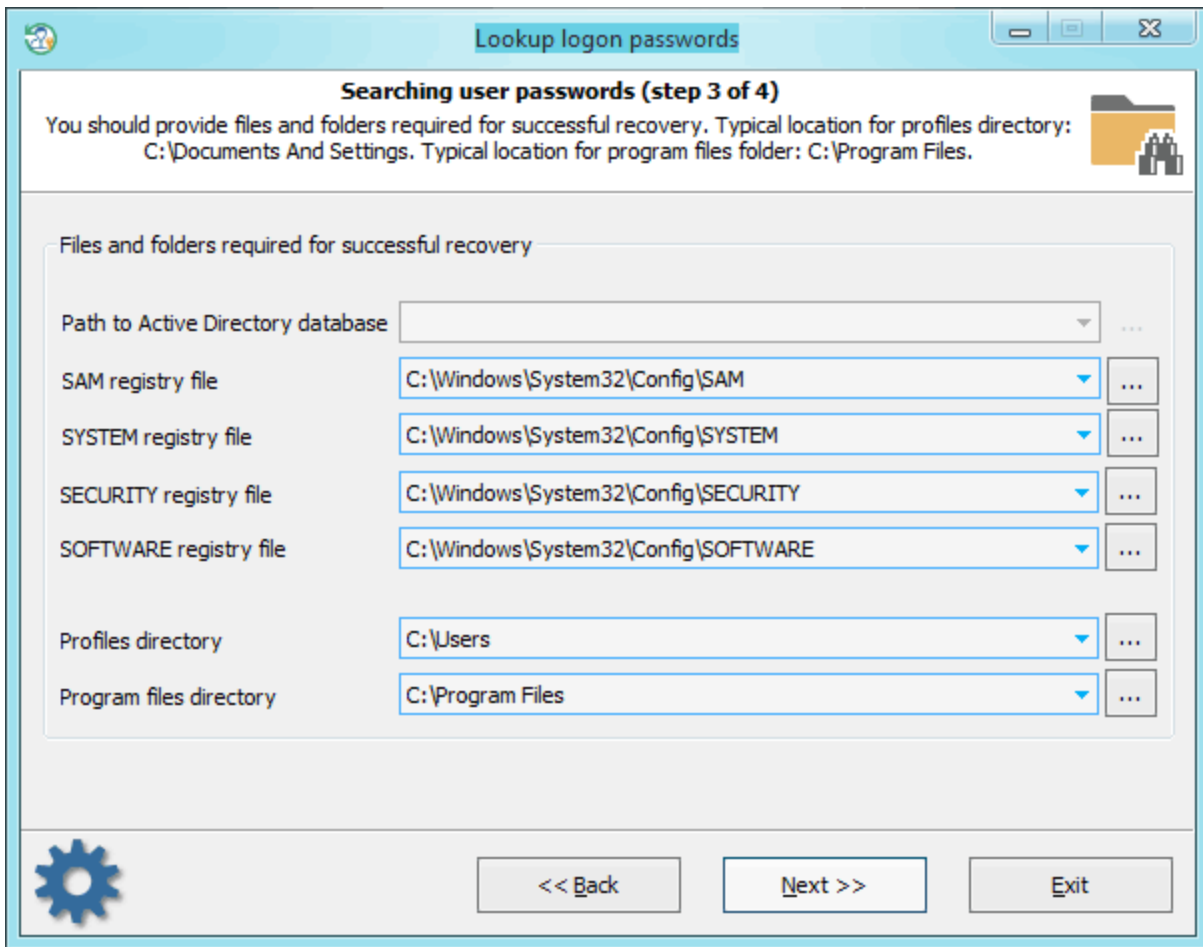
6.
7.

8.
9.
10.

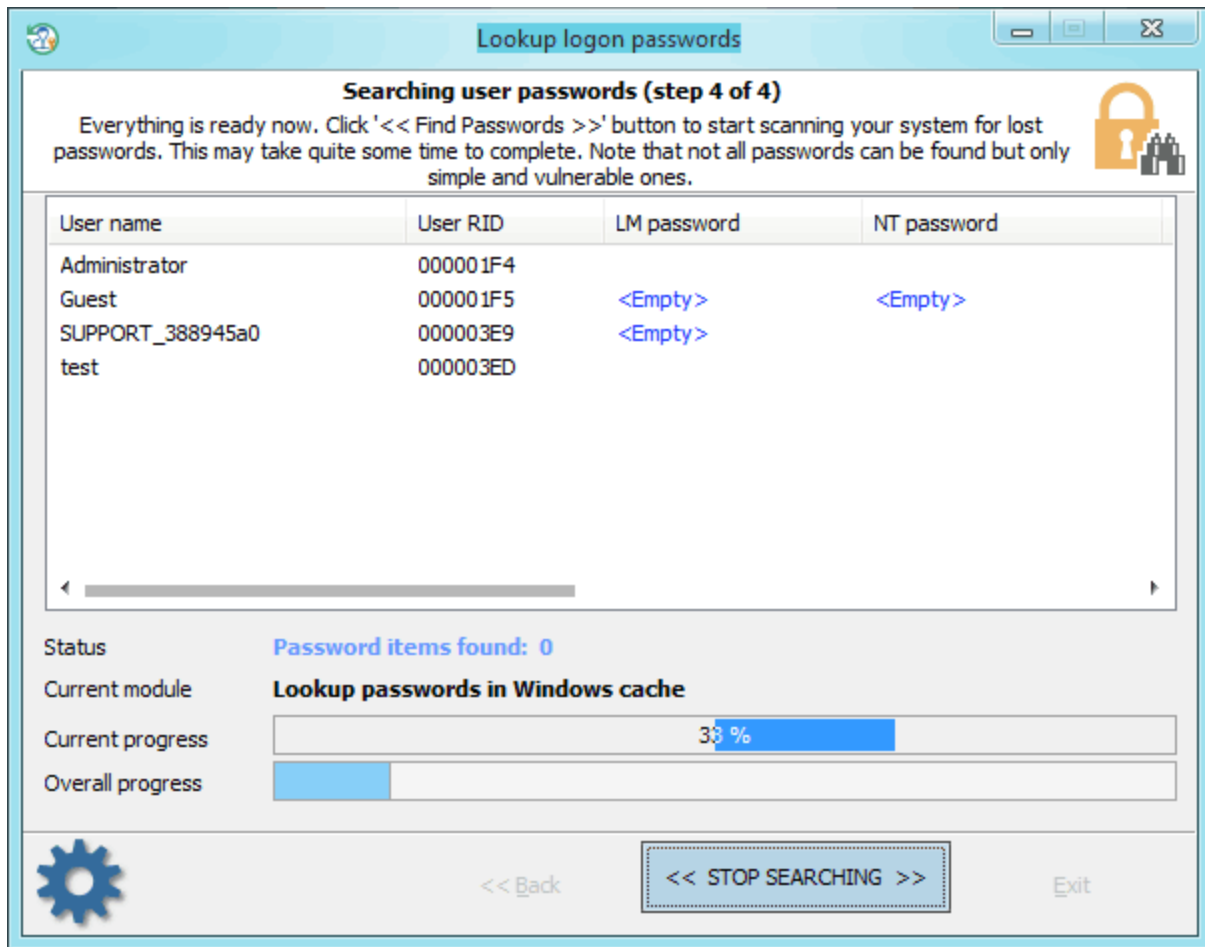
11.

LM, NTLM, ASCII, UNICODE
 'Password mutation level', 'Deep search',
 : RAM, hiberfil.sys, pagefile.sys
 (Microsoft Office),
 Bitlocker TrueCrypt.





2-
Reset Windows Password)



Passcape.

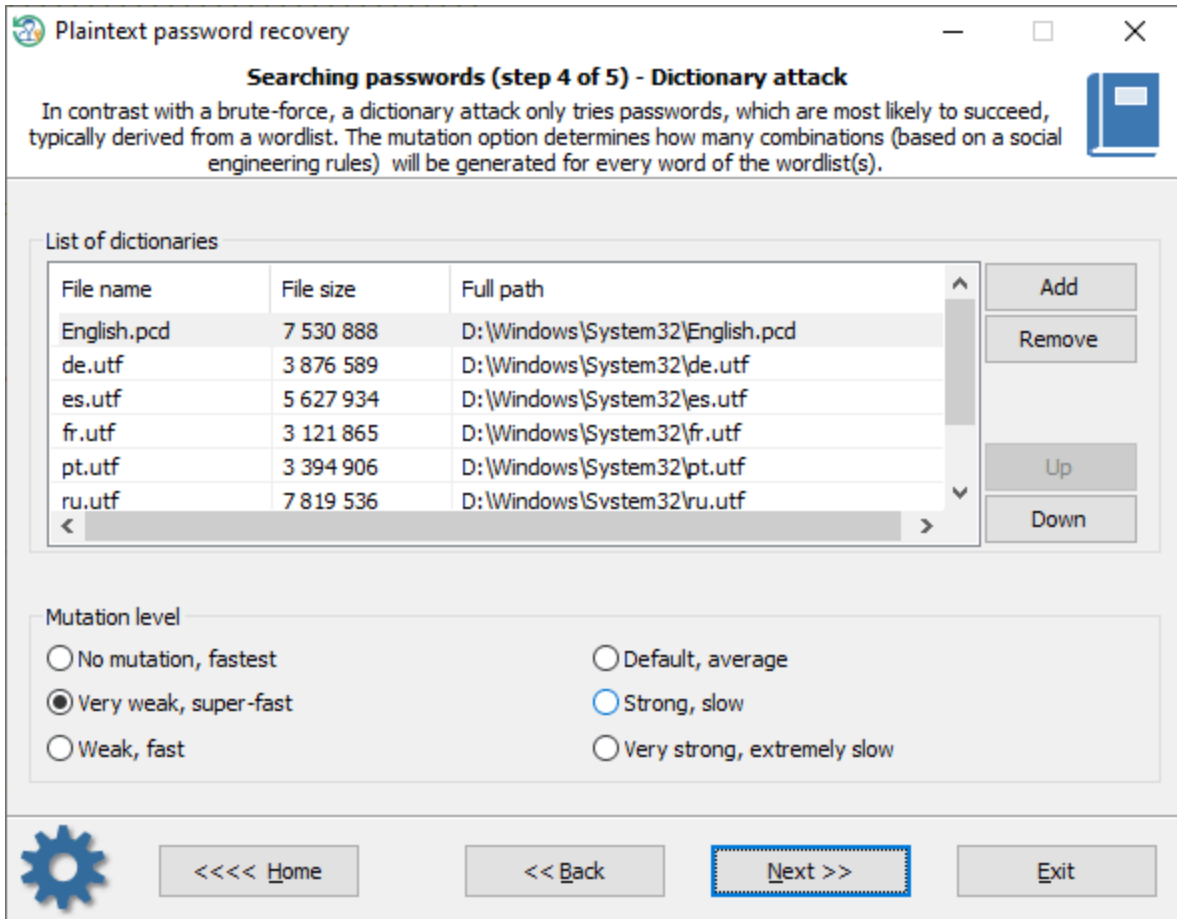
3-4

2-

3.5.1.1

3

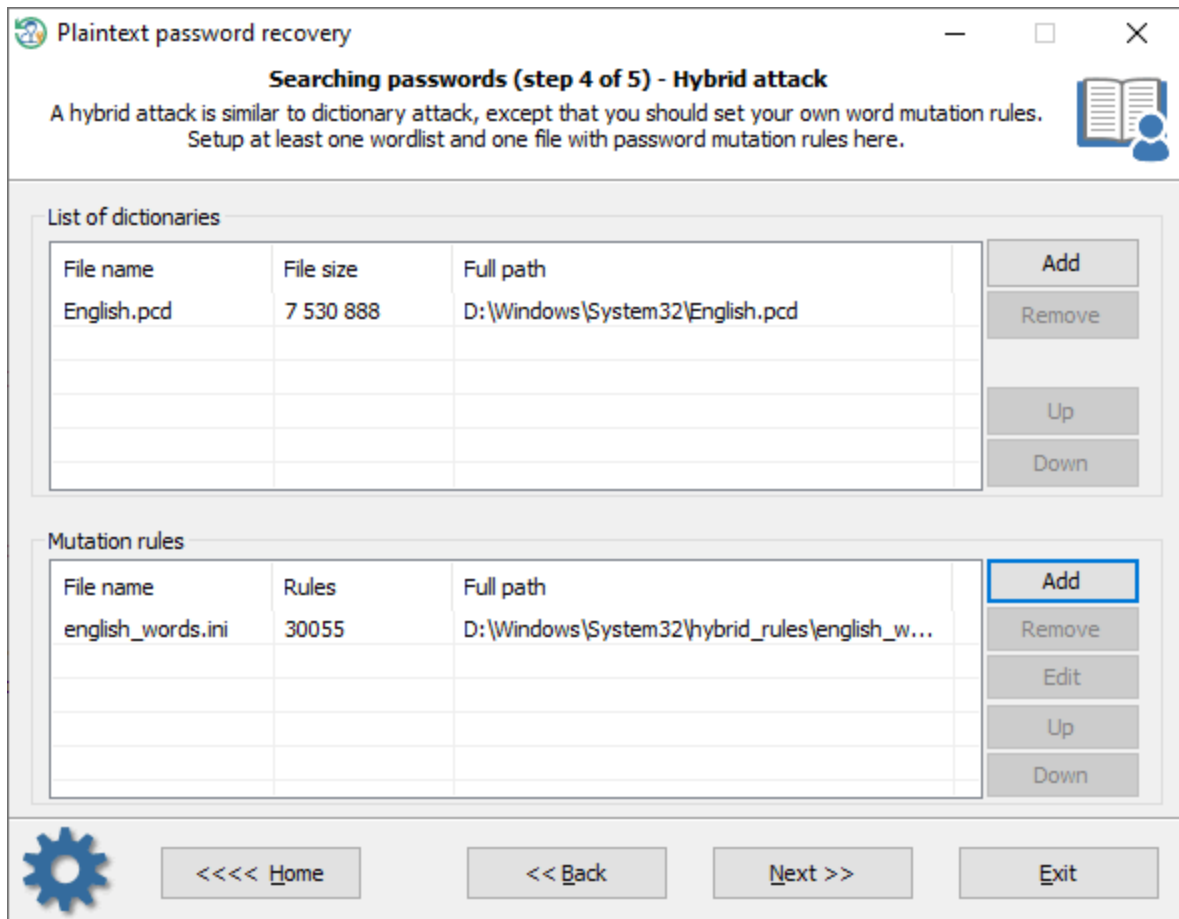
-
-
-

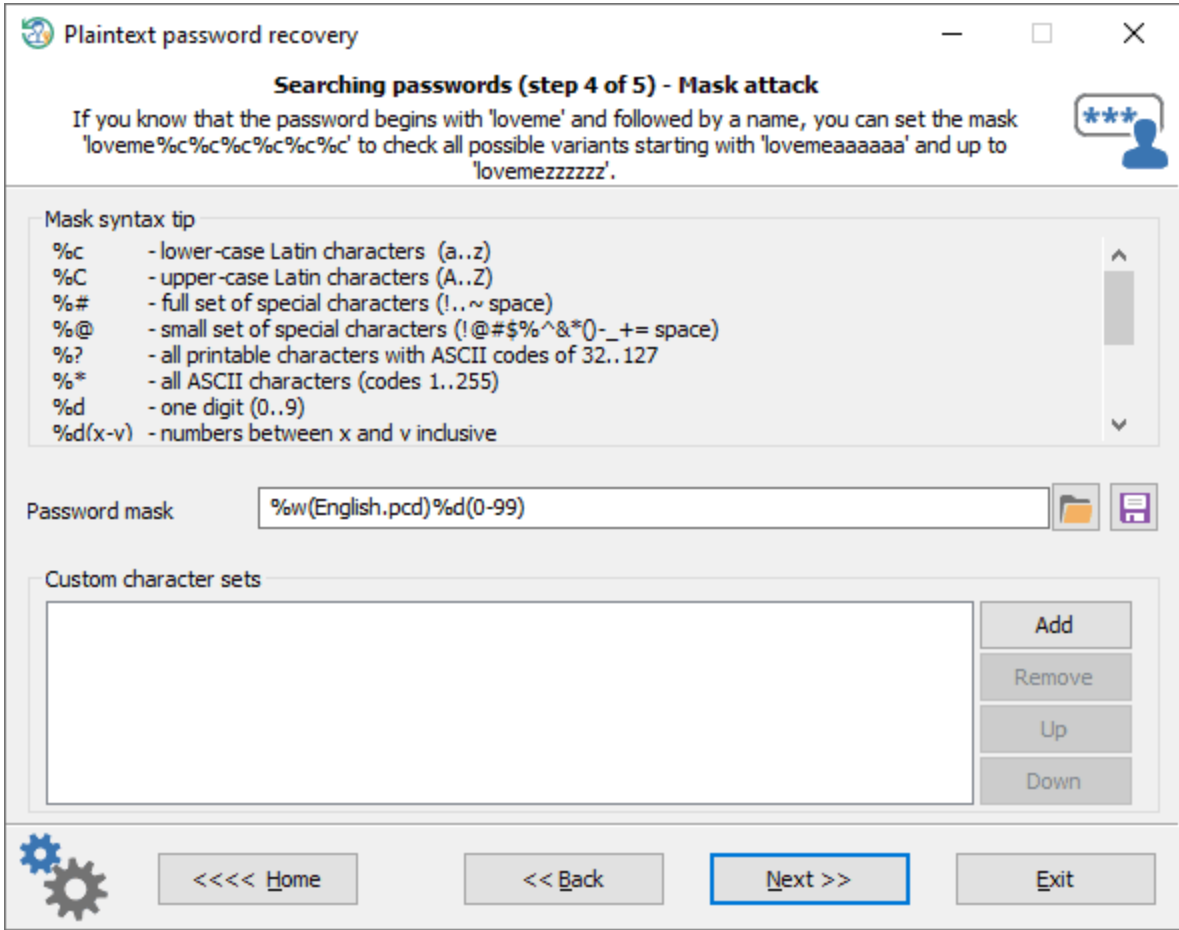


RWP

: ASCII, UNICODE, UTF8, PCD.

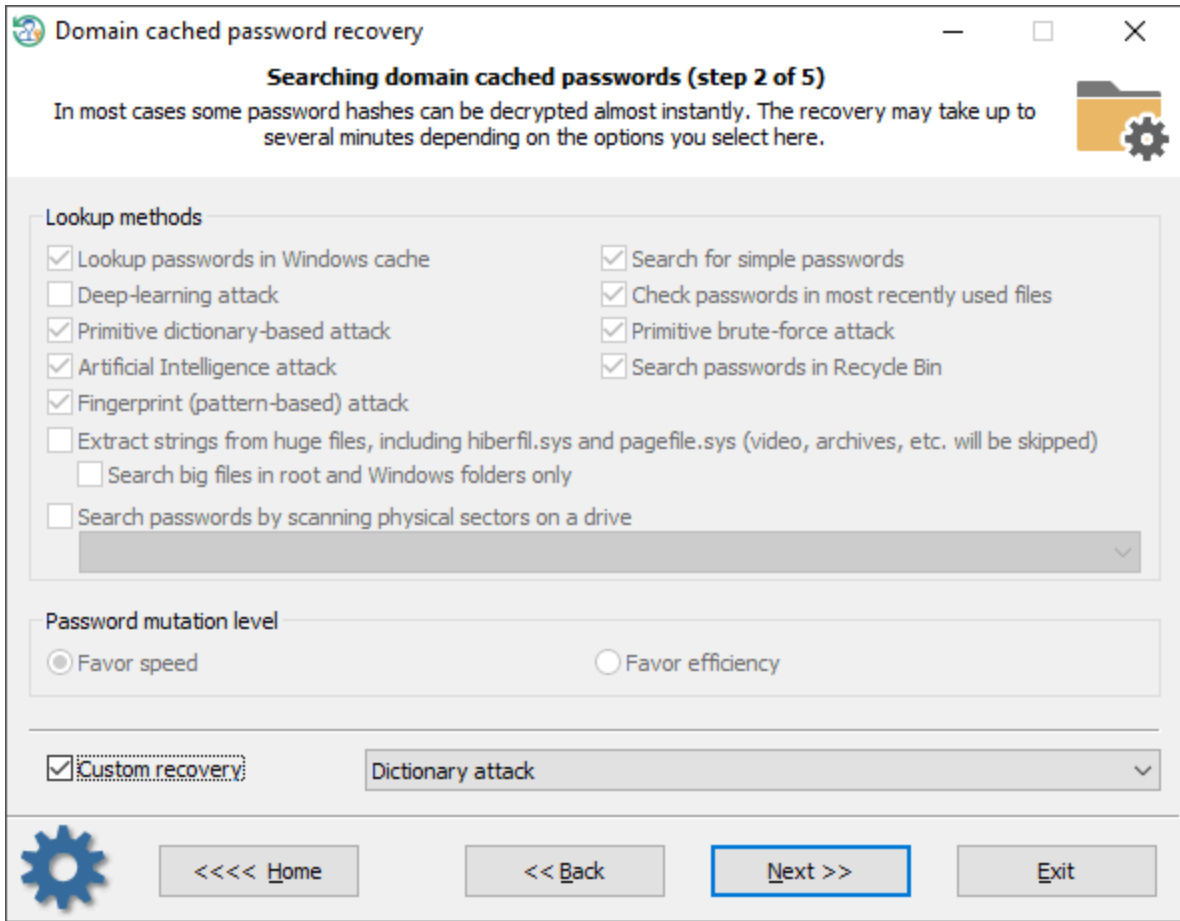
USB-





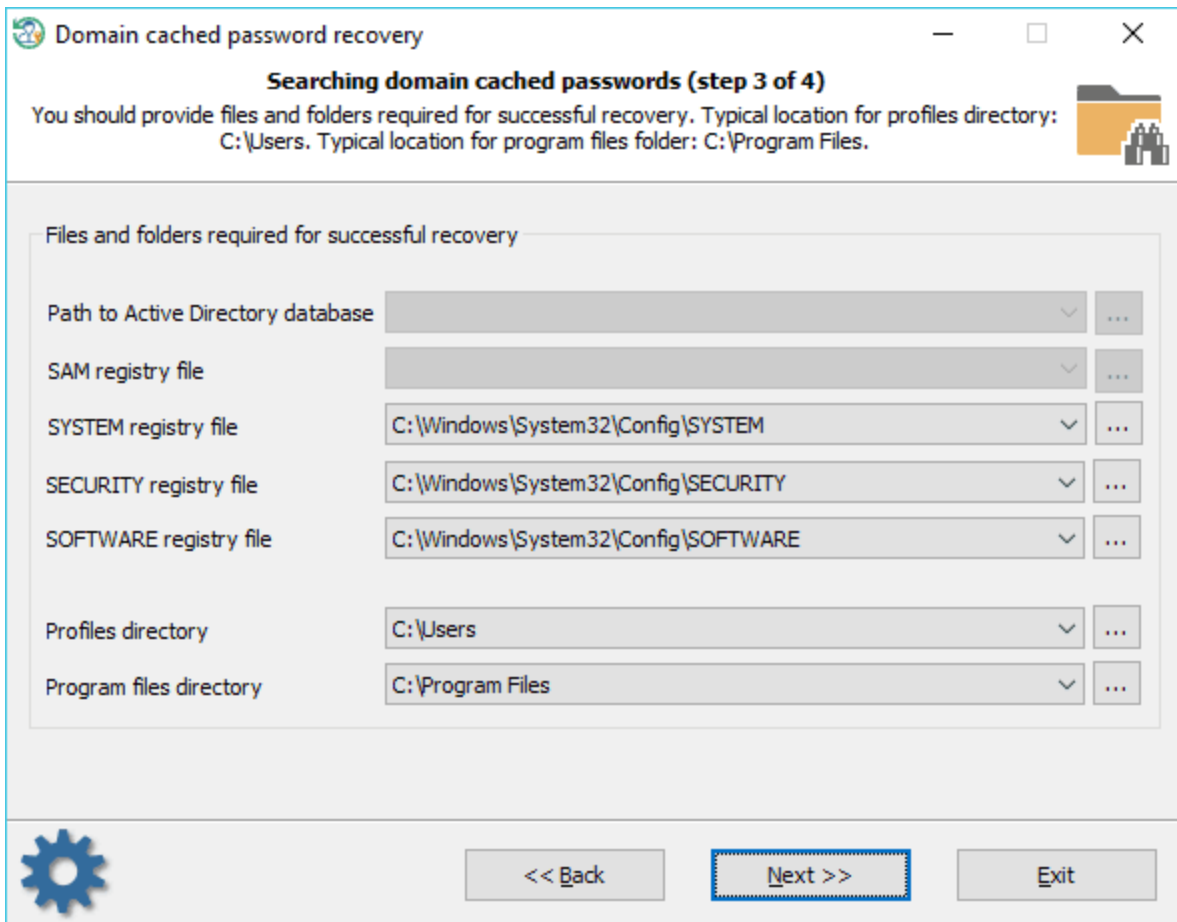
6 , , , 12 'loveme',
: loveme%c%c%c%c%c%c

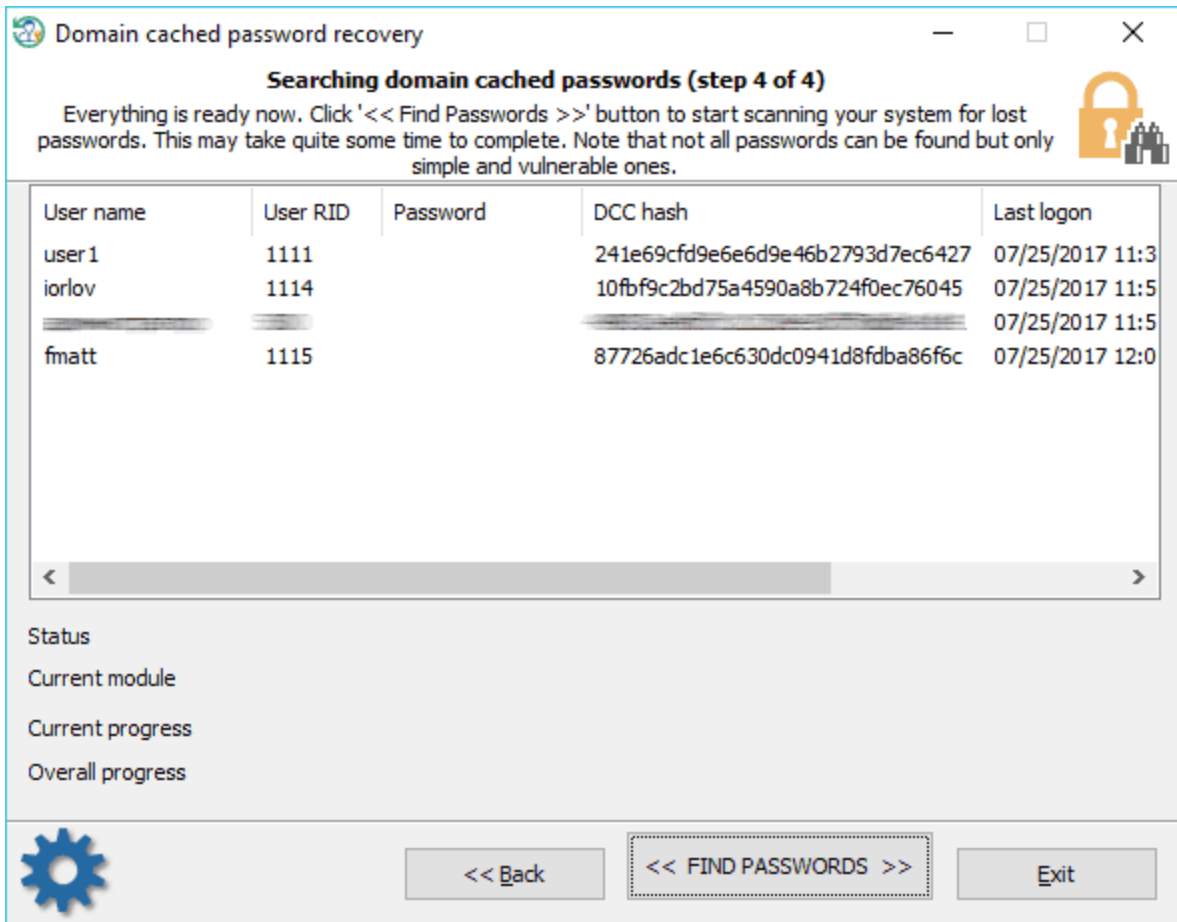
3.5.2



1. / : Windows. LSA, DSL, VPN, FTP, WiFi, Windows Search
2. 20
- 3.
4. Standard (Light
5.) Advanced
- 6.
- 7.
- 8.
9. : RAM , hiberfil.sys, pagefile.sys

10. 'Password mutation level' 'Deep search',





Windows 2000, Windows XP Windows 2003.

(Windows Vista)

8

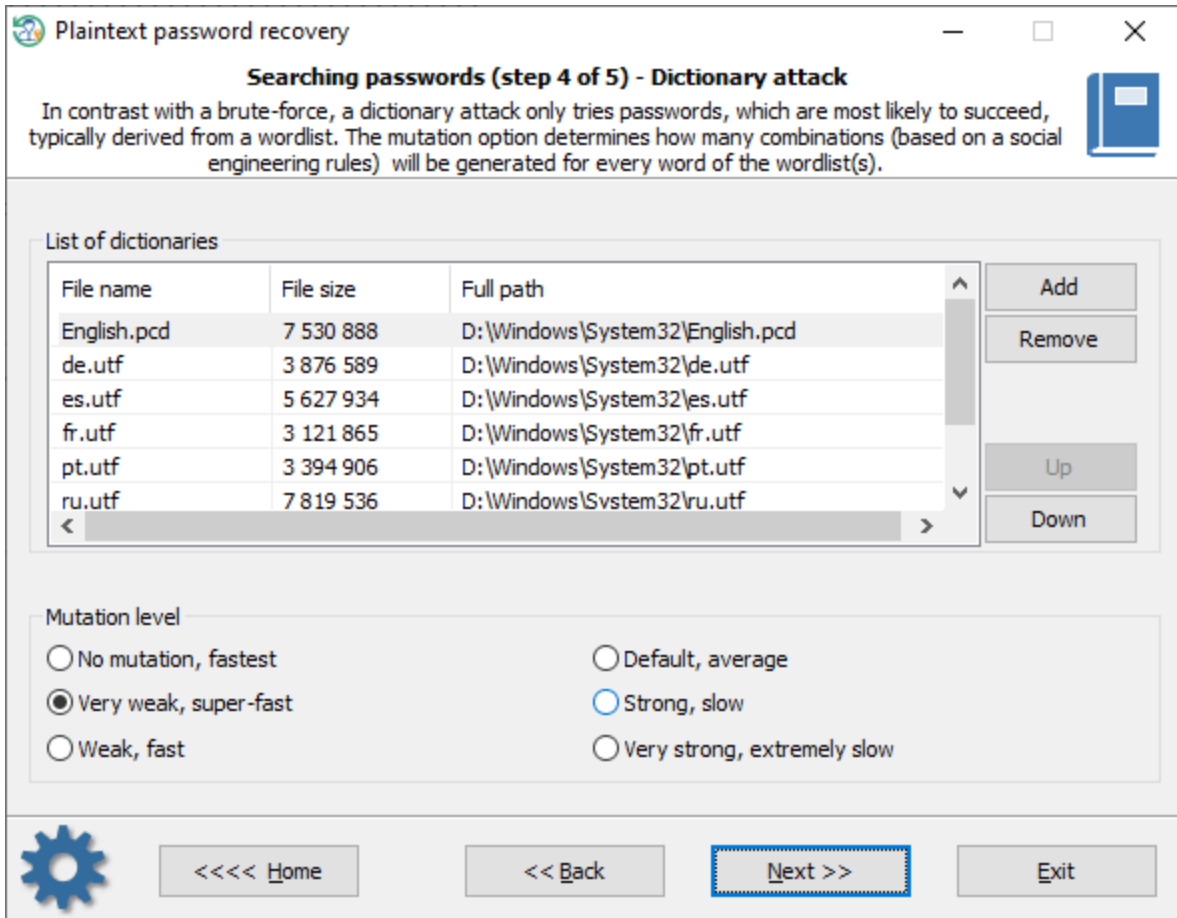
8

1000

3.5.2.1

3

-
-



. RWP

/

: ASCII, UNICODE, UTF8,
PCD.

USB-

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.

List of dictionaries

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

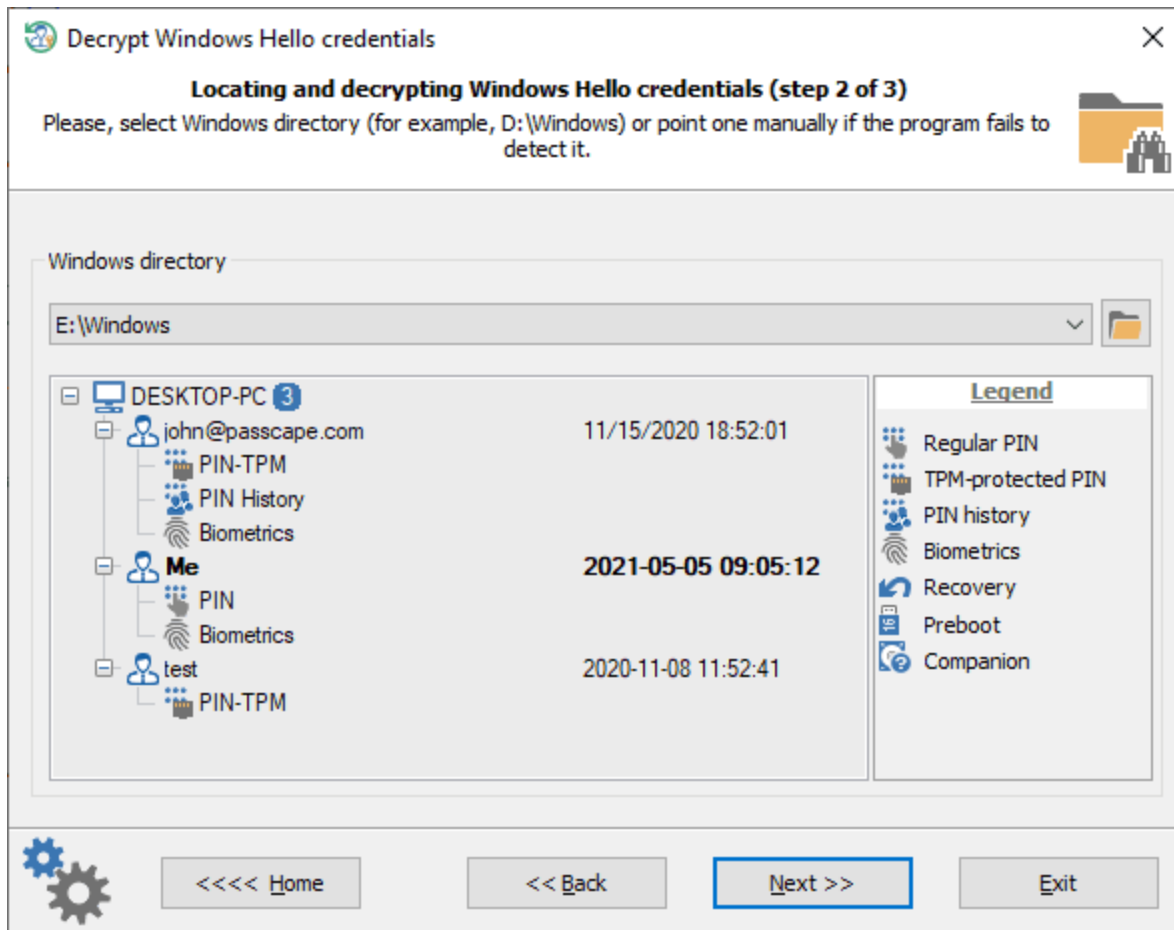
Add
Remove
Up
Down

Mutation rules

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

Add
Remove
Edit
Up
Down

Home <<<< << Back Next >> Exit



Reset Windows Password
Windows Hello.
Windows 10.

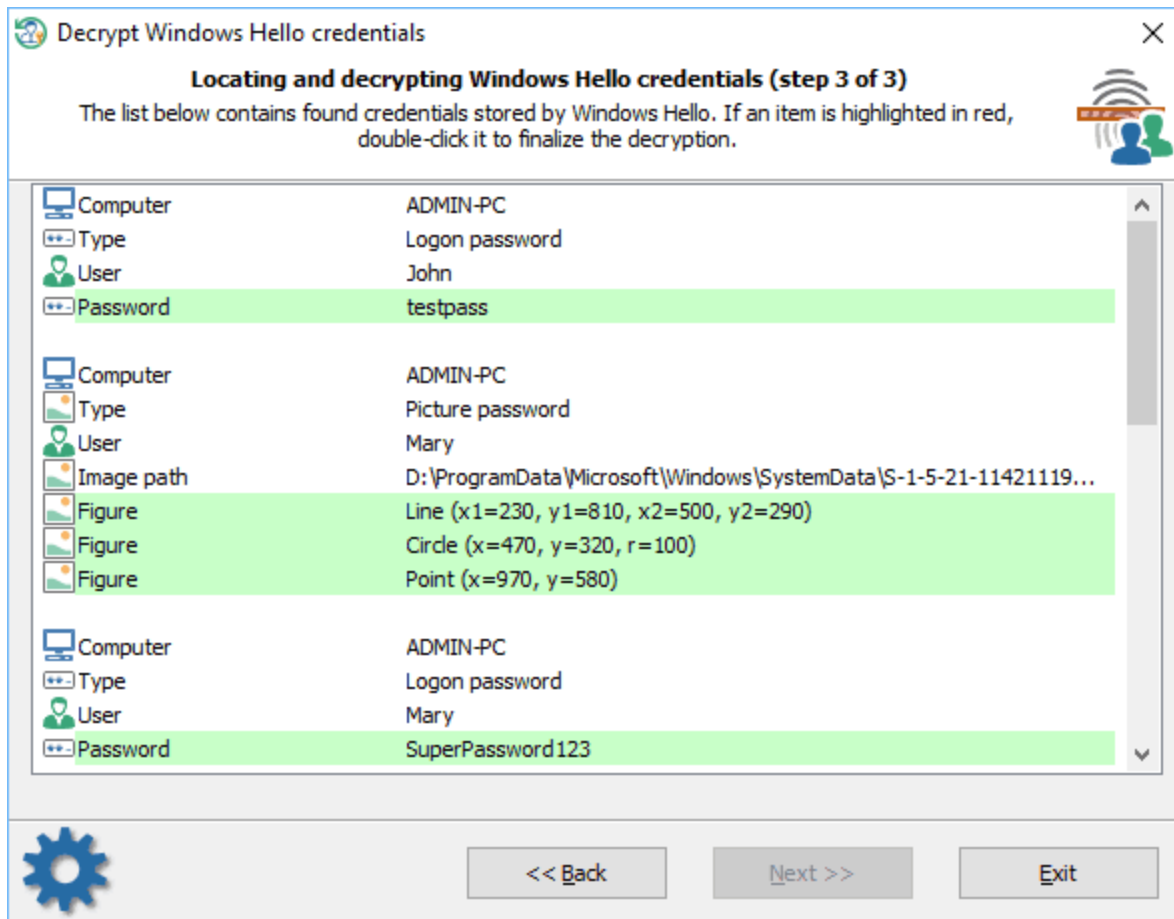
Windows

Windows Hello,

Windows Hello:

- PIN -
- PIN-TPM -
- PIN History -
- Biometrics -

TPM



Windows Hello

Reset Windows Password

PIN-

PIN-

3.5.4

PIN

Windows Hello

PIN- . PIN-

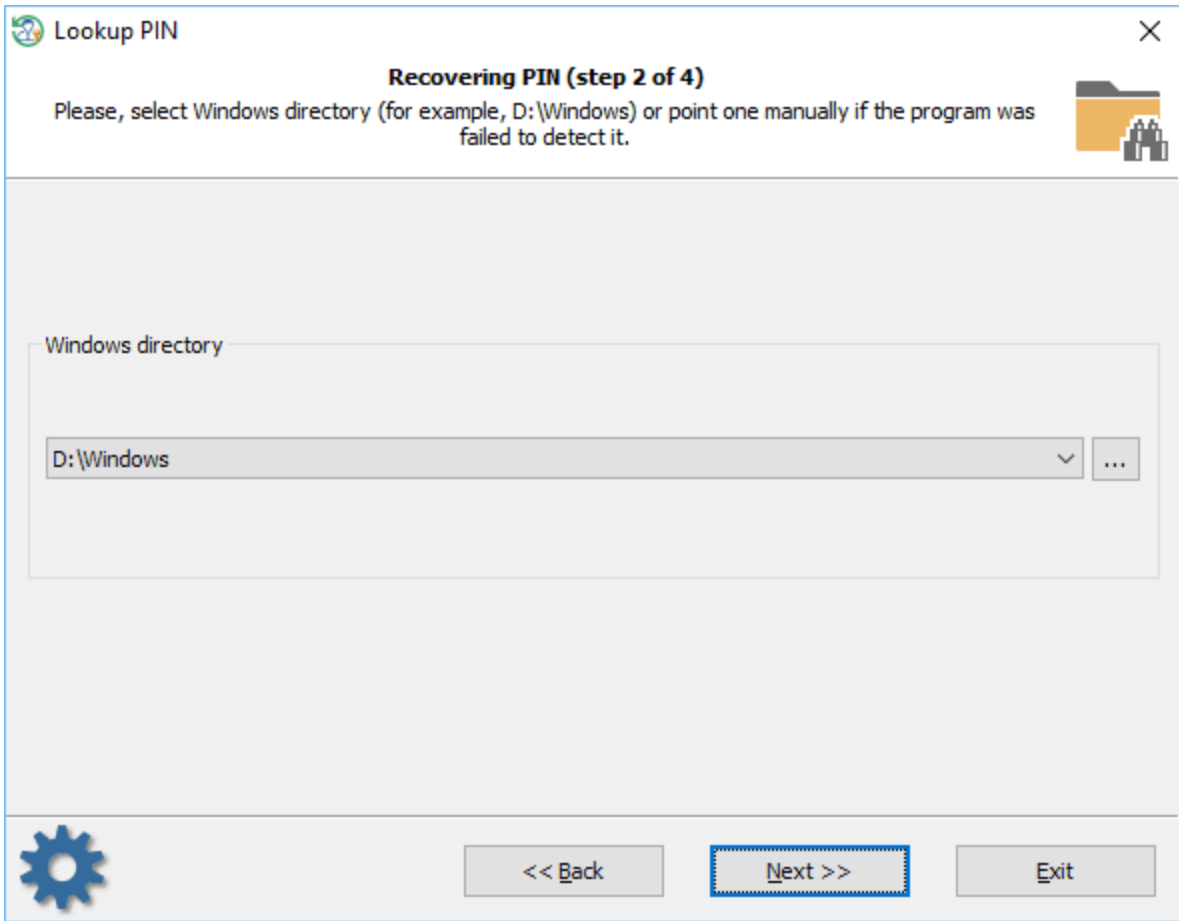
Windows 8,

PIN-

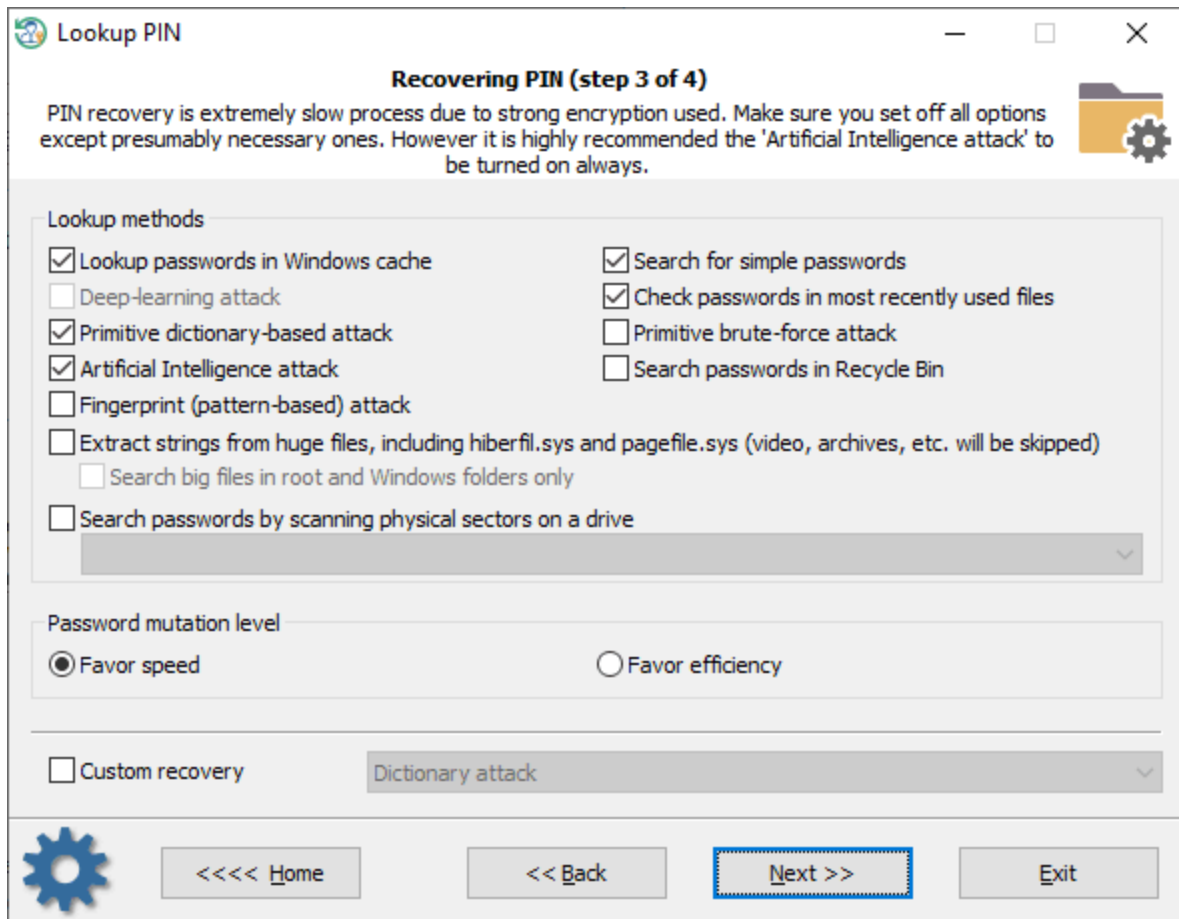
Windows 10

PIN.

Windows



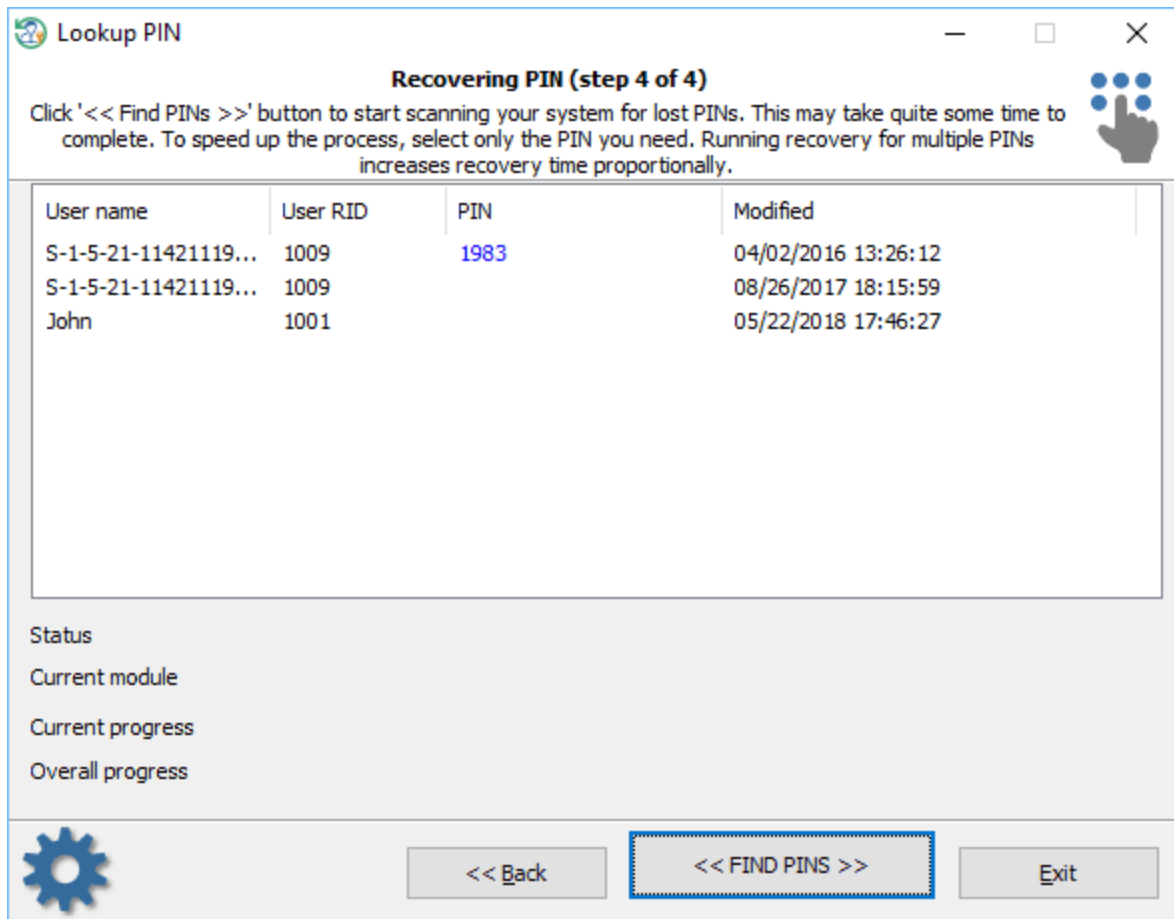
Windows



PIN.

PIN

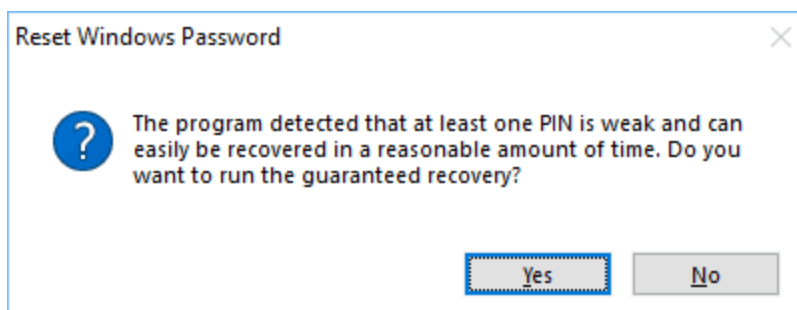
PIN-



PIN, . . . PIN

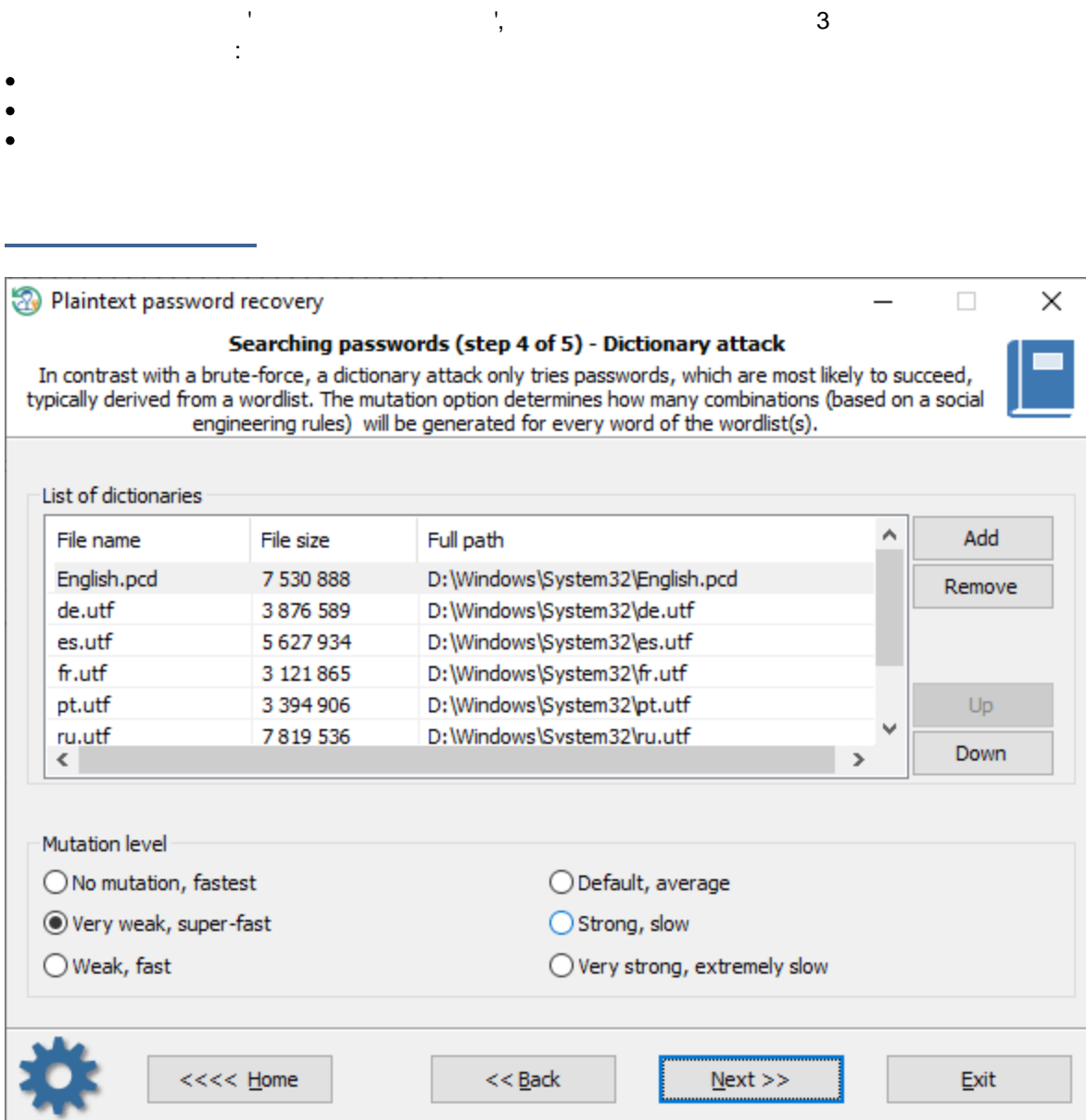
<< PIN >>

PIN-



<< PIN >>

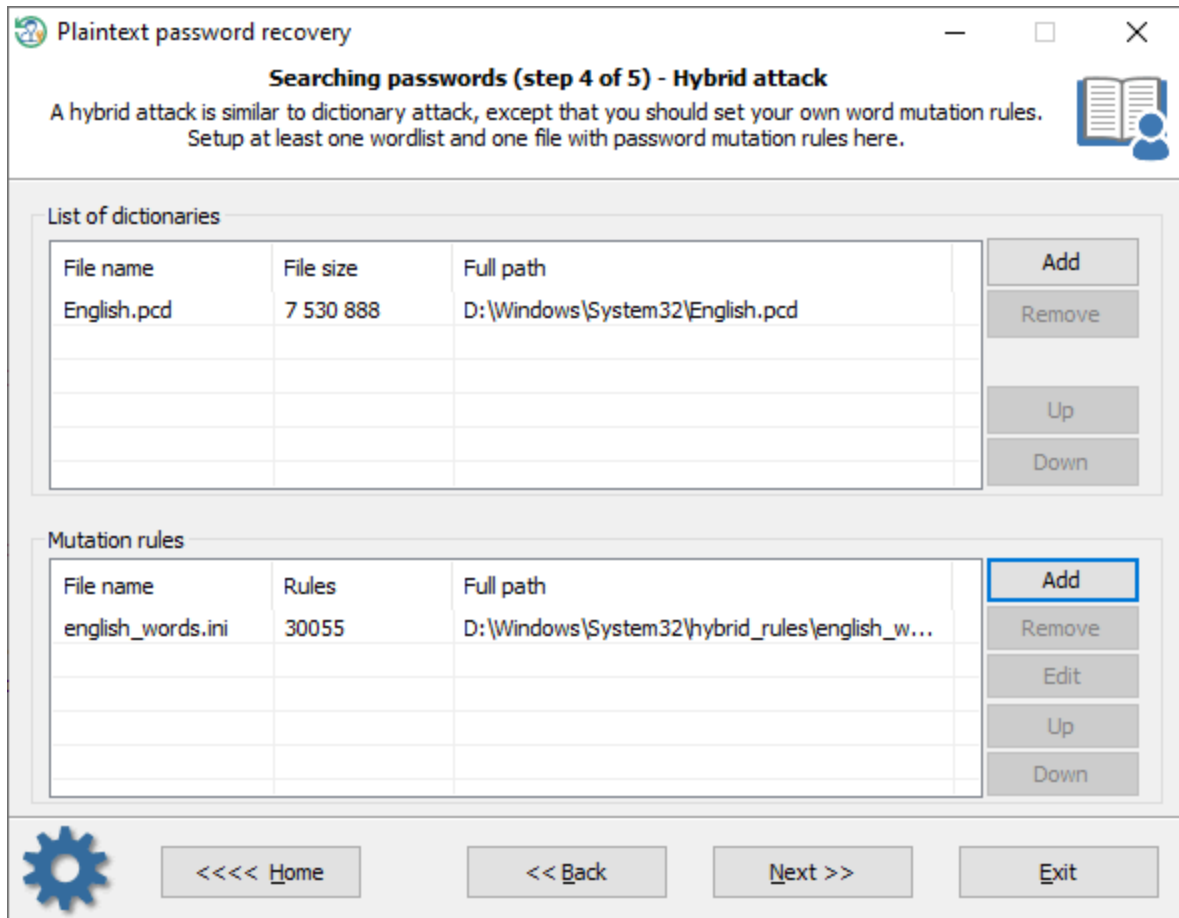
3.5.4.1



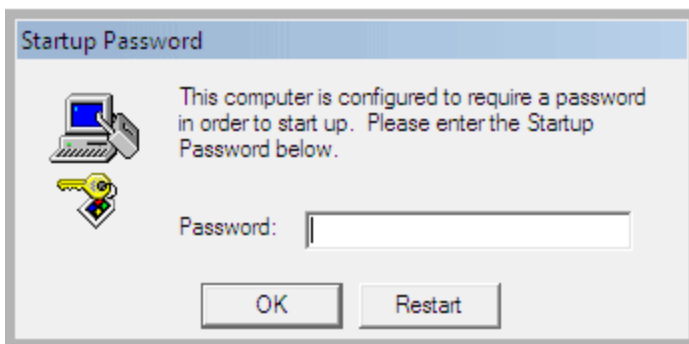
RWP /

: ASCII, UNICODE, UTF8, PCD.

USB-

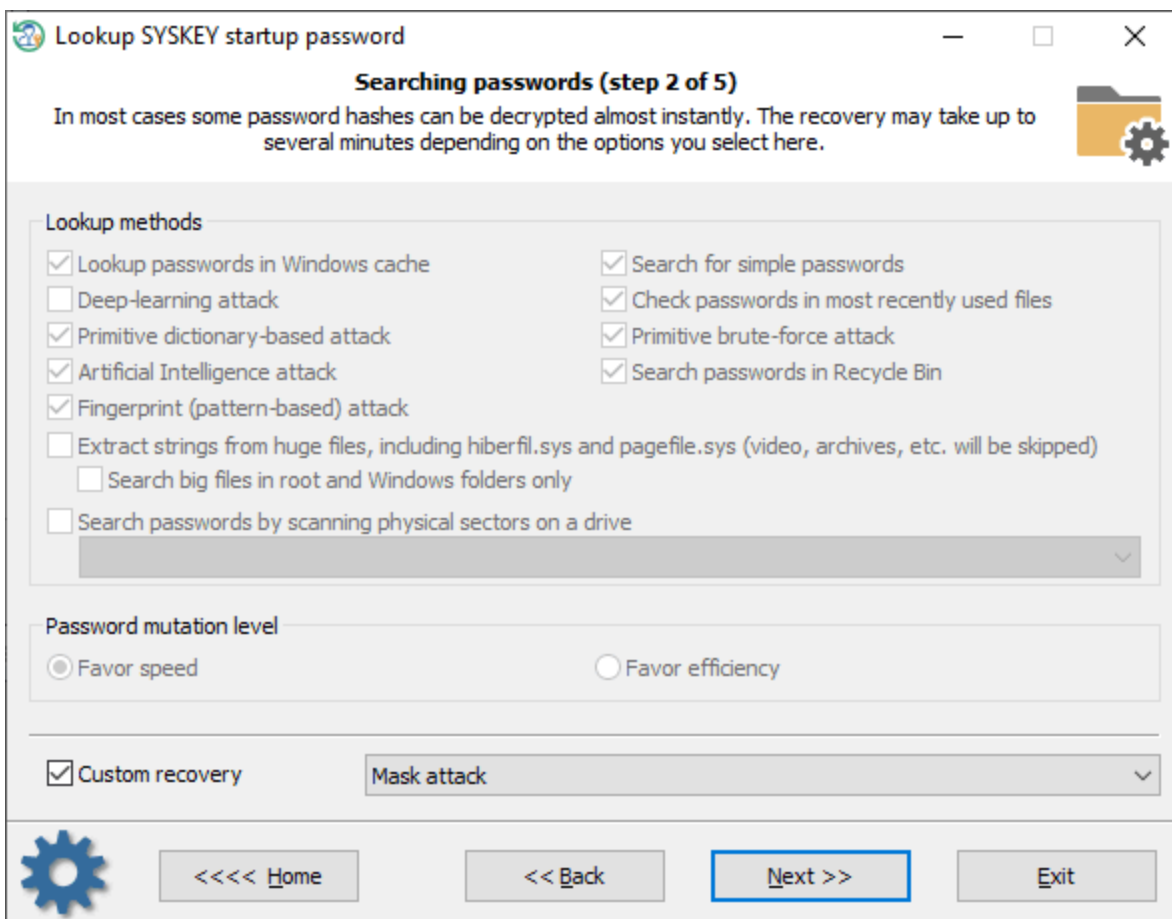


SYSKEY.



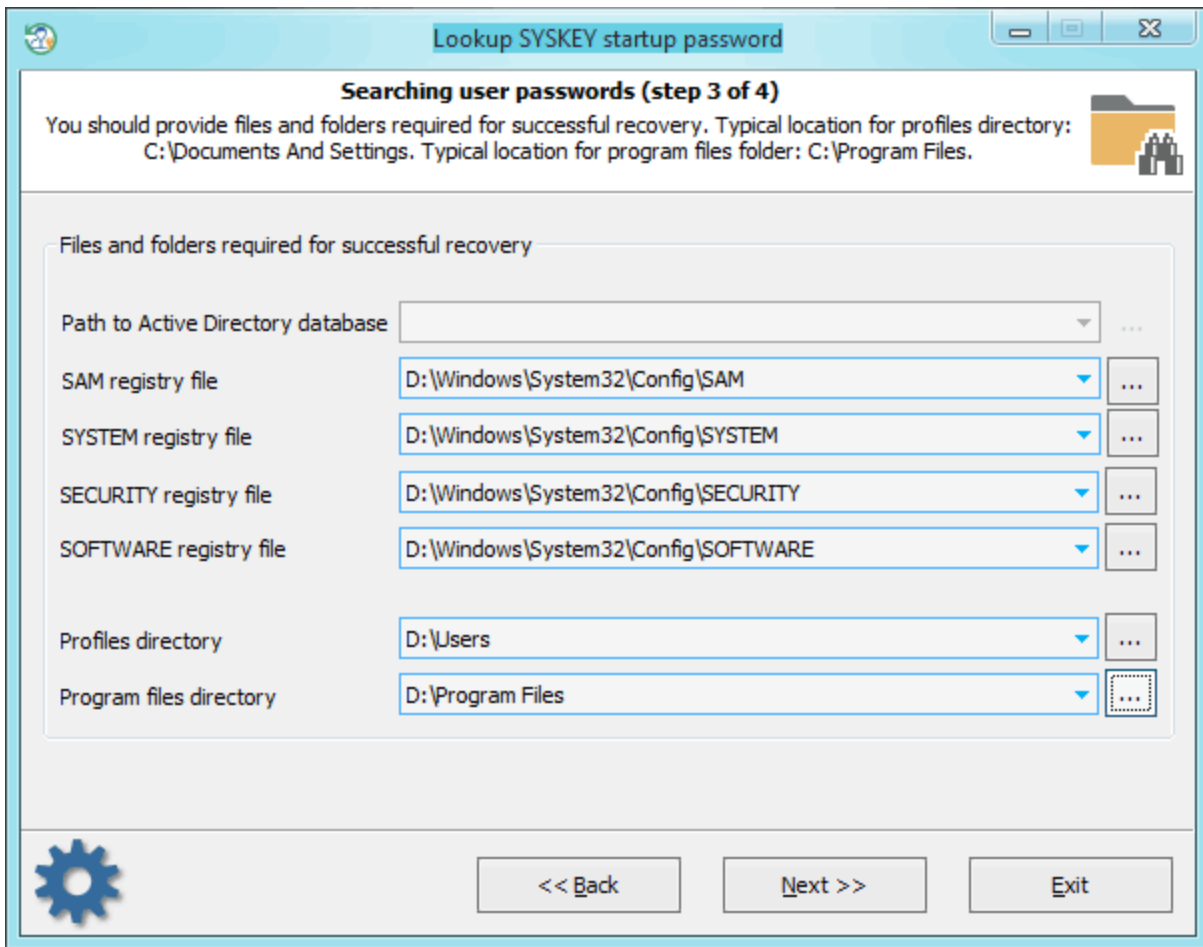
SYSKEY.

SYSKEY



SYSKEY

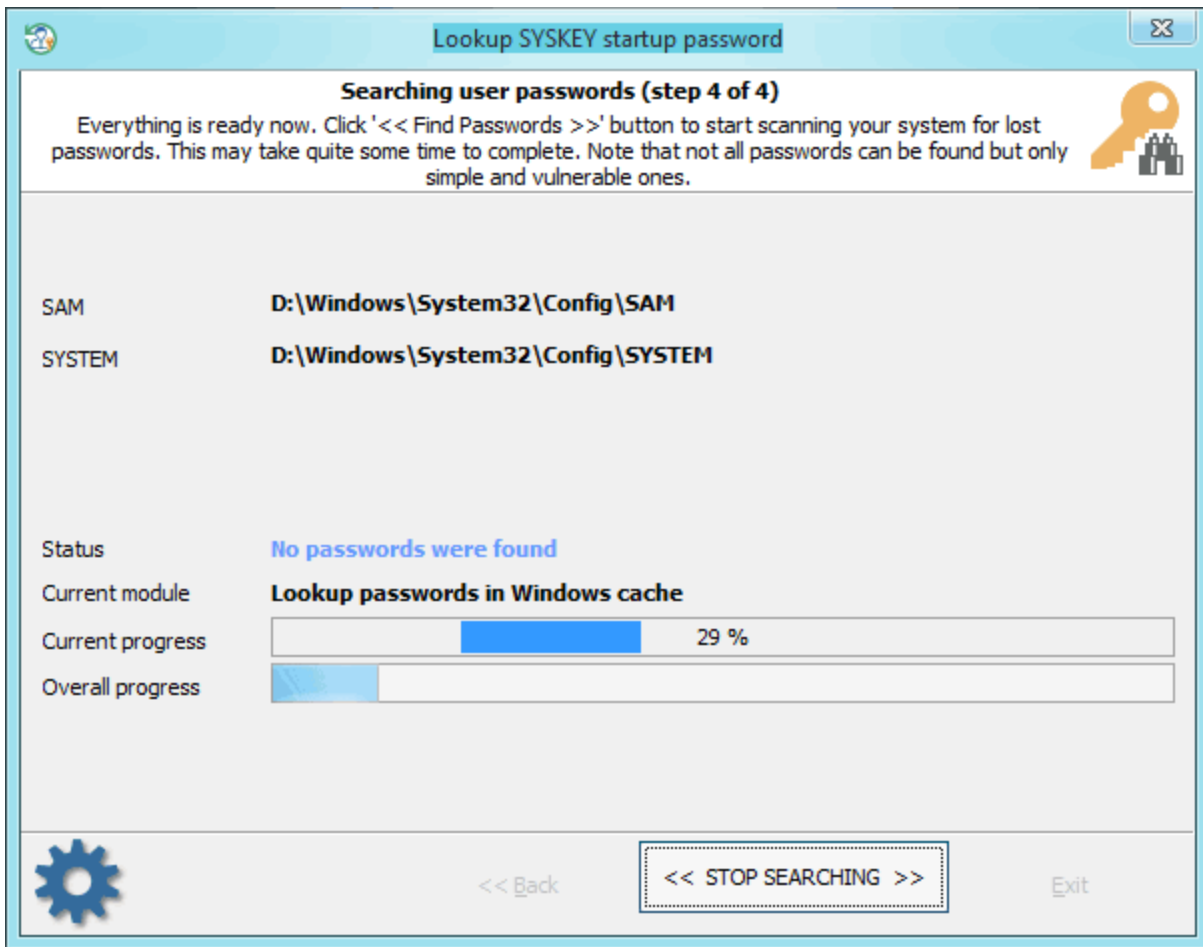
:



SYSKEY

2-

SYSKEY



SYSKEY

SYSKEY,

!

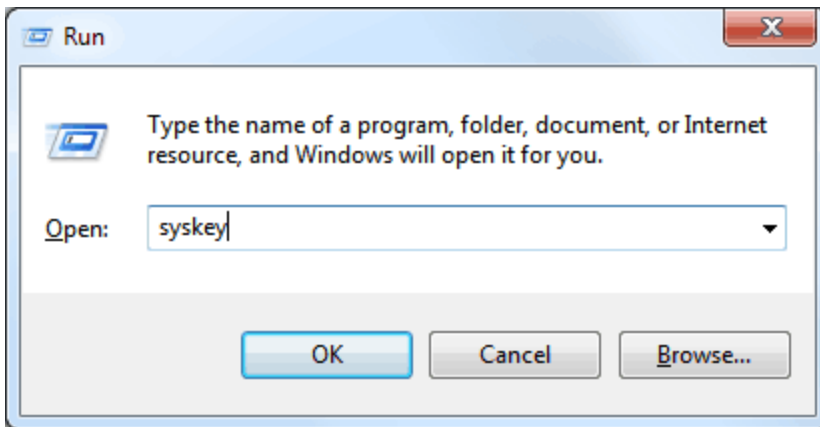
SYSKEY

Windows,

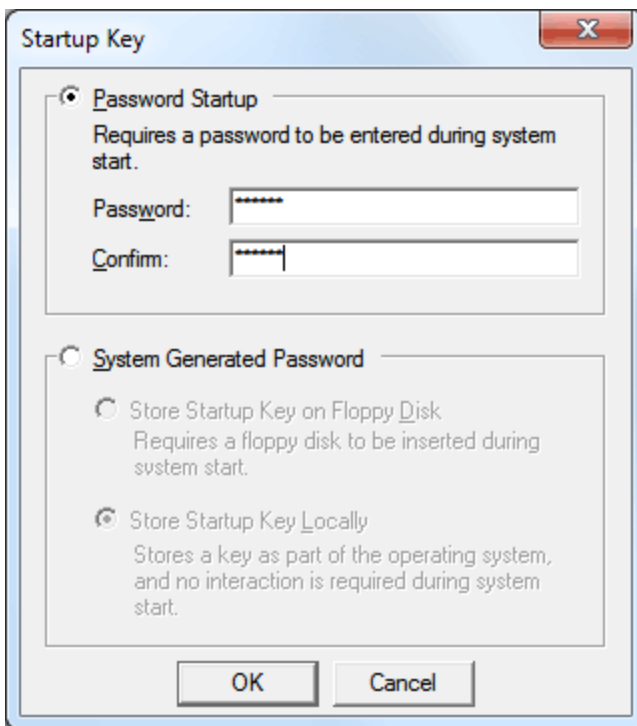
'Win+R',

'SYSKEY'

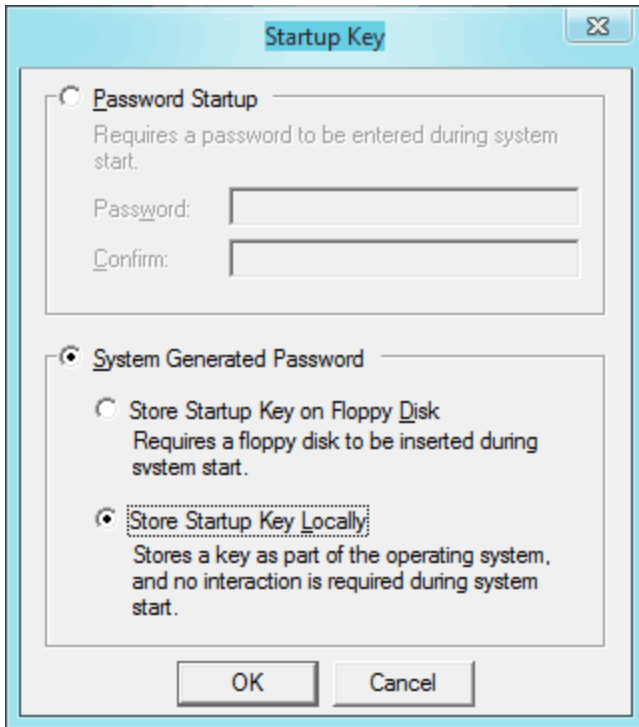
'OK',



'Update' , SYSKEY. ,
'Password Startup' , 'System Generated Password',



, SYSKEY :

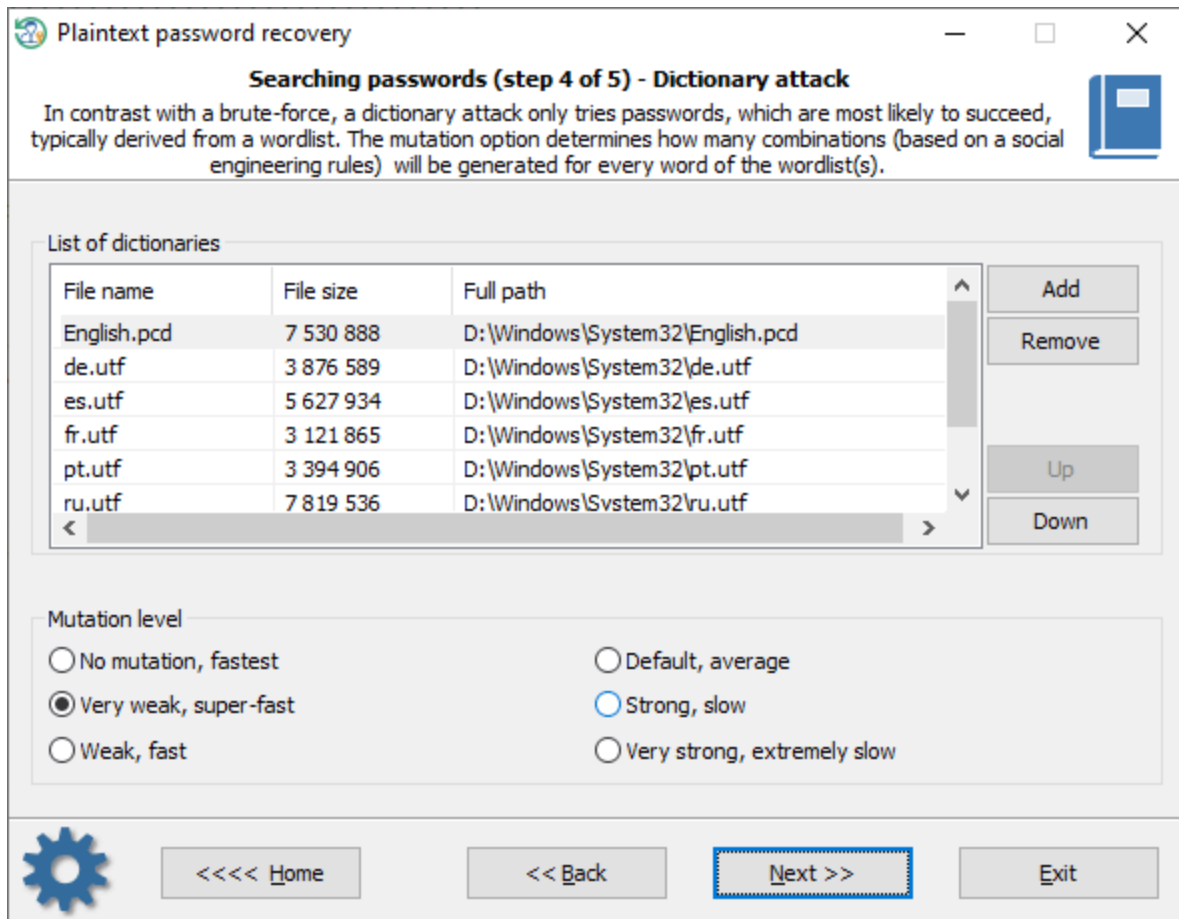


3.5.5.1

;

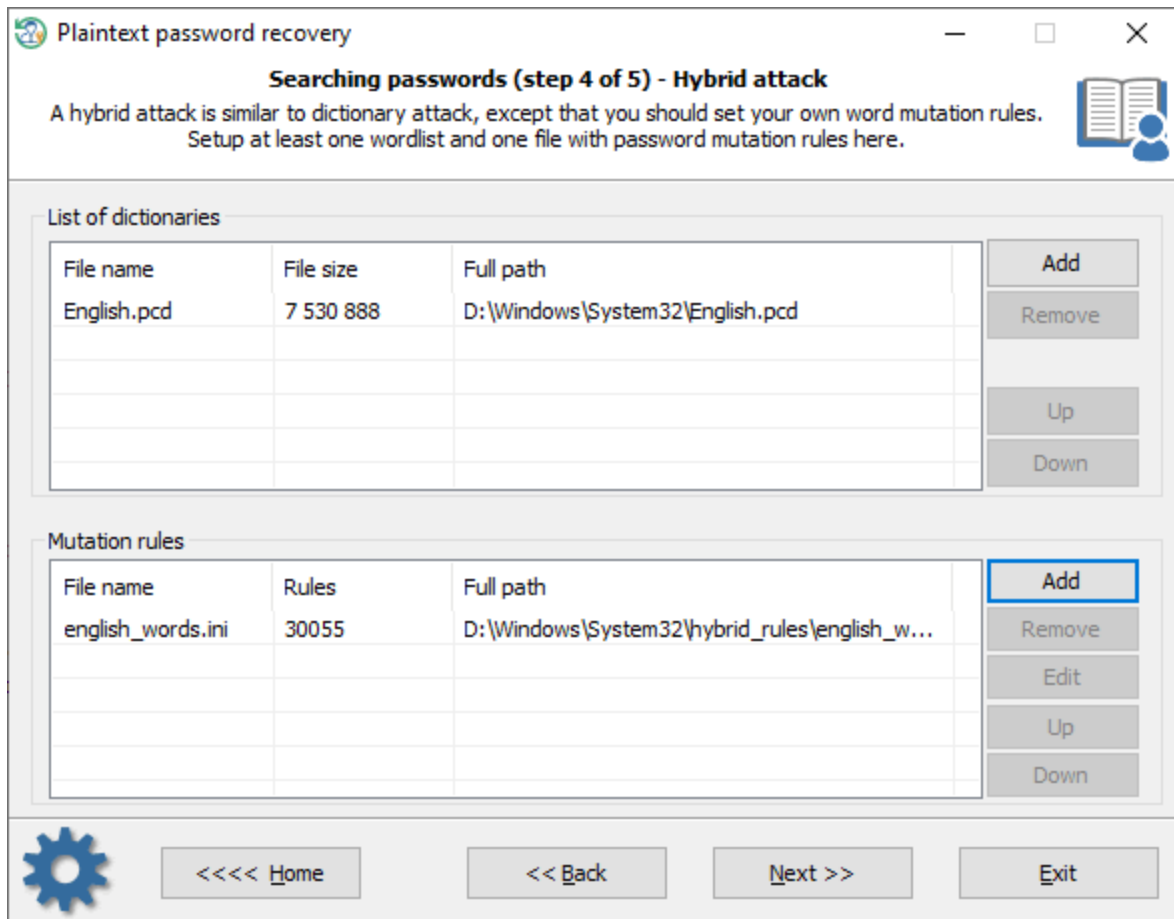
3

-
-
-



RWP : ASCII, UNICODE, UTF8, PCD.

USB-



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
 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

Search for simple passwords
 Check passwords in most recently used files
 Primitive brute-force attack
 Search passwords in Recycle Bin

Password mutation level

Favor speed
 Favor efficiency

Custom recovery
 Dictionary attack



Lookup passwords for virtual machines

Searching passwords (step 3 of 4)

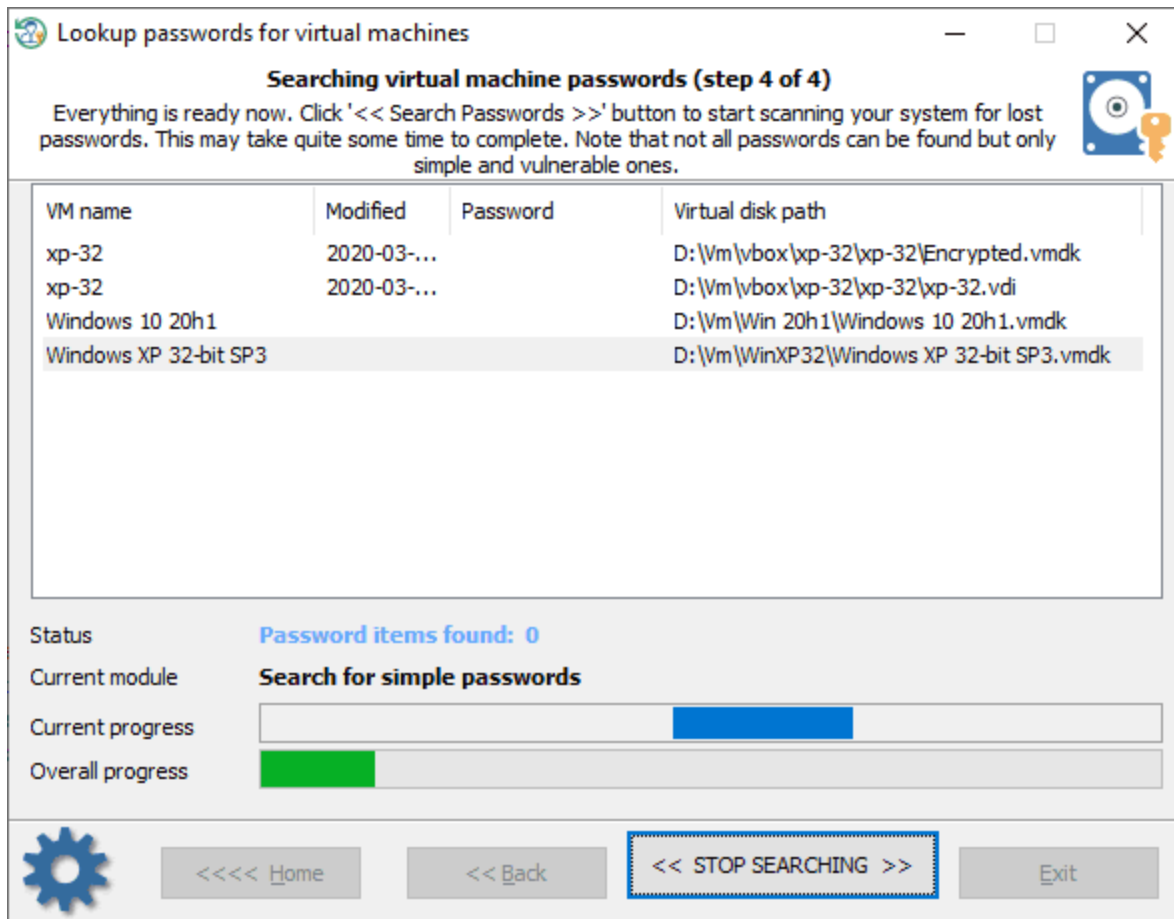
You should provide files and folders required for successful recovery. Typical location for profiles directory: C:\Users. Typical location for program files folder: C:\Program Files.

Files and folders required for successful recovery

Path to Active Directory database	<input type="text"/>	
SAM registry file	C:\Windows\System32\Config\SAM	
SYSTEM registry file	C:\Windows\System32\Config\SYSTEM	
SECURITY registry file	<input type="text"/>	
SOFTWARE registry file	<input type="text"/>	
Profiles directory	D:\Users	
Program files directory	<input type="text"/>	

<<<< Home << Back Next >> Exit

RWP

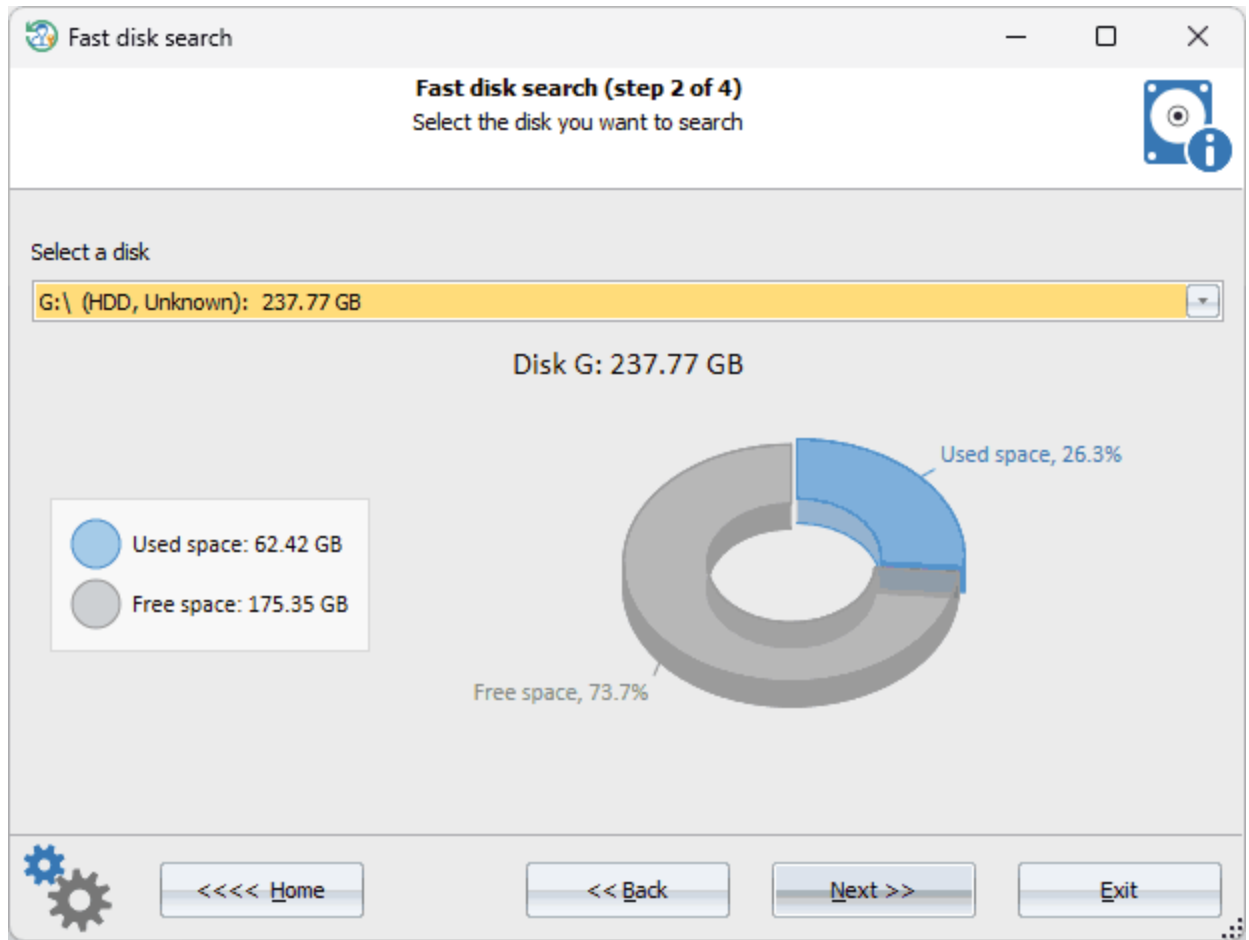


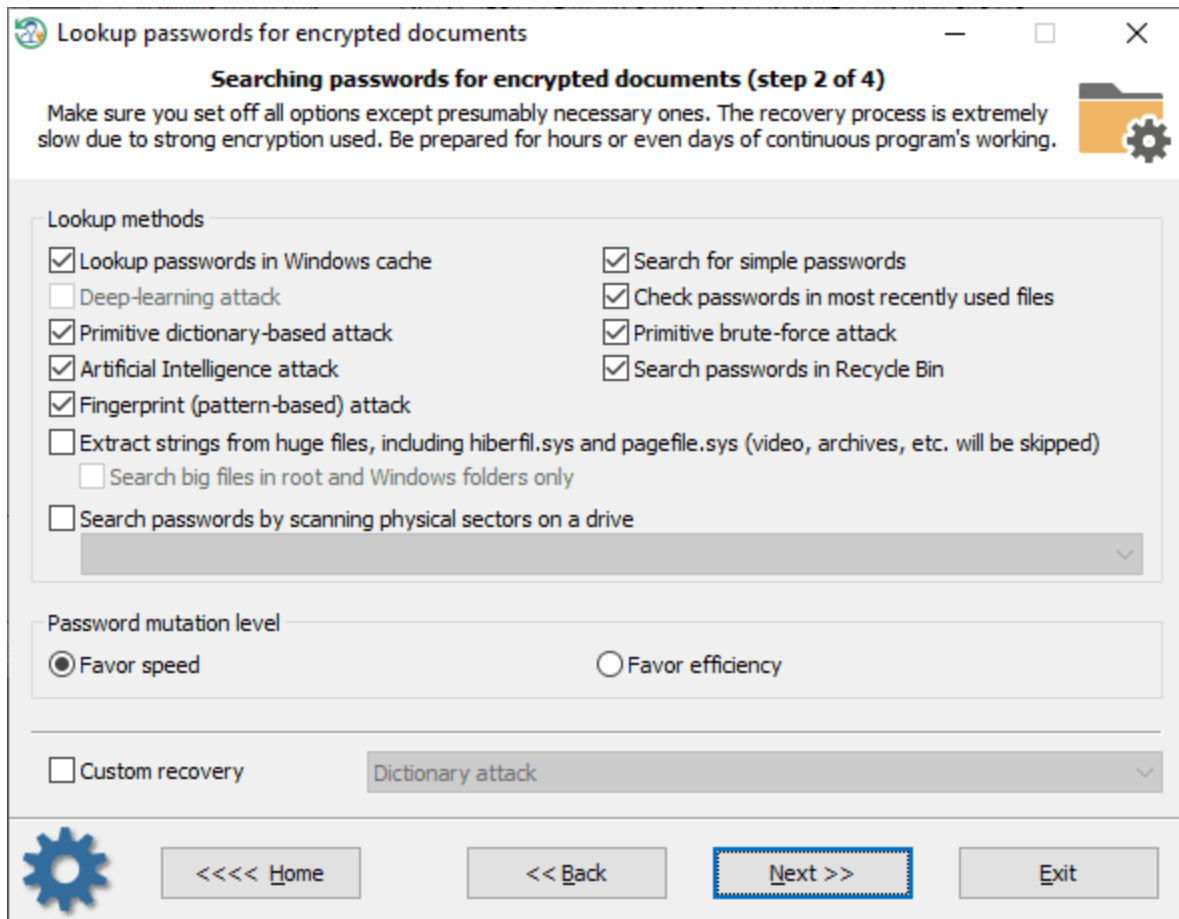
3.5.7

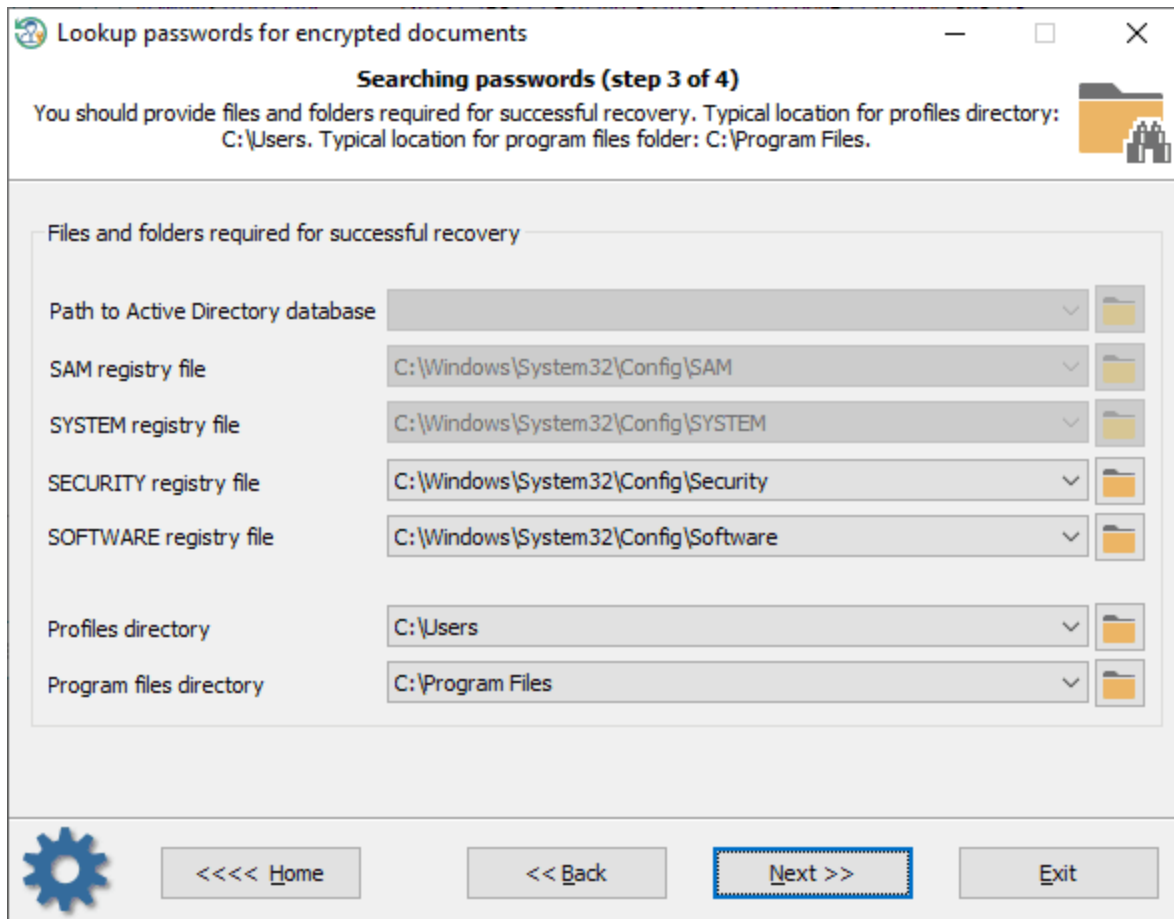
RWP

(RWP)

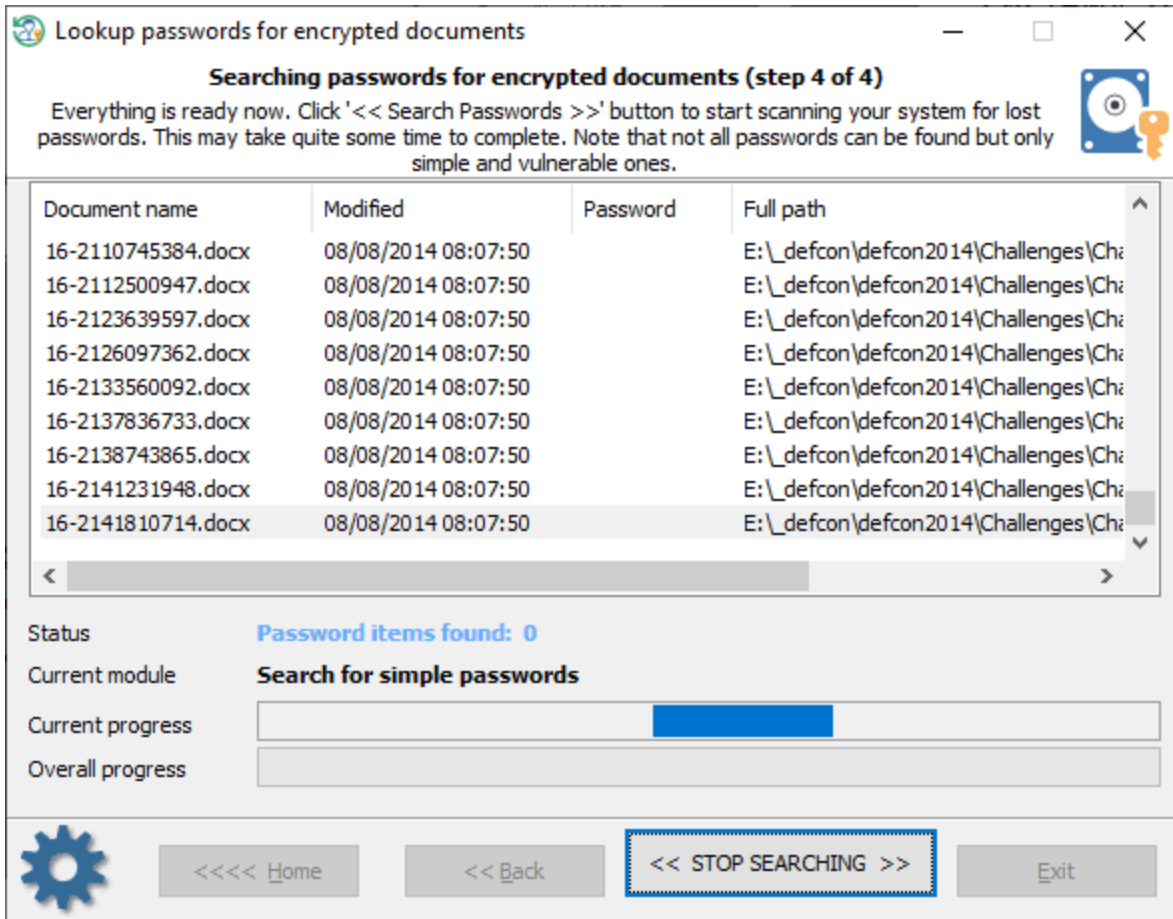
- Microsoft Office 97
- OpenDocuments: OpenOffice, LibreOffice, MyOffice.
- PDF (,).







RWP



Microsoft Office 2013

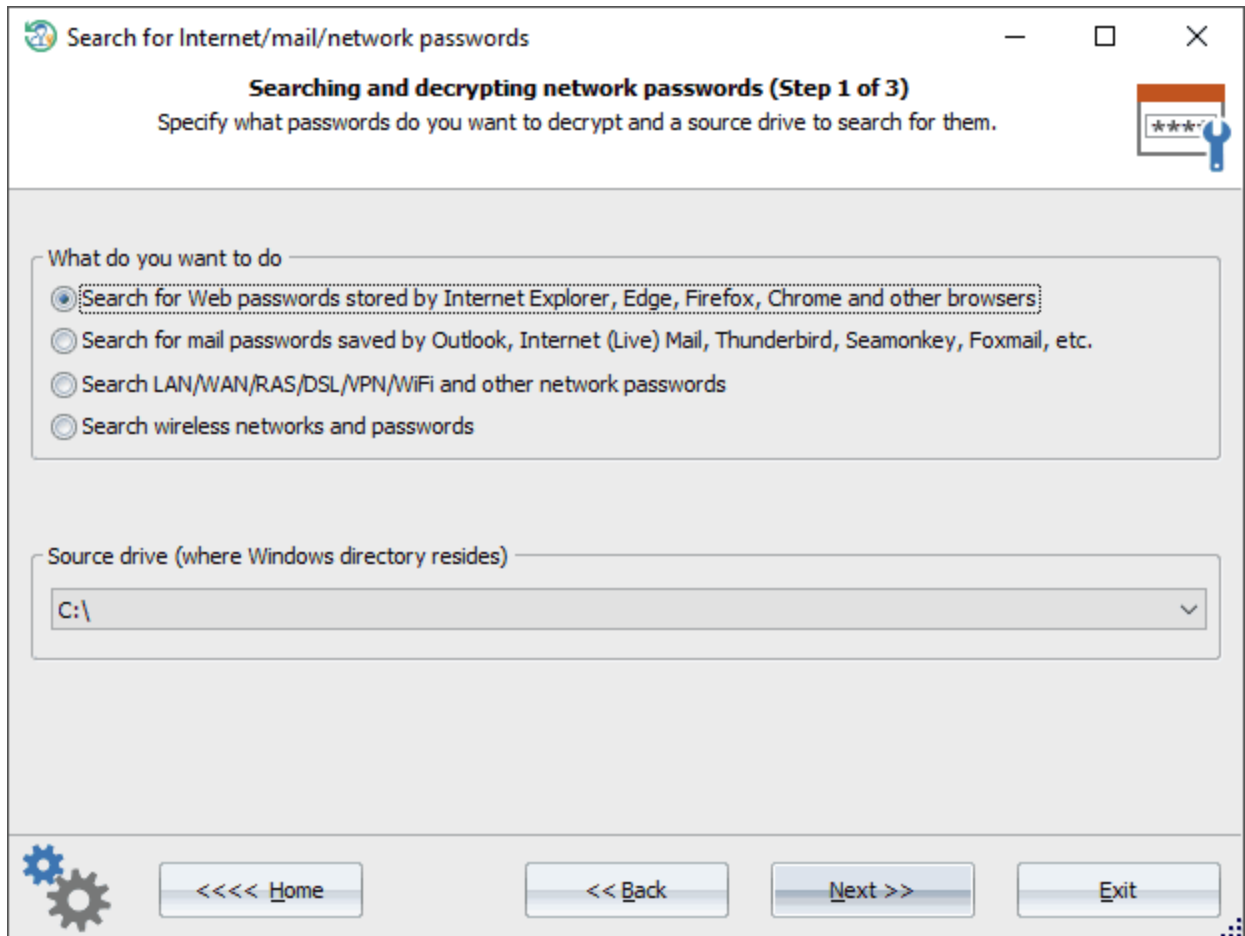
1-2

!

(
). [Aadhaar](#)
 Aadhaar e-pan
 PDF
 Aadhaar
 e-pan -
 Reset Windows Password
 Aadhaar/e-pan,
 (PDF Aadhaar/e-pan
 7 100%

3.5.8

. Reset Windows Password




Windows.

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

Where to search

Search for all local accounts

Search for selected user account


User profiles

Profiles directory

User profile directory

Advanced options

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

 <<<< Home << Back **Next >>** Exit

Windows,

[TBAL](#) _____),

(DPAPI ,

DPAPI,
LSA

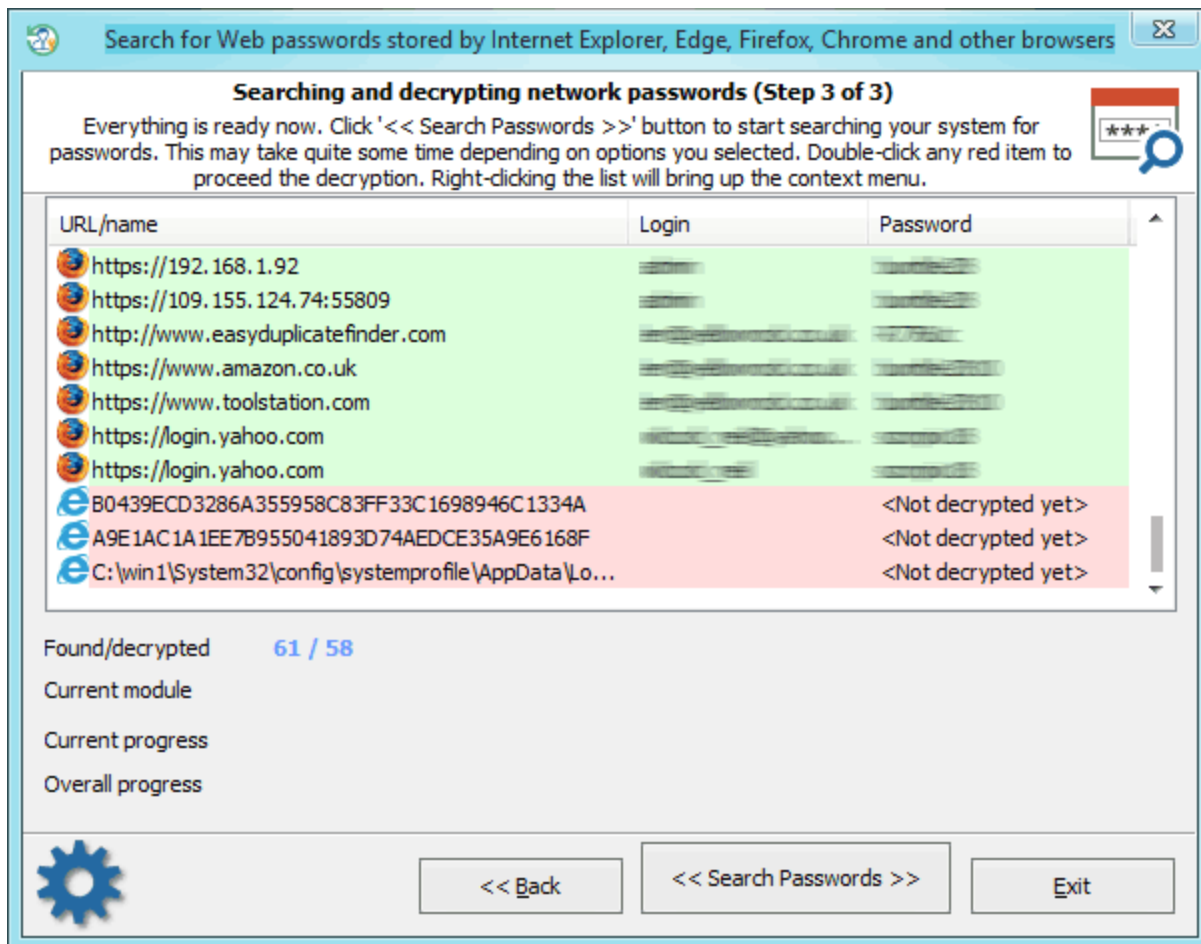
/DSL/RAS/LAN

DPAPI ,

<<

>>

3.5.8.1



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

- Internet Explorer 4-6
- Firefox
- Opera ()
- Mozilla ()

- Internet Explorer 10
- Edge
- Firefox ()
- Opera ()
- Chrome
- Safari

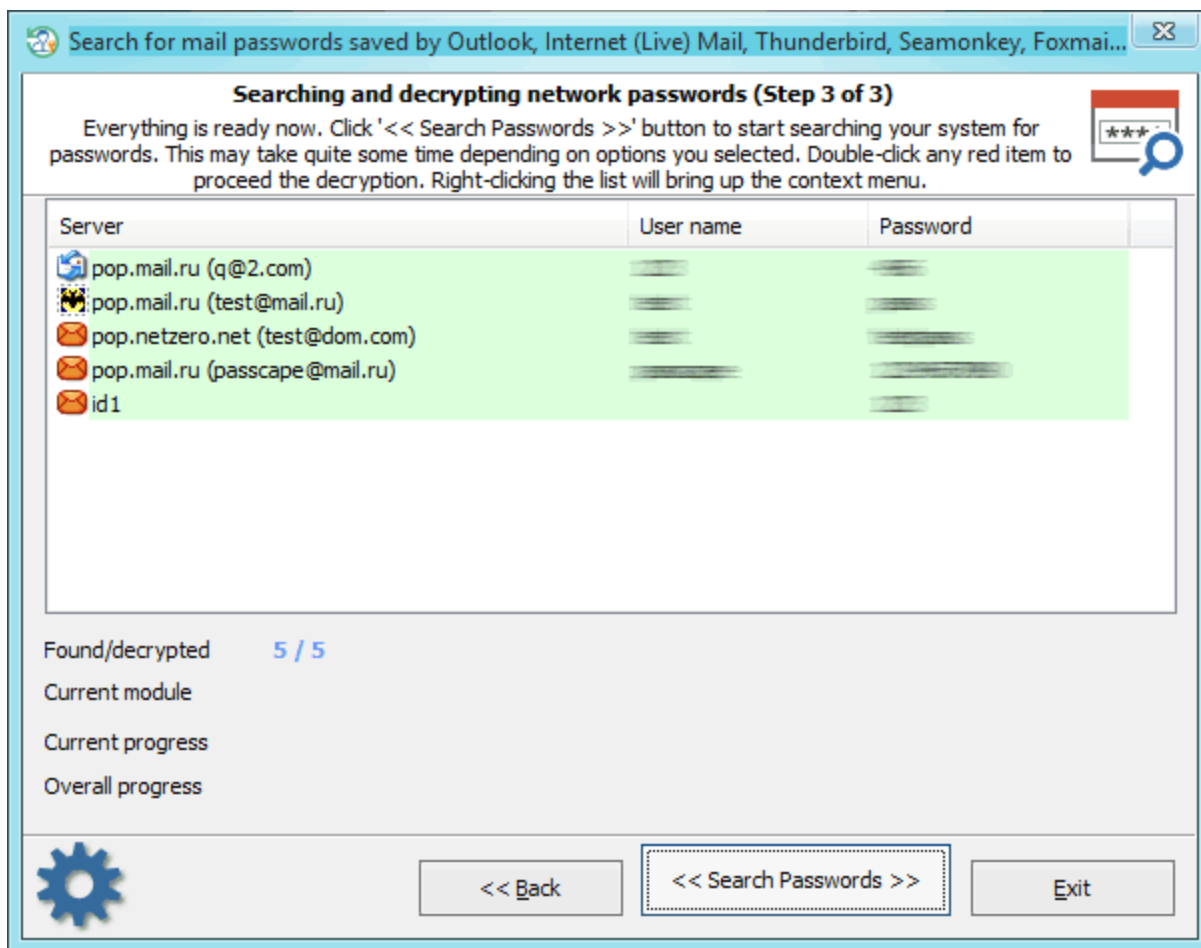
Internet Explorer 7-9

URL

Internet Explorer 7-9,

3.5.8.2

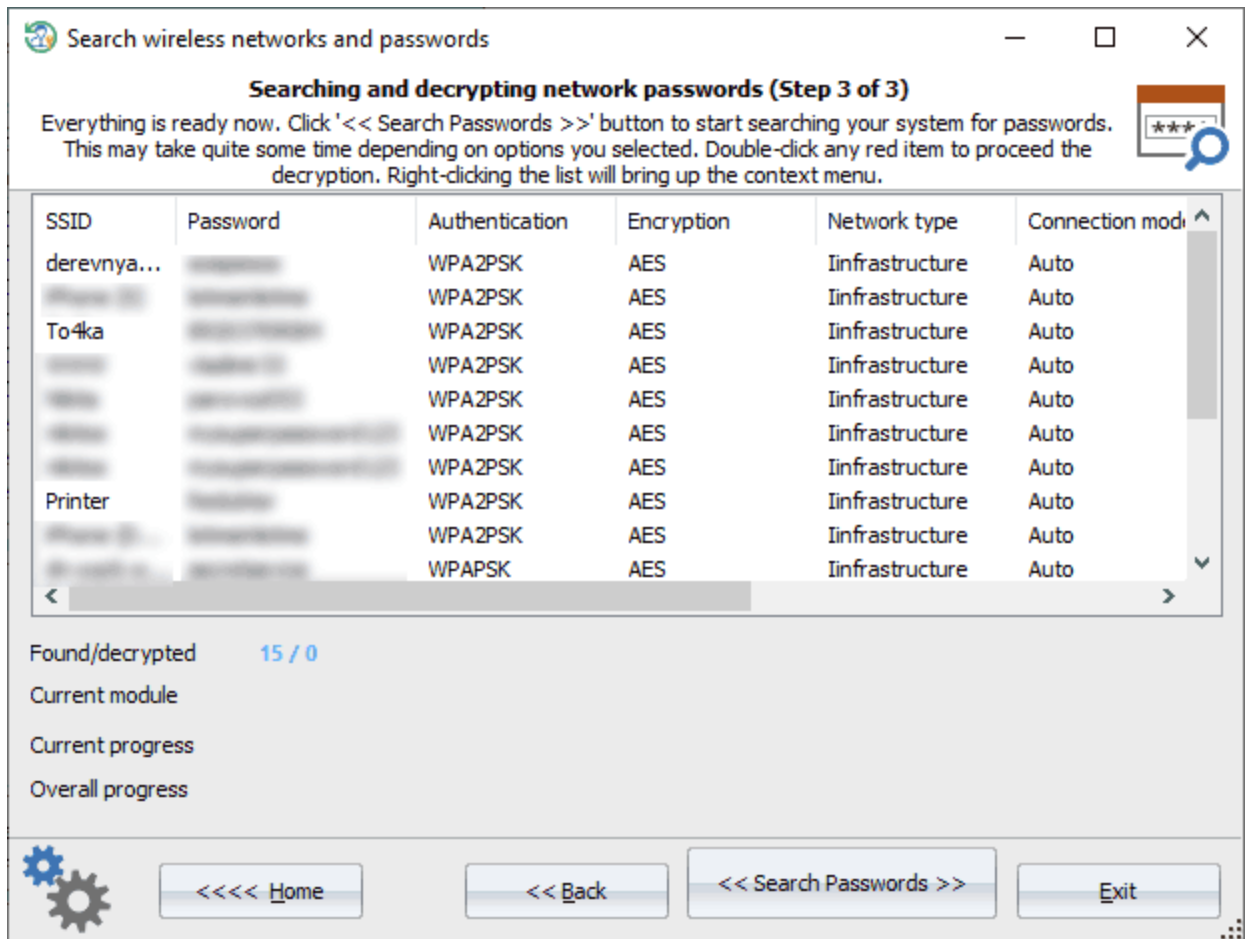
e-mail



- Outlook Express
- Microsoft Office Outlook

-
- , SQL ,
-
-
- : RAS, DSL, VPN . . .
- IE/Outlook/OE/FTP .
- WPA/WPA2
-
- VNC
- Tortoise SVN
- Open VPN
-
- DPAPI,
- : 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: IE/Outlook/Windows Mail, (Windows 8).
PIN/Picture
- DPAPI _____ ,
- DPAPI _____
- _____ !
- _____

3.5.8.4



()

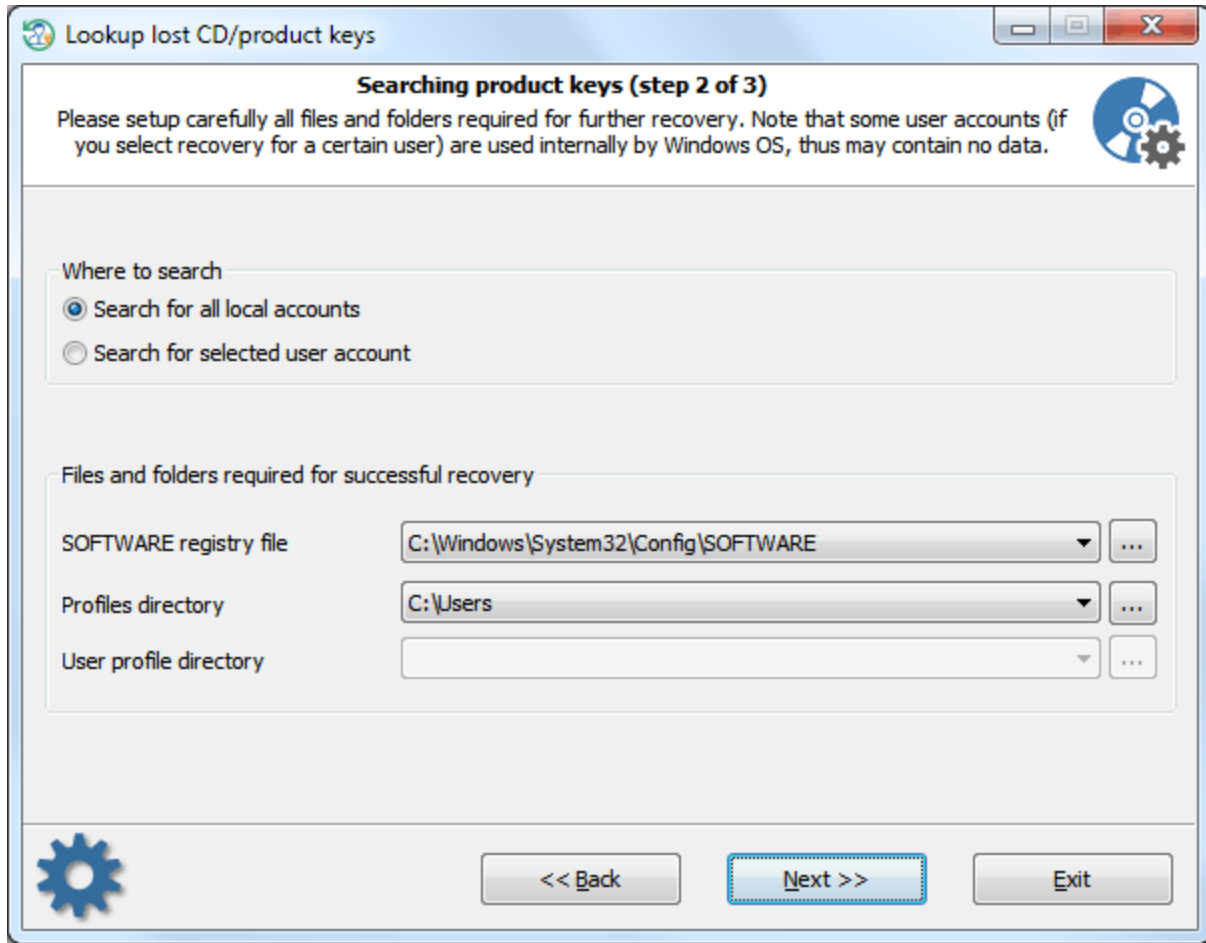
3.5.9

(),

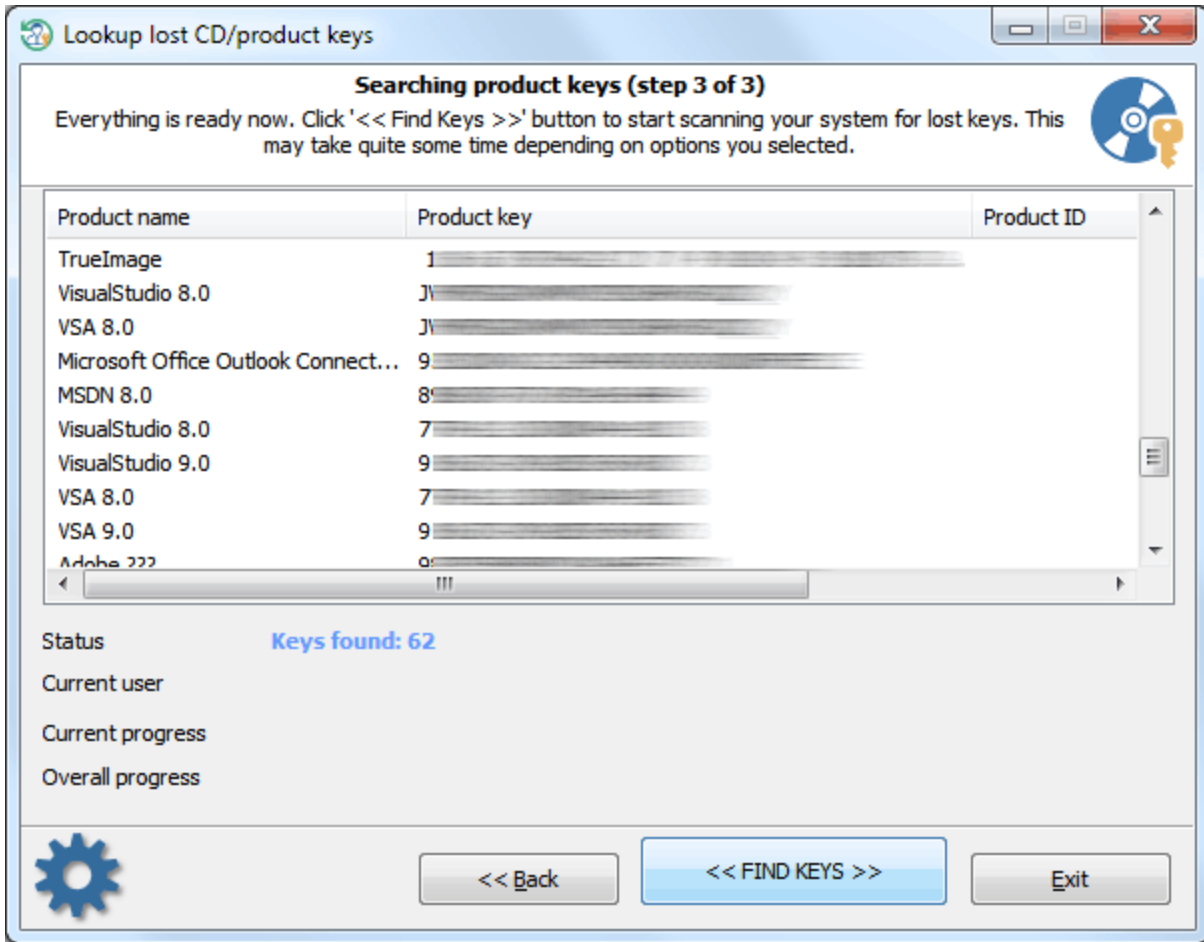
Windows,

, Reset Windows Password

1000



1. SOFTWARE, 'C:\Windows\System32\Config'.
Windows , 'D:\Windows', 'E:\Win'
2. Windows Vista , 'C:\Users'.
Windows XP 'C:\Documents and Settings'.
Windows,



'<<' '>>'

3.6

3.6.1

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	

 << Back **Next >>** Exit

Recent user activity

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


<< Back Next >> Exit

Recent user activity

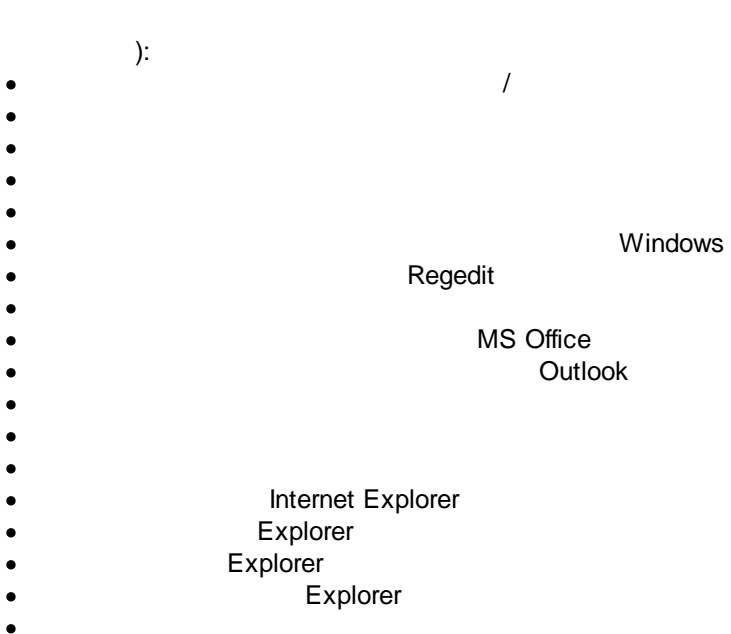
Extract and view history information (step 4 of 4)

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:\ProgramC
Wireless profile history	test1_enterprise	22.08.2018 13:11:46		D:\ProgramC
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		

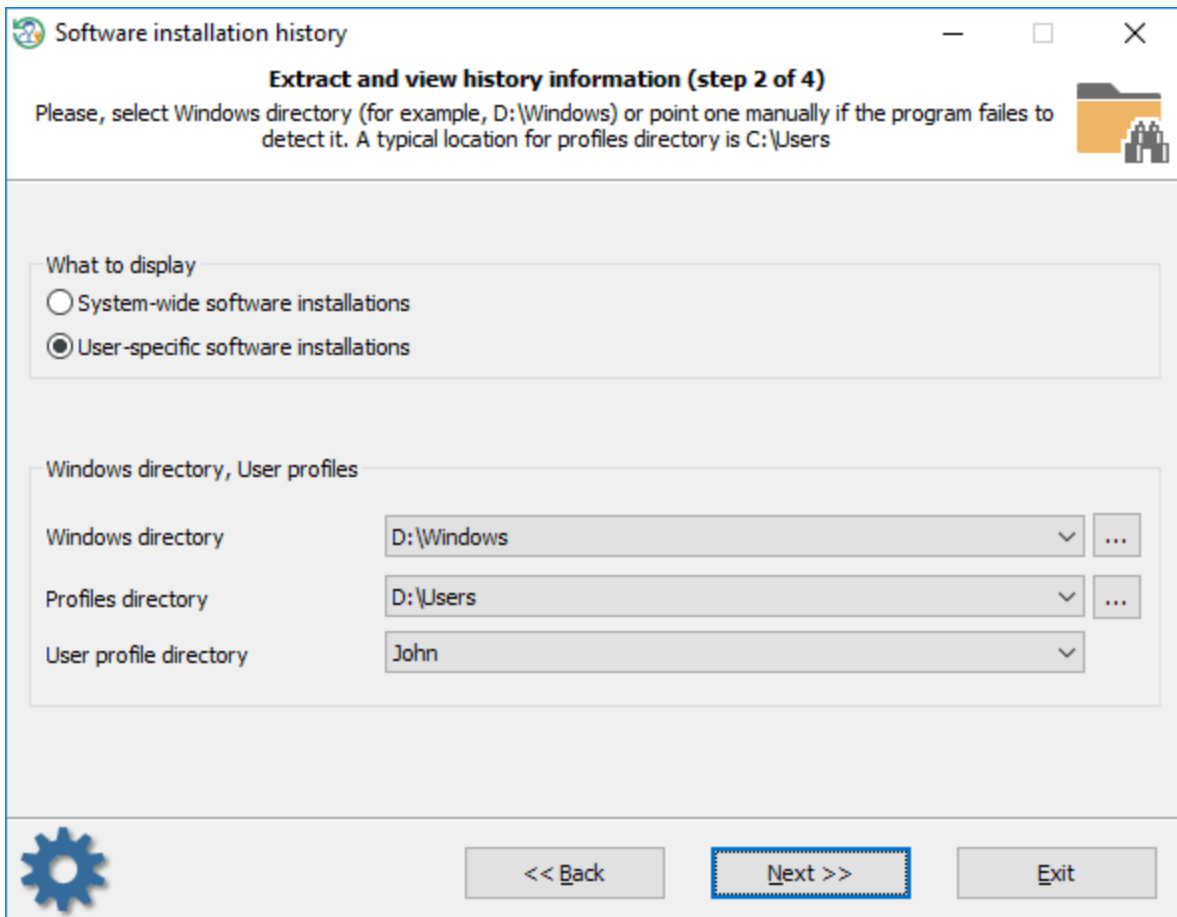
Settings icon: 

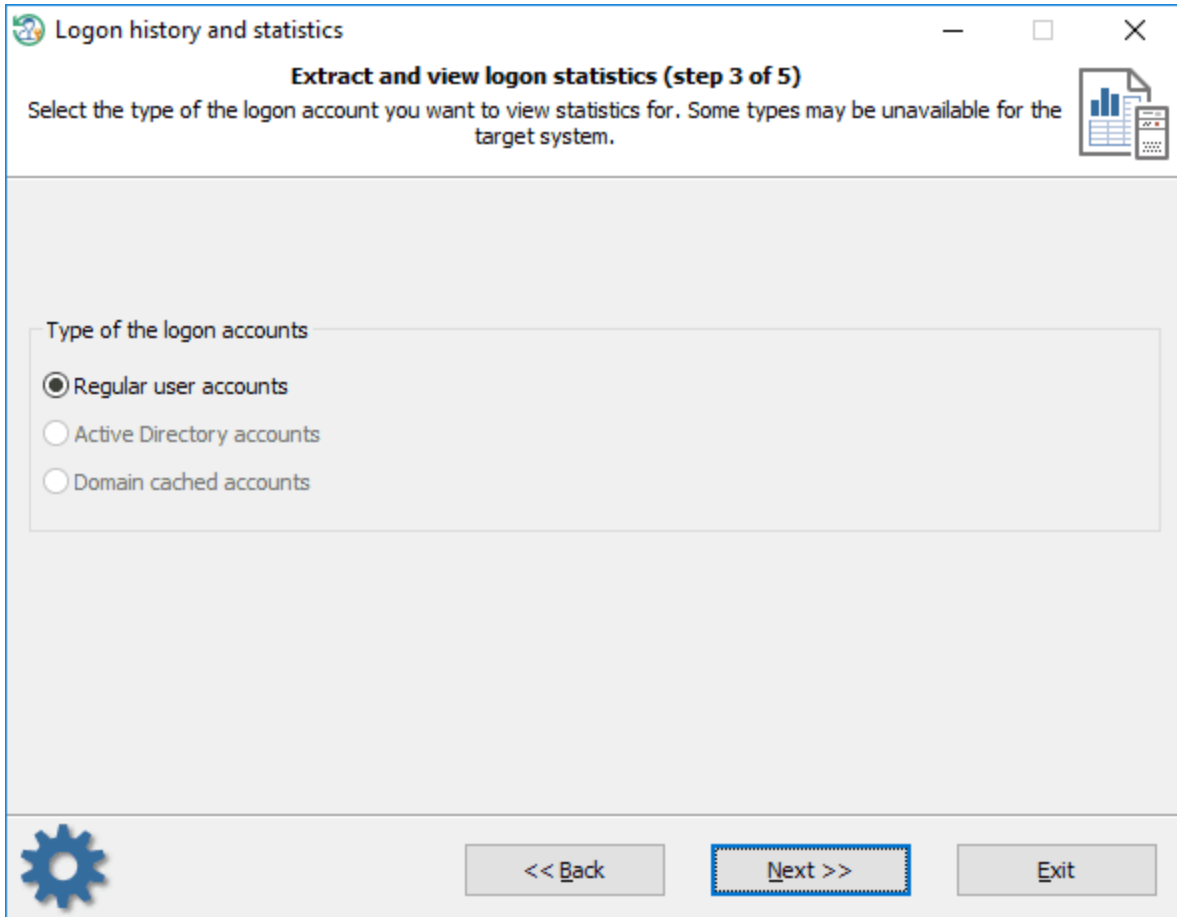
Navigation buttons: << Back, Exit



-
-
- Bluetooth
-
- Windows
-

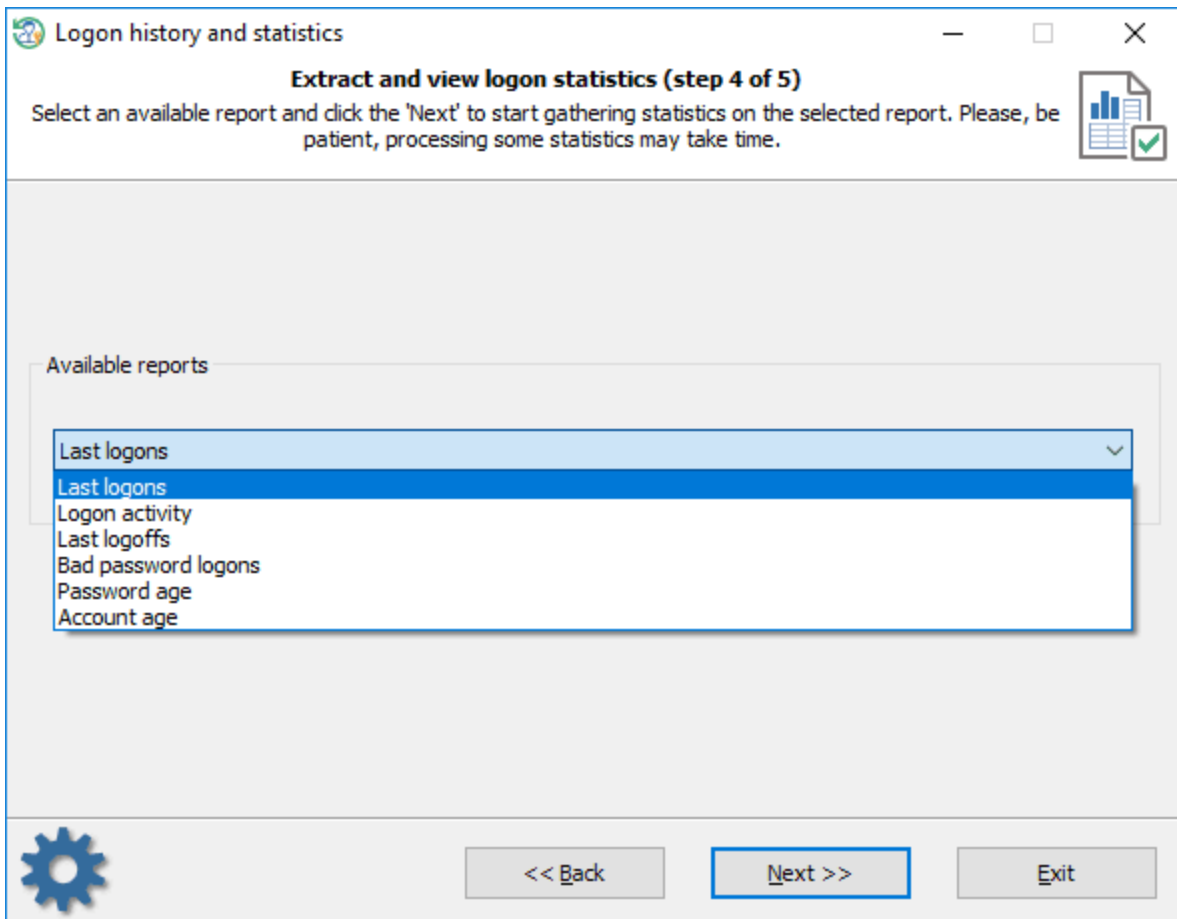
3.6.2 C





Windows
(

).



- Last logons -
- Logon activity -
- Last logoffs -
- Bad password logons -
- Password age -
- Account age -

Windows


Last logons

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.

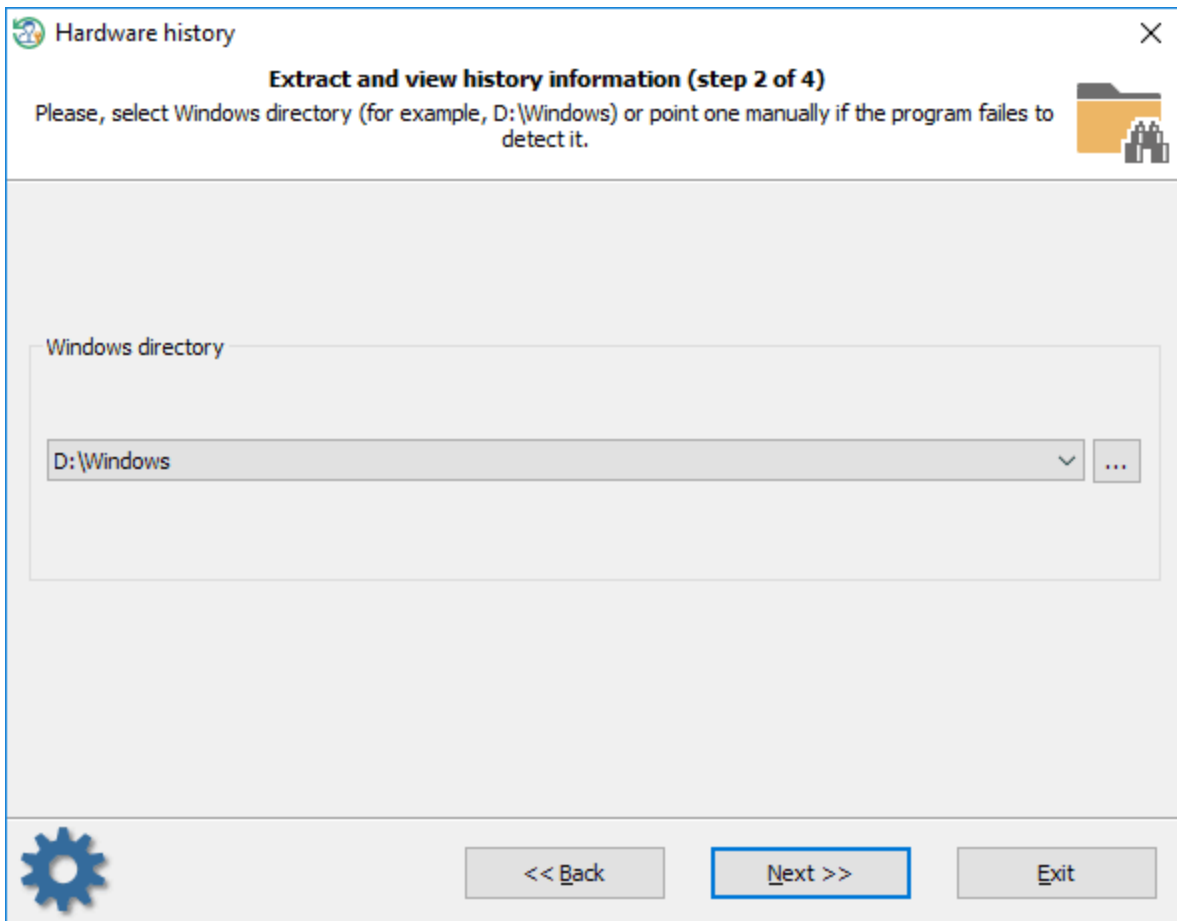
User name	Last logon	Days ago	RID	Account description
Administrator	21.11.2010 6:47:20	2 909	000001F4	Built-in account for administering the c
Guest	30.08.2013 10:05:53	1 896	000001F5	Built-in account for guest access to th
John	13.09.2015 17:34:29	1 151	000003E8	
test	04.10.2013 16:17:58	1 860	000003F0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

< >

 << Back Exit

3.6.3

Windows



Windows.

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


<< Back Next >> Exit

Hardware 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.

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

Settings icon: 

Navigation buttons: << Back, Exit

3.6.4

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 fails 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	

 << Back Next >> Exit

Software installation history

Extract and view history information (step 3 of 4)
Set up additional output filters to skip unnecessary items.


Output filter

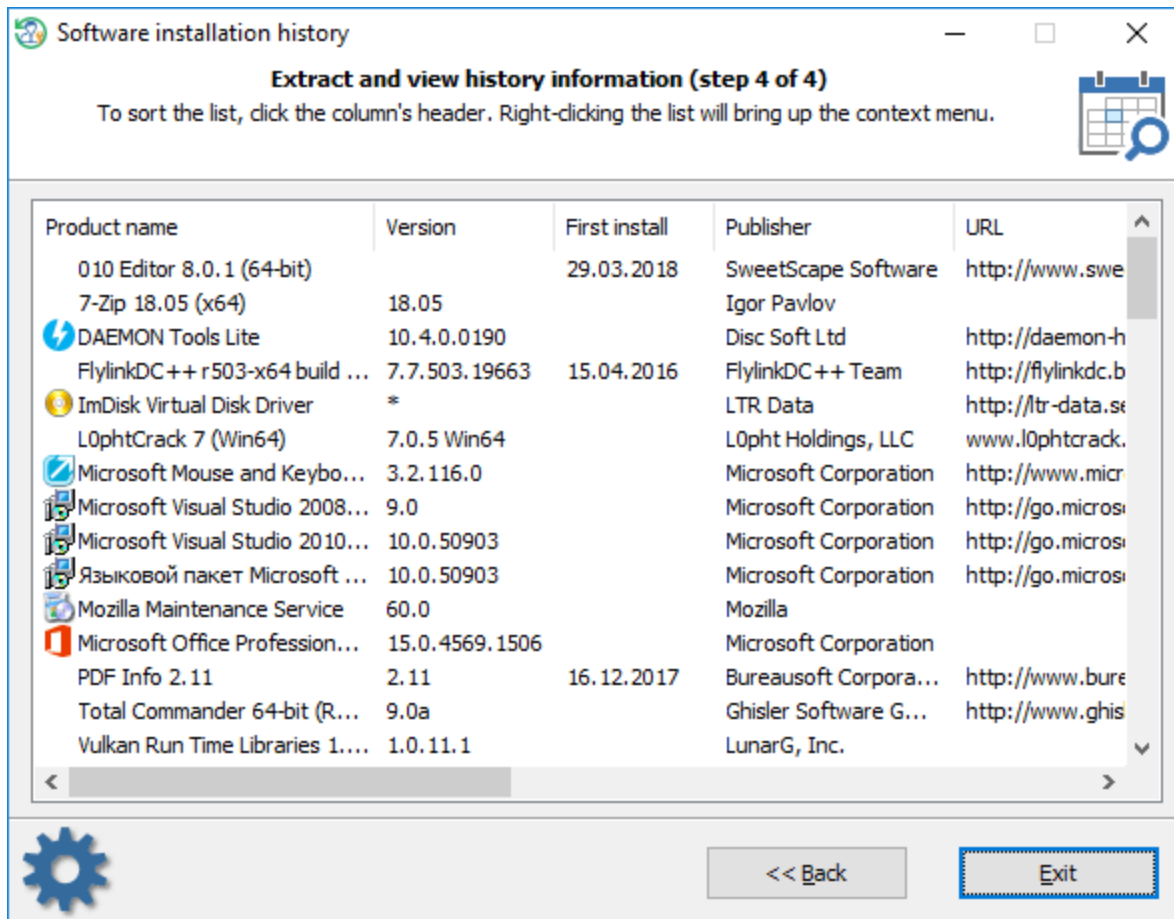
Show all
 Show items created between given dates only

From date: 08.11.2018 11:22:44
To date: 08.11.2018 11:22:44

Advanced output options

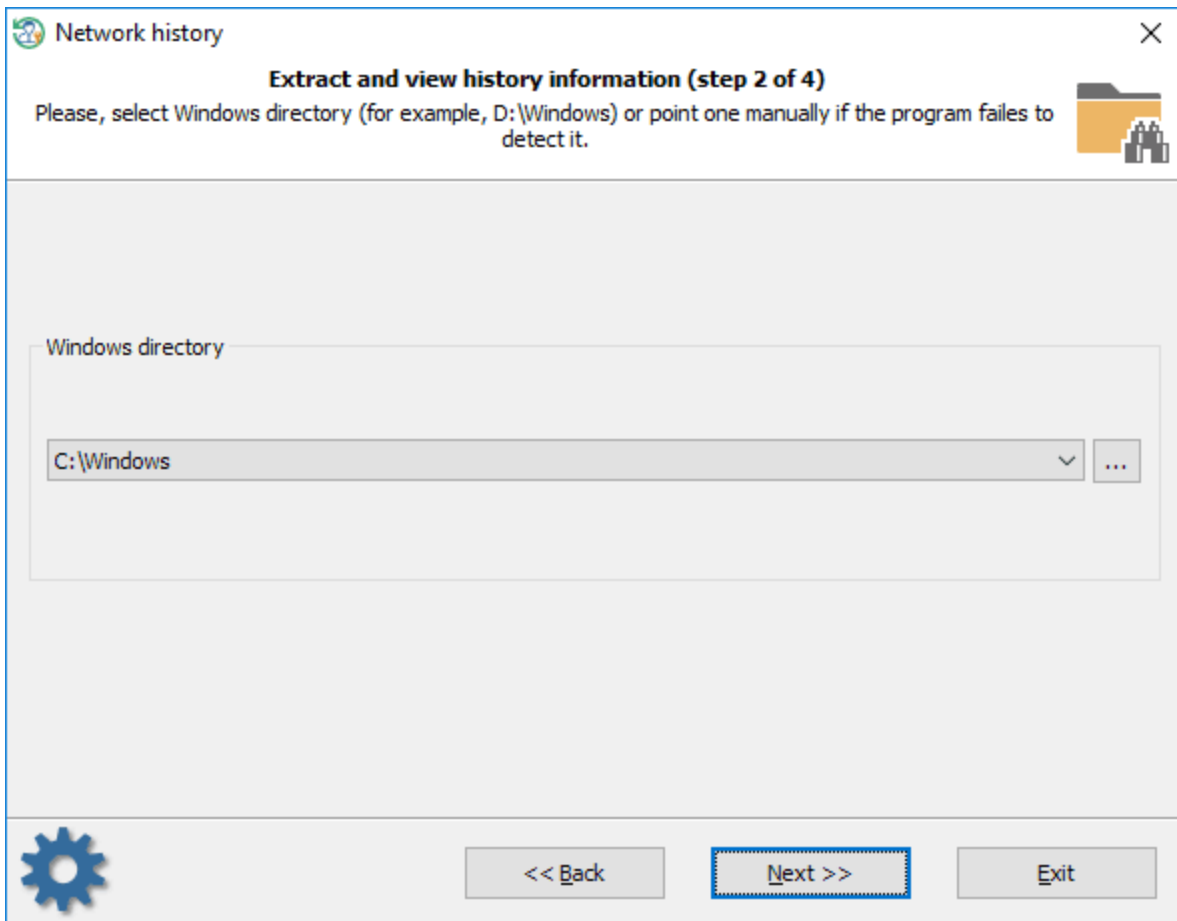
Do not show system components

 << Back Next >> Exit



3.6.5

Windows



Windows.

Network history

Extract and view history information (step 3 of 4)
Set up additional output filters to skip unnecessary items.

Output filter

Show all

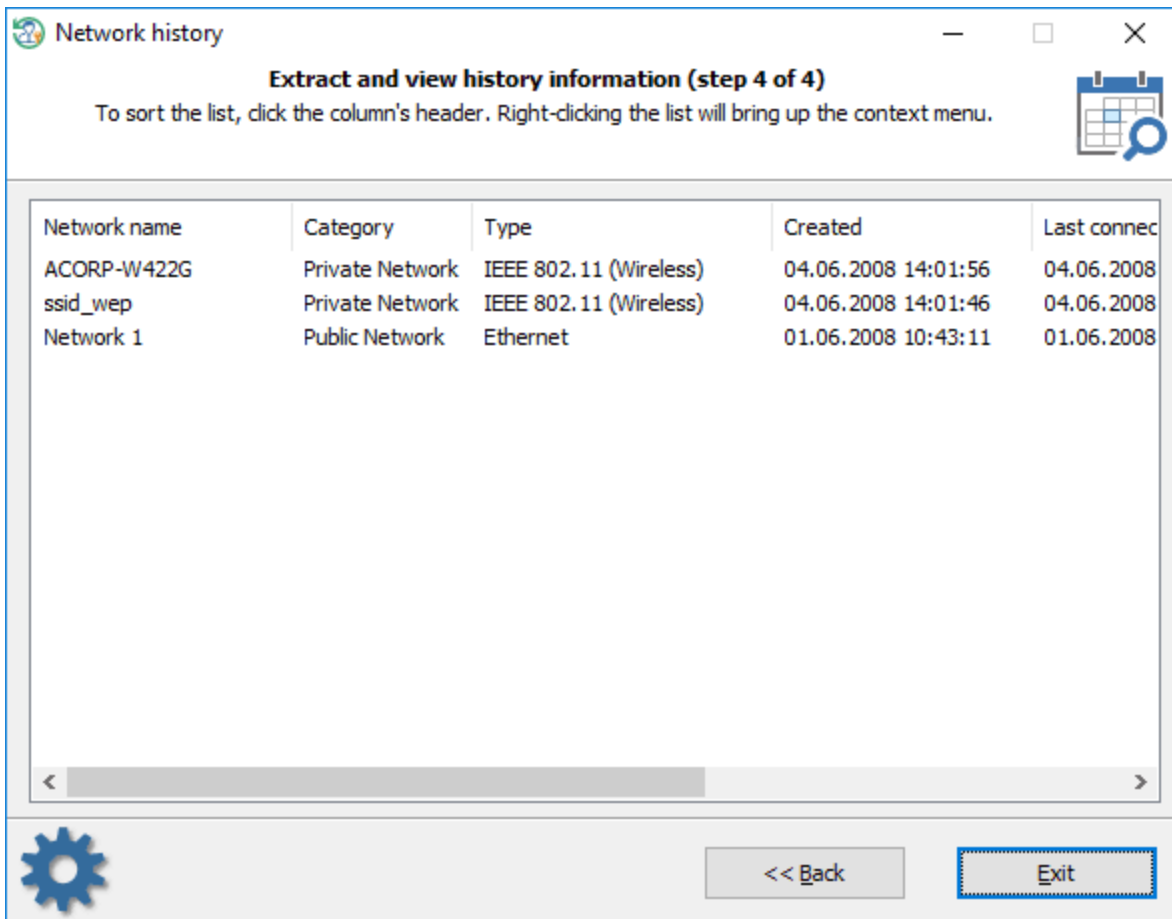
Show networks which creation date fits into the specified range

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

<< Back Next >> Exit



3.6.6

Windows
 Microsoft,
 'C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent' -
 Windows
 Windows > > >
 Windows 'Recent'.

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

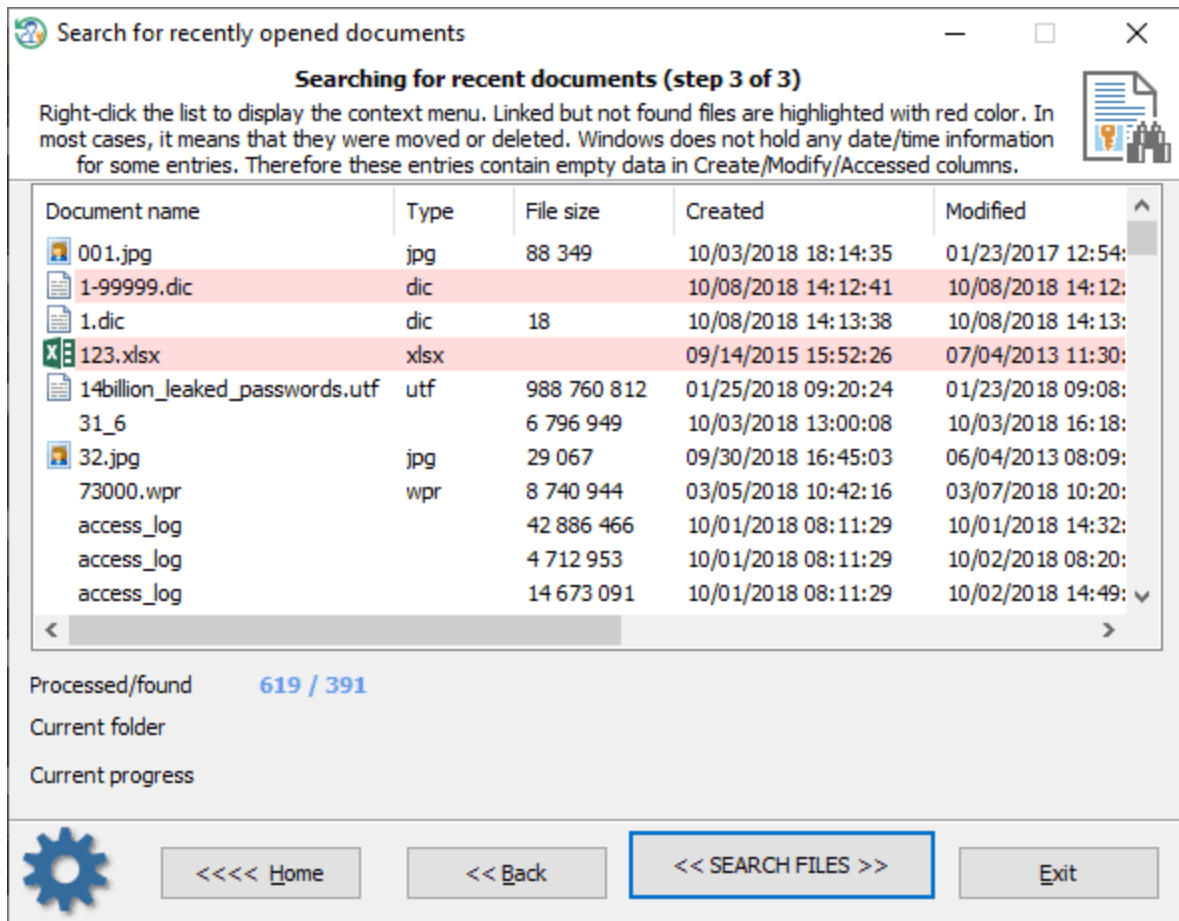
System-wide data

User-specific data

Windows directory, User profiles

Windows directory	D:\Windows	▼	
Profiles directory	D:\Users	▼	
User profile directory	John	▼	

 <<<< Home << Back **Next >>** Exit



<< >>

3.6.7

Edge, Opera, Mozilla (Firefox, SeaMonkey . . .), Chromium (Google Chrome, Internet Explorer 4-11, YandexBrowser, 360 Extreme Explorer . . .) Web

Web history

Extract and view history information (step 2 of 5)

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

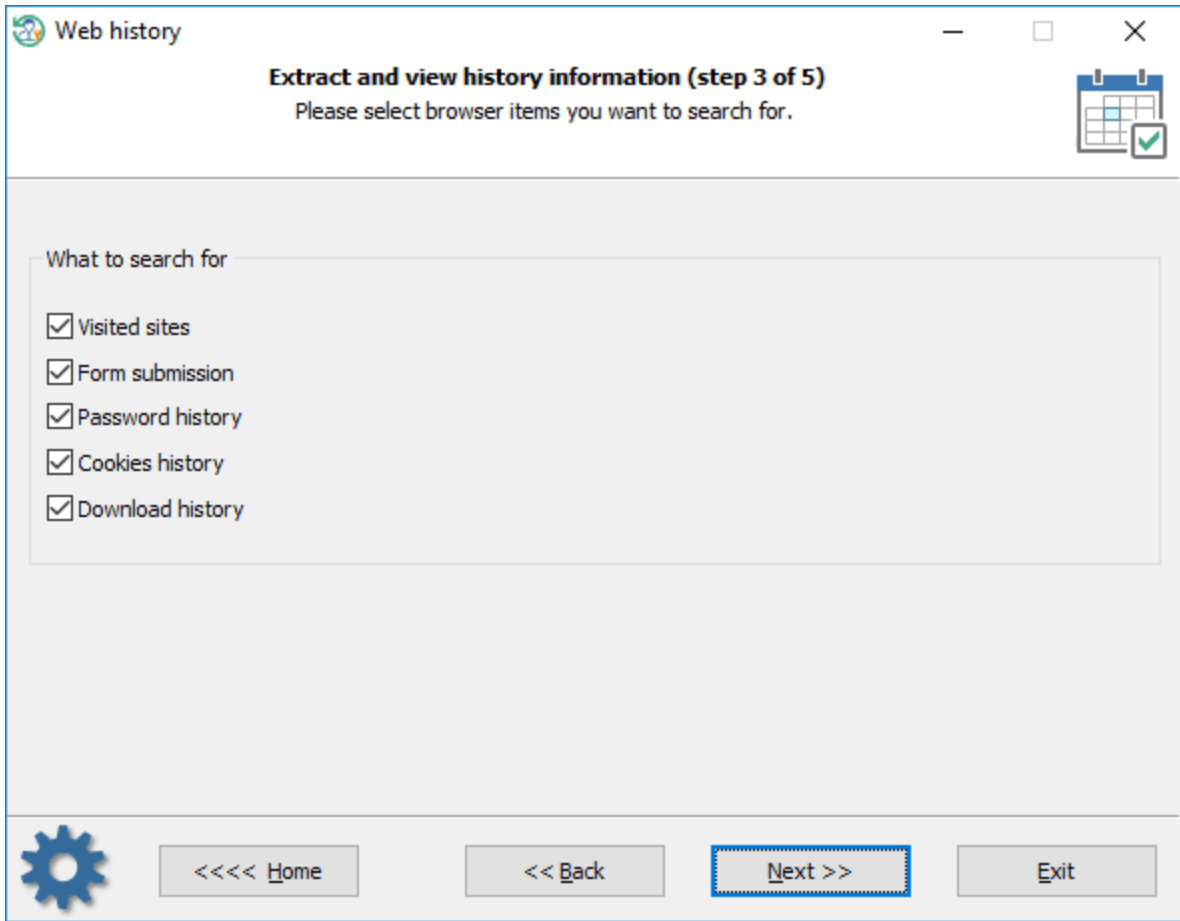
Web history for all users

User-specific history

Windows directory, User profiles

Windows directory	D:\Windows	...
Profiles directory	D:\Users	...
User profile directory	John	

Home <<<< << Back Next >> Exit



- Web :
- ()
- ()


Web history

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

 <<<< Home << Back **Next >>** Exit

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...

Navigation: <<<< Home << Back Next >> Exit

?

Internet Explorer

index.dat. index.dat : URL-
 (Client UrlCache MMF) - , cookie . .

Internet Explorer 5. index.dat , ,

- C:\Users\<USERNAME>\AppData\Local\Microsoft\History
 - C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\History
 - C:\Users\<USERNAME>\AppData\Roaming\Microsoft\Internet Explorer\UserData
- , Windows XP,

Internet Explorer - URL
 HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

Microsoft Edge

Internet Explorer, Microsoft Edge
 WebCacheV01.dat, cookie,
 index.dat. WebCacheV01.dat
 C:\Users\<<USERNAME>\AppData\Local\Microsoft\Windows\WebCache

Opera ()
 global_history.dat, global.dat vlink4. dat
 ().

Chrome (Chromium)
 URL- SQLite history. history
 C:\Users\<<USERNAME>\AppData\Local\Google\Chrome\User Data\Default

Firefox (Mozilla)
 Web history.dat (mork) places.sqlite
 C:\Users\<<USERNAME>\AppData\Roaming\Mozilla\Profiles\owec6tnk.default

?

Internet Explorer

Internet Explorer v4-6

HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

Internet Explorer v7-9

(IE 4-6),

, IE 7-9

URL-

Reset Windows Password

IE 7-9.

[PIEPR.](#)

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage1

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\FormData

Internet Explorer v10+ Microsoft Edge

[Windows](#)

[Vault](#)

[DPAPI.](#)

RWP

Windows Vault

C:\Users\<<USERNAME>\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28

Opera ()

C:\Users\<<USERNAME>\AppData\Roaming\Opera\Profile\typed_history.xml

C:\Users\<<USERNAME>\AppData\Roaming\Opera\Profile\search_field_history.dat

Chrome (Chromium)
 history Web Data, SQLite.
 Chrome:
 C:\Users\<>USERNAME>\AppData\Local\Google\Chrome\User Data\Default

Firefox (Mozilla)
 formhistory.dat () formhistory.sqlite
 C:\Users\<>USERNAME>\AppData\Roaming\Mozilla\>PROGRAM>\Profiles\>PROFILENAME>.
 C:\Users\<>USERNAME>\AppData\Roaming\Mozilla\Firefox\Profiles\owec6tnk.default\formhistory.sqlite

?

Internet Explorer

Internet Explorer v4-6
 HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

Internet Explorer v7-9
 HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2

Internet Explorer v10:
 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

IE HTTP basic authentication
 (Windows Vista). DPAPI
 C:\Users\<>USERNAME>\AppData\Roaming\Microsoft\Credentials

, Reset Windows Password Chrome
 Internet Explorer,

Opera ()
 wand.dat
 C:\Users\<>USERNAME>\AppData\Roaming\Opera\Profile\wand.dat

Chrome (Chromium)
 Chromium Windows DPAPI
 Login Data, SQLite.
 Google Chrome:
 C:\Users\<>USERNAME>\AppData\Local\Google\Chrome\User Data\Default>Login data

Firefox (Mozilla)
 Mozilla
 signons.txt. 2 signons2.txt, "#2C"
 signons3.txt "#2D" 3
 signons.sqlite Firefox v32.x
 - logins.json, JSON.

\Users\

C:

3.6.8

IP

(

IP-

),

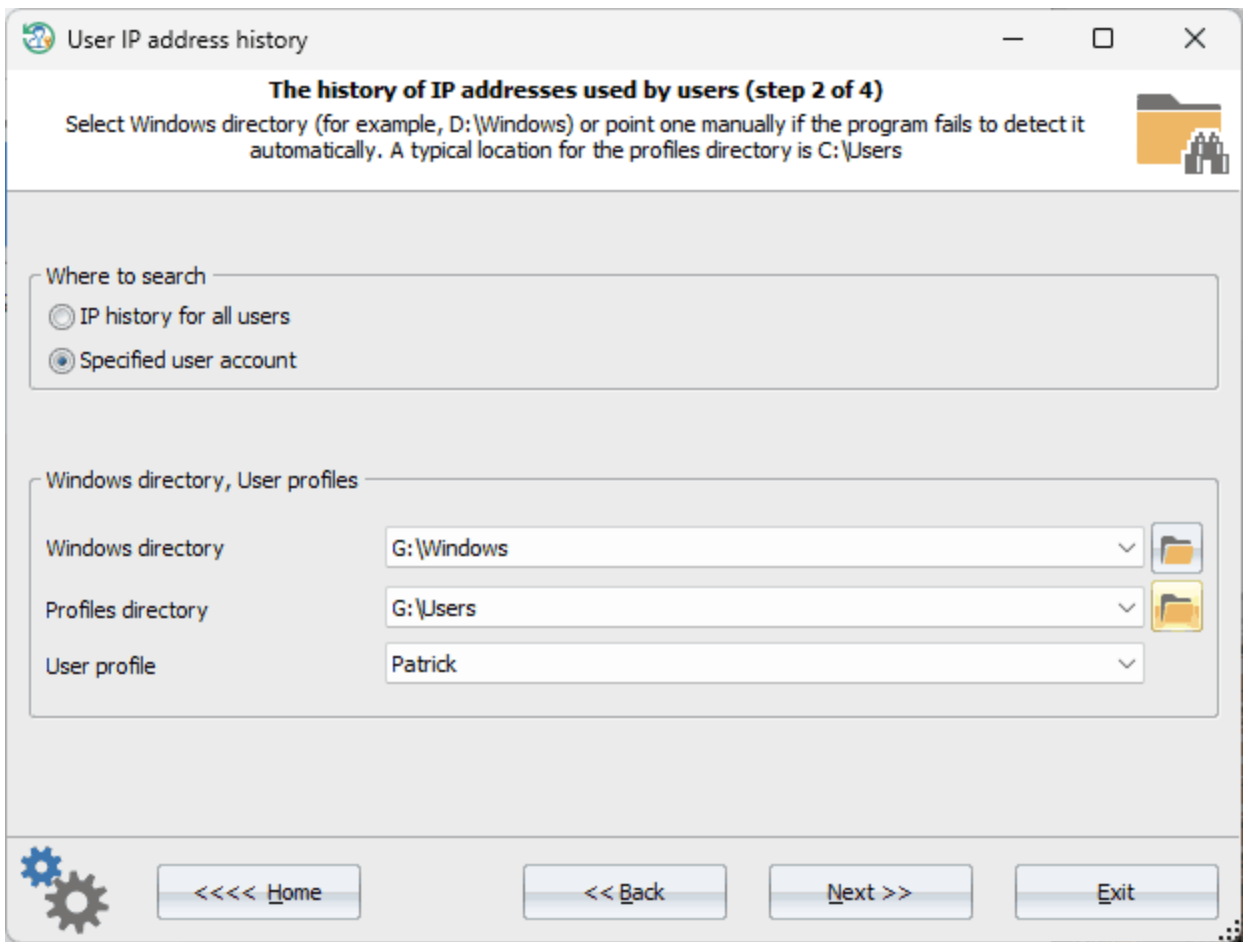
Windows.

IP-

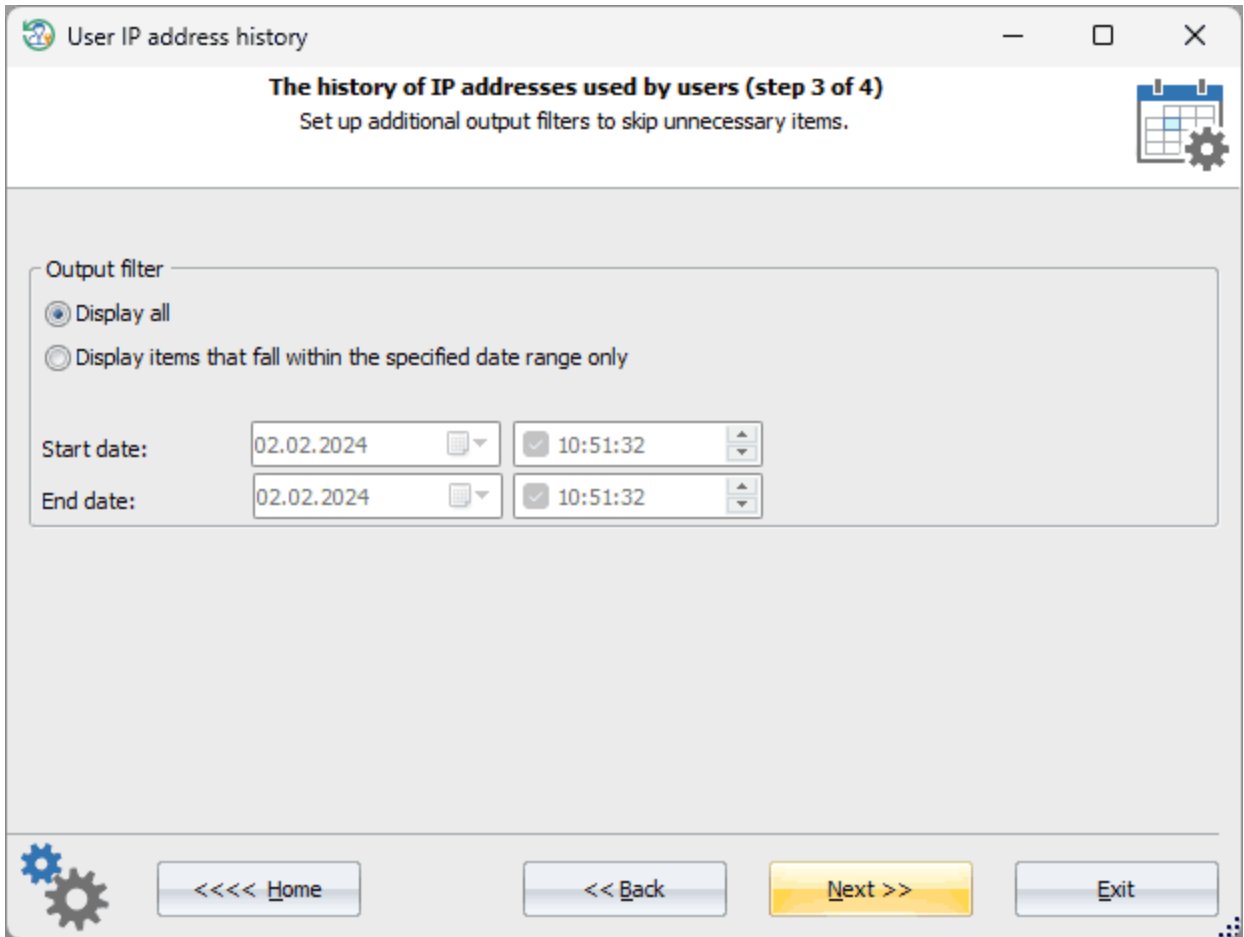
, Microsoft

IP-

IP



IP-



IP

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

Navigation: Home, Back, Next, Exit

IP

Windows

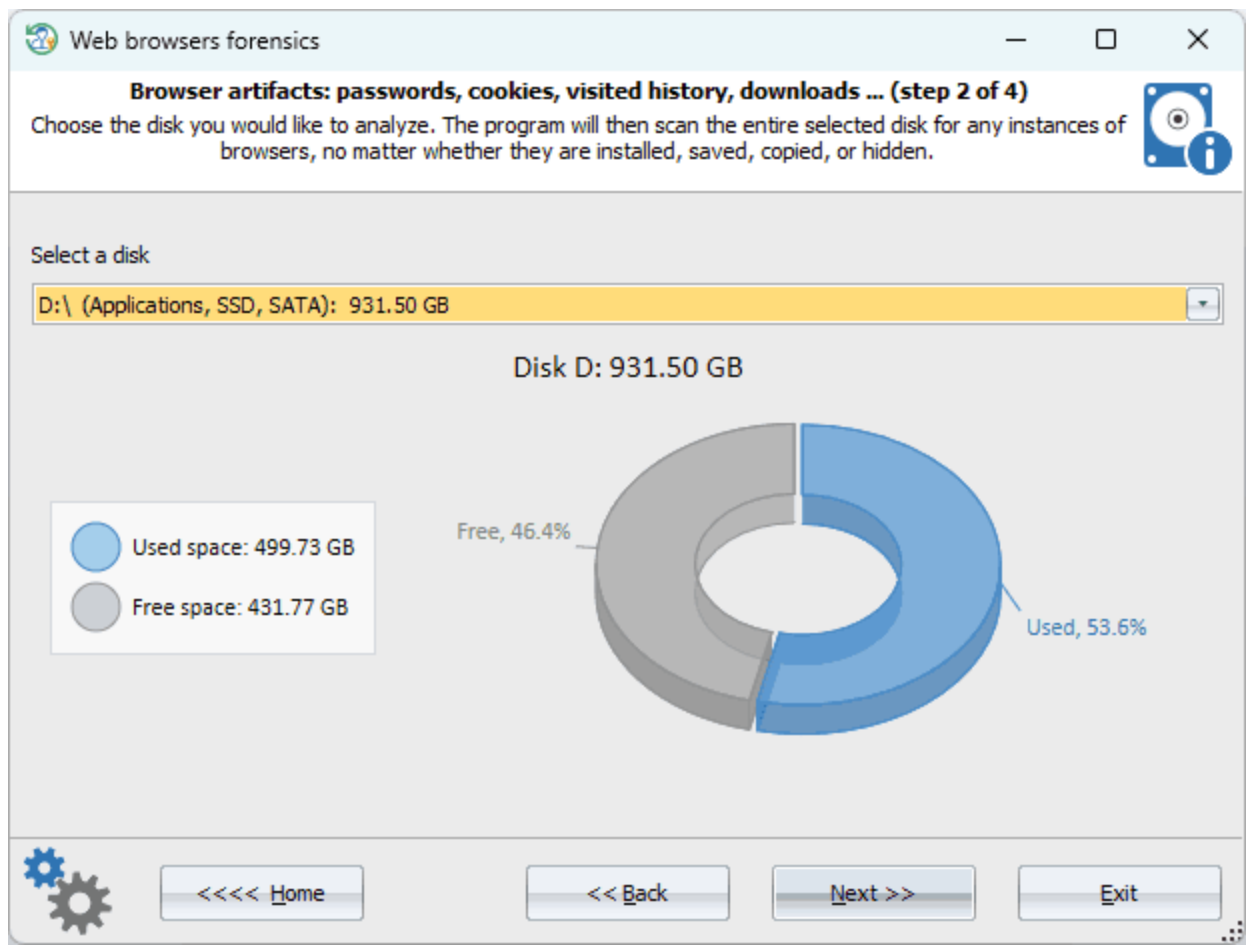
IP-

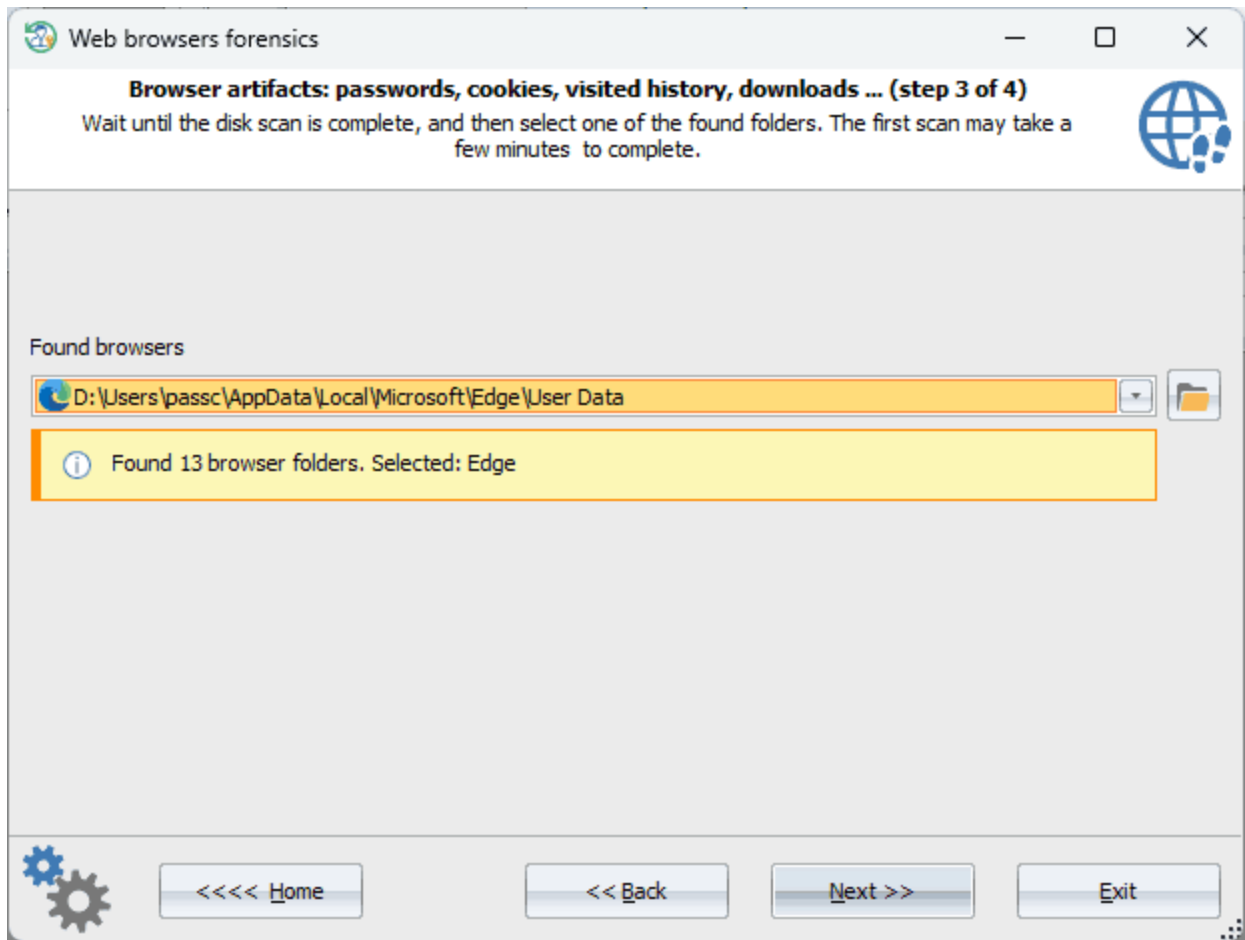
HTML

3.7

3.7.1

- Chromium,
- Windows.
- cookie,






- URL- : URL-
 - Chromium).
 - Chromium).
 - Chromium).
- Chromium Mozilla.

3.7.2

Windows
 - AMCache,
 . AMCache Windows 7.
 BCF.
 %WINDIR%
 \appcompat\Programs. AMCache.hve RecentFileCache.bcf -
 BCF

Windows

 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		

 <<<< Home << Back **Next >>** Exit

Windows,

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
wifpr.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


<<<< Home
<< Back
<< SEARCH FILES >>
Exit

<<

>>

HTML

3.7.3

Windows

Windows 10,

1803.

Windows 10

->

->

->

Windows

<USER_PROFILE>\AppData\Local\ConnectedDevicesPlatform

CPDS

CPDS,

Connected Platform Device Settings.

JSON,

.CPDS,

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

<<<< Home << Back **Next >>** Exit

Windows

Windows 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>	<All>
notepad.exe		Clipboard...	2022.02.22 16:39:45	2022.02.22 16:39:45			%System
notepad.exe		Clipboard...	2022.02.22 16:39:58	2022.02.22 16:39:58			%System
Command Prompt		Opening	2022.01.11 15:20:21				%System
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	%System
cmd.exe		Using	2022.02.07 08:54:08	2022.02.07 08:56:10	94	122	%System
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				Micromen

Home <<<< Back << Next >> Exit

Excel-

Application -

Document name -

Activity type -

/ /URL,

/ /URL,

Activity started -

Activity ended -

Active usage -

()

Total usage -

()

Application path -

Document location - (/)
Parent application - . ,
Source host - URL- ,
Clipboard content - Windows (**Activity type -**)
User - , , 3
Account type - : ,
User status - ,
User timezone - , ,
Device - (,),
Status - , : , ,

3.7.4

Windows Media

Windows Media
 Windows Photos. Windows Photos
 Windows Photos
 Windows 10
 C:\Users\%username%
 \AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\LocalState\MediaDb.v1.sqlite
 C:\Users\%username%\AppData\Local\Packages\Microsoft.ZuneVideo_8wekyb3d8bbwe
 C:\Users\%username%\AppData\Local\Packages\Microsoft.ZuneMusic_8wekyb3d8bbwe

-
-
-
- ISO
-
-
-
-

/'visa' /

'visa'.

3.7.4.1.2


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	demotU888.jpg		1	42	43	4		C:\Users\Adi
121	Screenshot 2017-...	183		117	118		100%	C:\Users\Adi
122	hotdem_ru_6191...		2	40	40	4		C:\Users\Adi
123	hotdem_ru_9509...		3	91	91		100%	C:\Users\Adi
124	1352947747_06.j...			70	70		100%	C:\Users\Adi
125	de5a6b.jpg	141	1	121	121	3	0%	C:\Users\Adi
126	IMG_30062017_...			32	32	4		C:\Users\Adi

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





3.7.4.1.3

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	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





3.7.4.1.4


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	bam	Yes	4

Photos with selected tag: apple_watch.png

 C:\Users\Sofia\Pictures\apple_watch.png Confidence 13%



-
-
-
-

3.7.4.1.5

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

Home Back Next Exit

Windows Photo

-
-
-
-
-
-
-

3.7.4.1.6

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,



Navigation buttons: Home, Back, Next, Exit

EXIF,

-
-
-
-

3.7.4.1.7

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>
124	2018	5	18	1
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

Home <<<< Back Next >> Exit

3.7.4.1.8

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

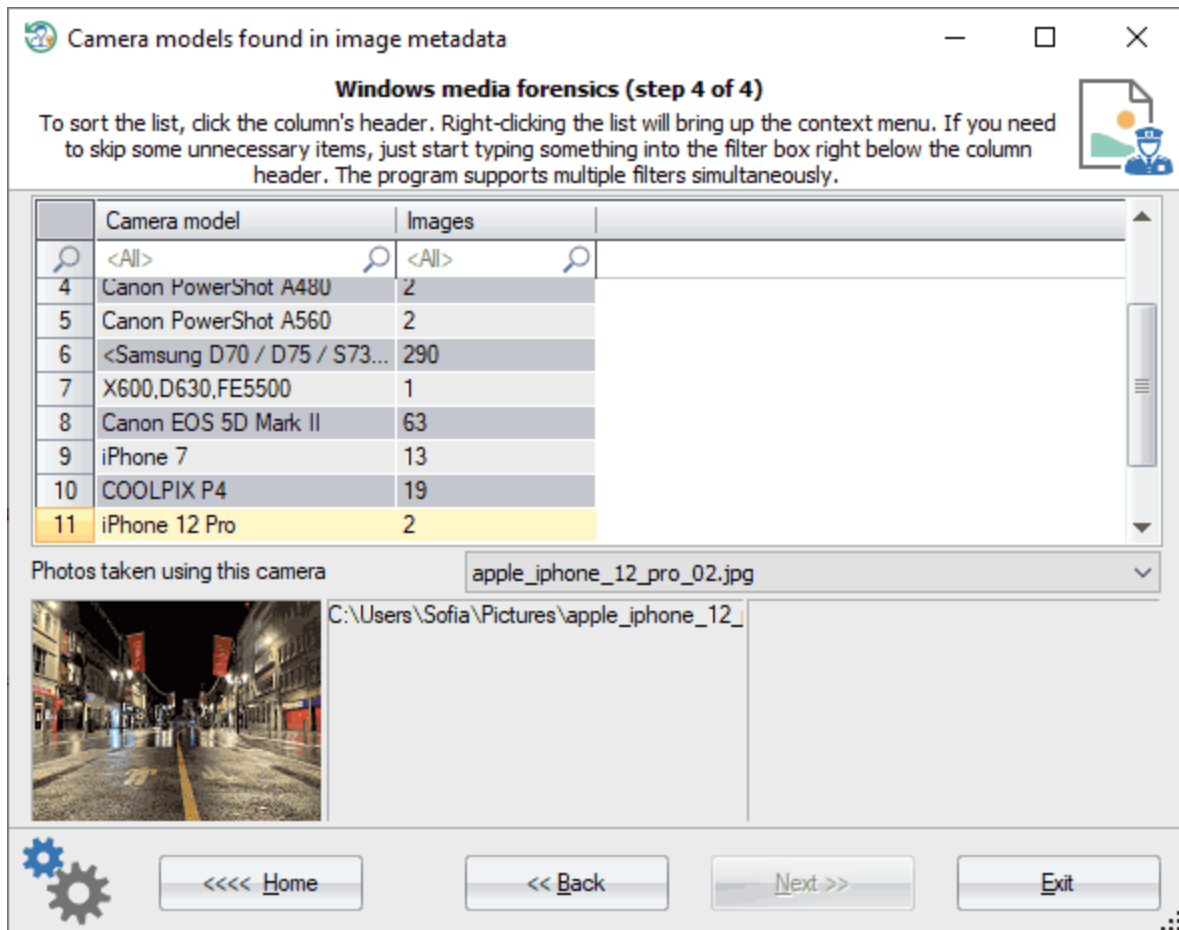
Photos taken using this camera: apple_iphone_12_pro_02.jpg

C:\Users\Sofia\Pictures\apple_iphone_12_



Navigation buttons: <<<< Home, << Back, Next >>, Exit

3.7.4.1.9



3.7.4.1.10

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 A...	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

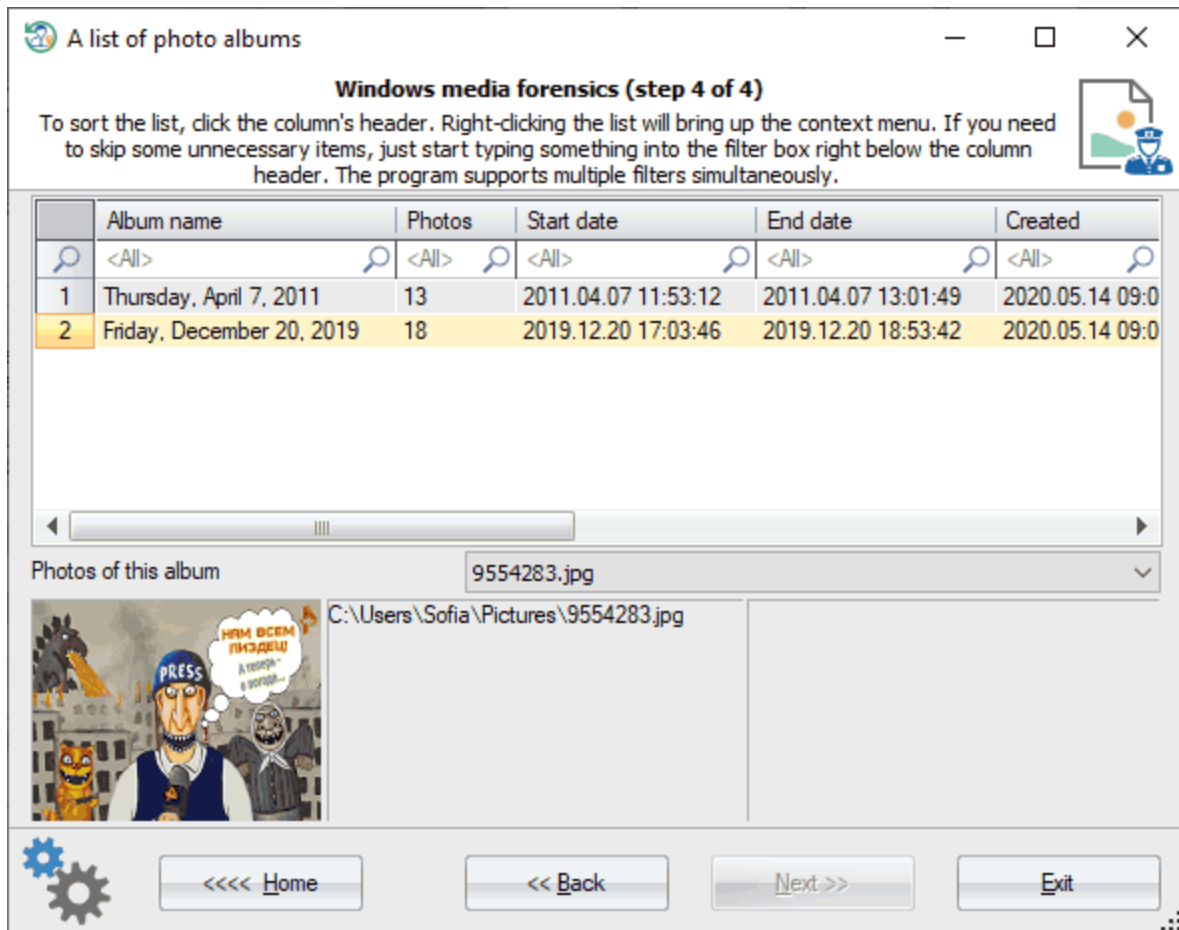
Photos edited using this application: 9554283.jpg

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



Navigation buttons: Home, Back, Next, Exit

3.7.4.1.11



Windows Photo.

3.7.4.2

3.7.4.2.2

A list of faces detected in video files

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

Home Back Next Exit

-
-
-
-
-
-
-
-

3.7.4.2.3

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



3

3.7.4.2.4


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%



-
-
-
-

3.7.4.2.5


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

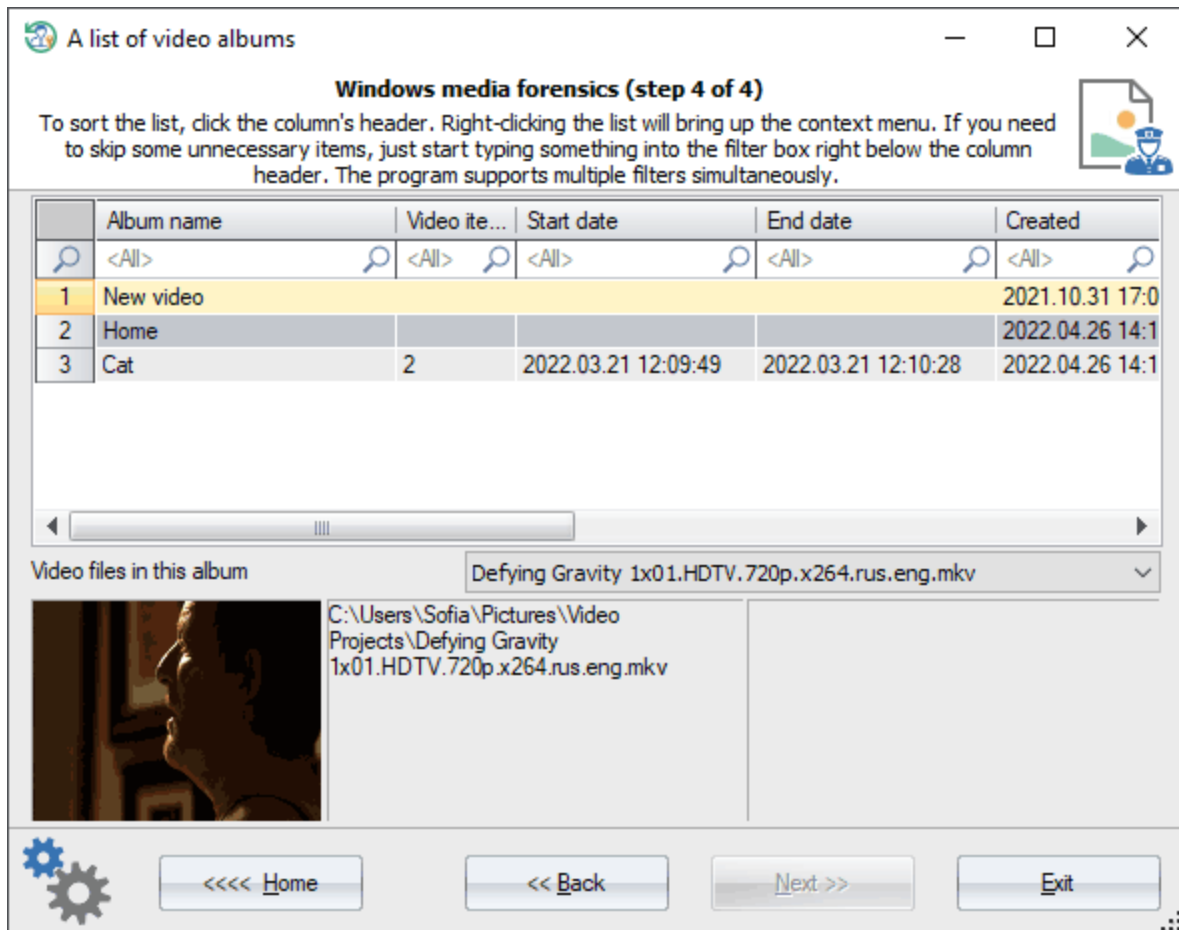


C:\Users\Sofia\Pictures\Video
Projects\Defying Gravity
1x01.HDTV.720p.x264.rus.eng.mkv

2019.07.30 13:19:47


<<<< Home
<< Back
Next >>
Exit

3.7.4.2.6



Windows Photo.

3.7.4.3

3.7.4.3.1

Album view statistics

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	

<<<< Home << Back Next >> Exit

3.7.4.3.2


Media view statistics

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

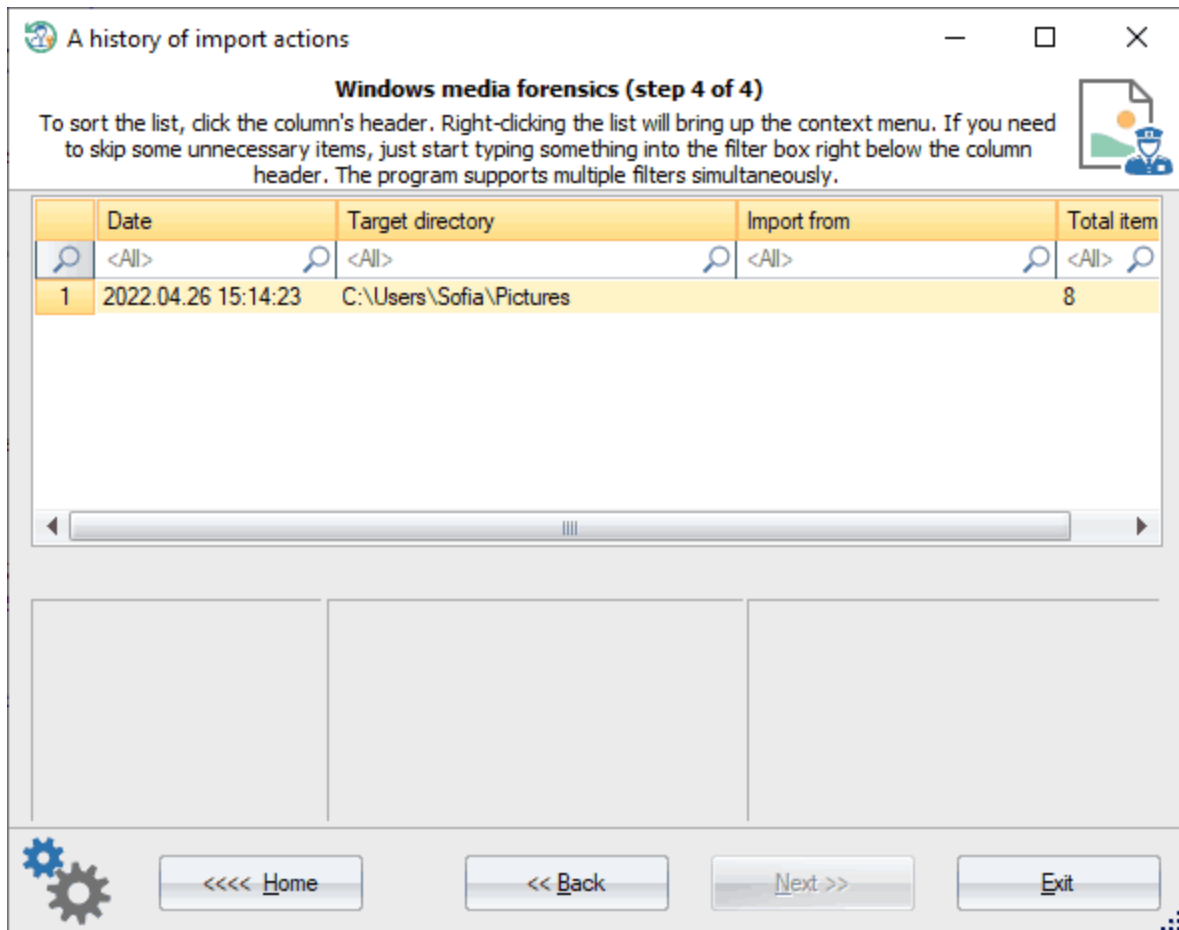
C:\Users\Sofia\Pictures\FUN\36 (2).jpg



Navigation buttons: Home, Back, Next, Exit

Windows.

3.7.4.3.3



Windows.

3.7.4.3.4

A history of search requests

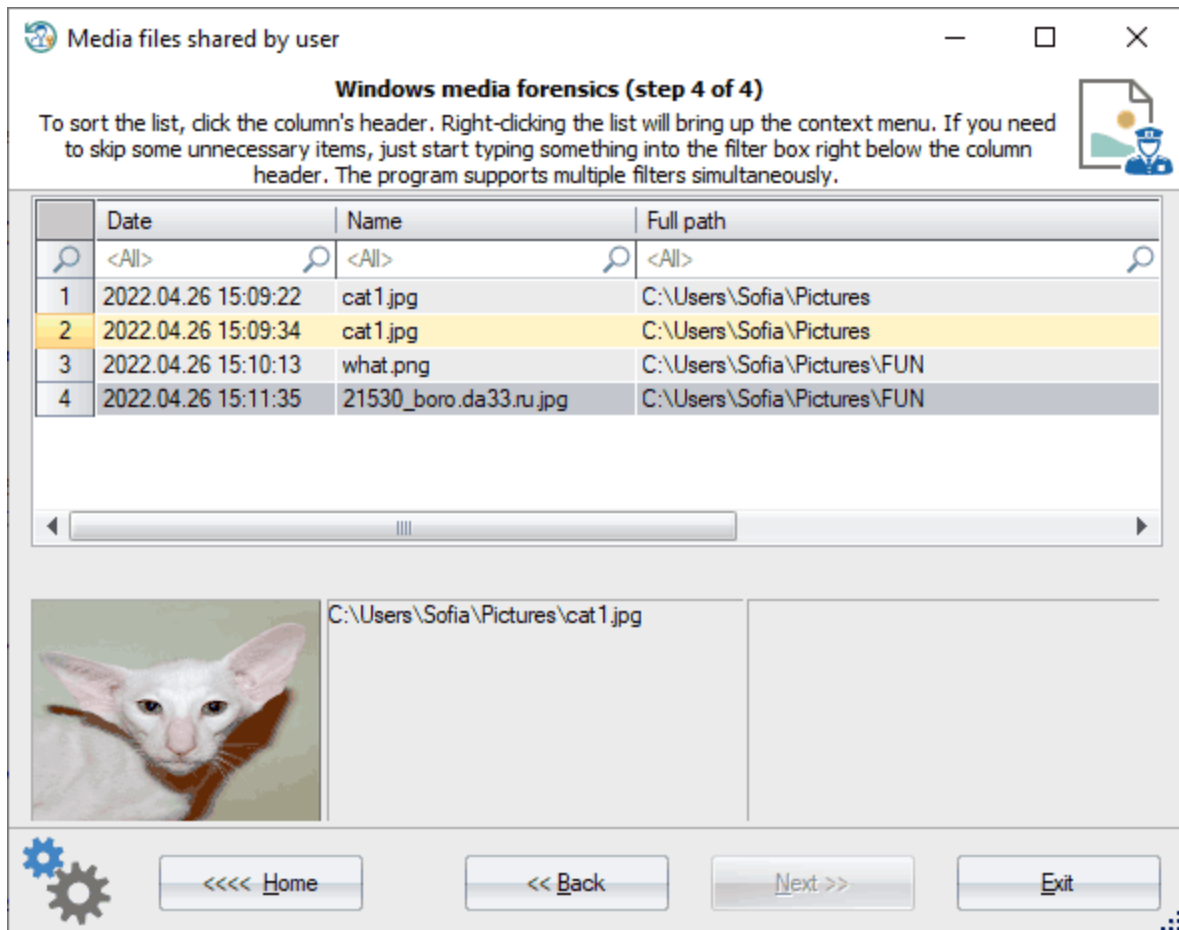
Windows media forensics (step 4 of 4)

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
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

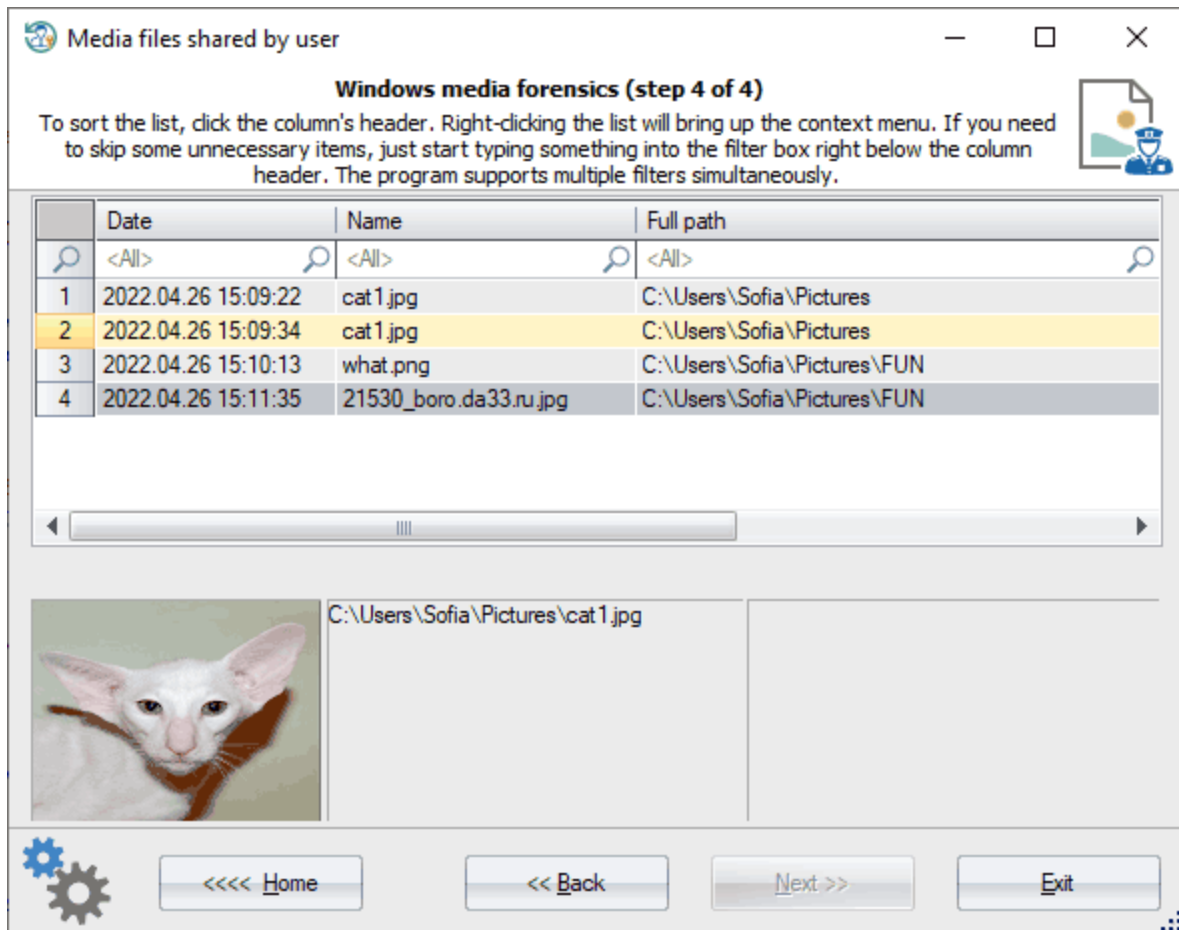
Windows Photo.

3.7.4.3.5



Windows.

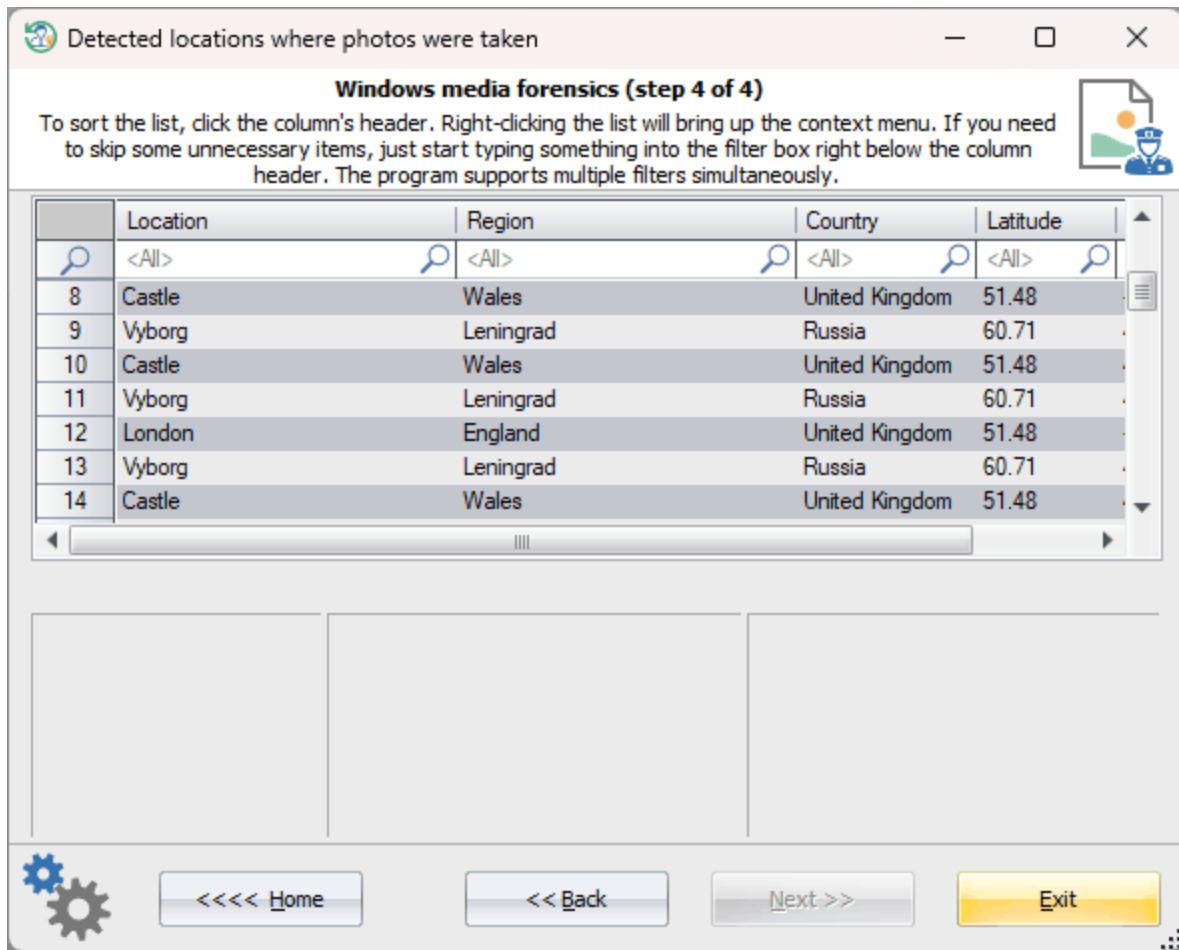
3.7.4.3.6



Windows.

3.7.4.4

3.7.4.4.2



-
-
-
-
-

3.7.4.4.3

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

C:\Users\Adm

- tsb.gif
- tsb.gif
- PeopleHDRBackground_AppleiPhone13Pro_DxOMark_05-00.jpeg

Home Back Next Exit

3.7.4.4.4


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:

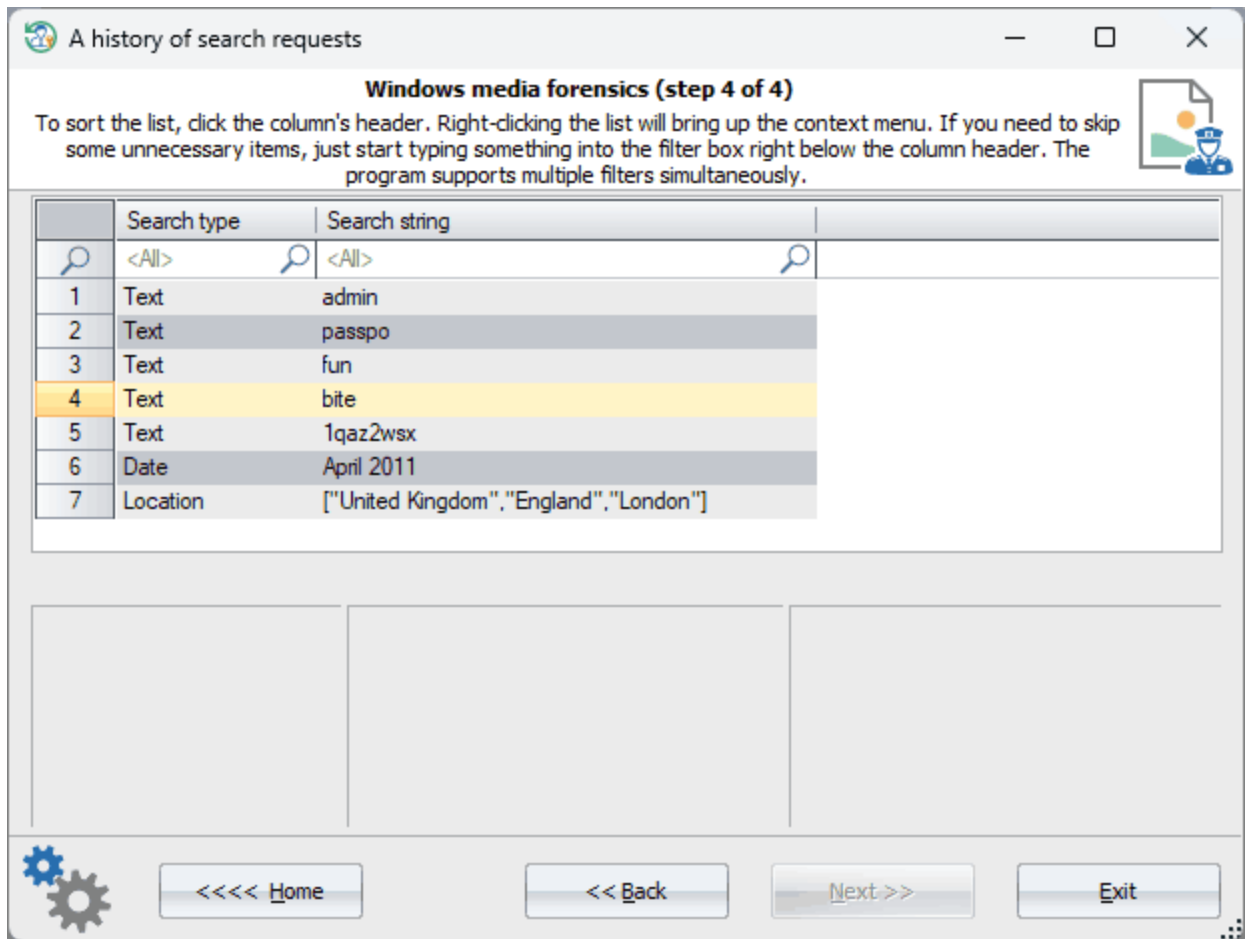
C:\Users\John\Pictures\Imported\IMG_1174.I



Photos.

3.7.4.5

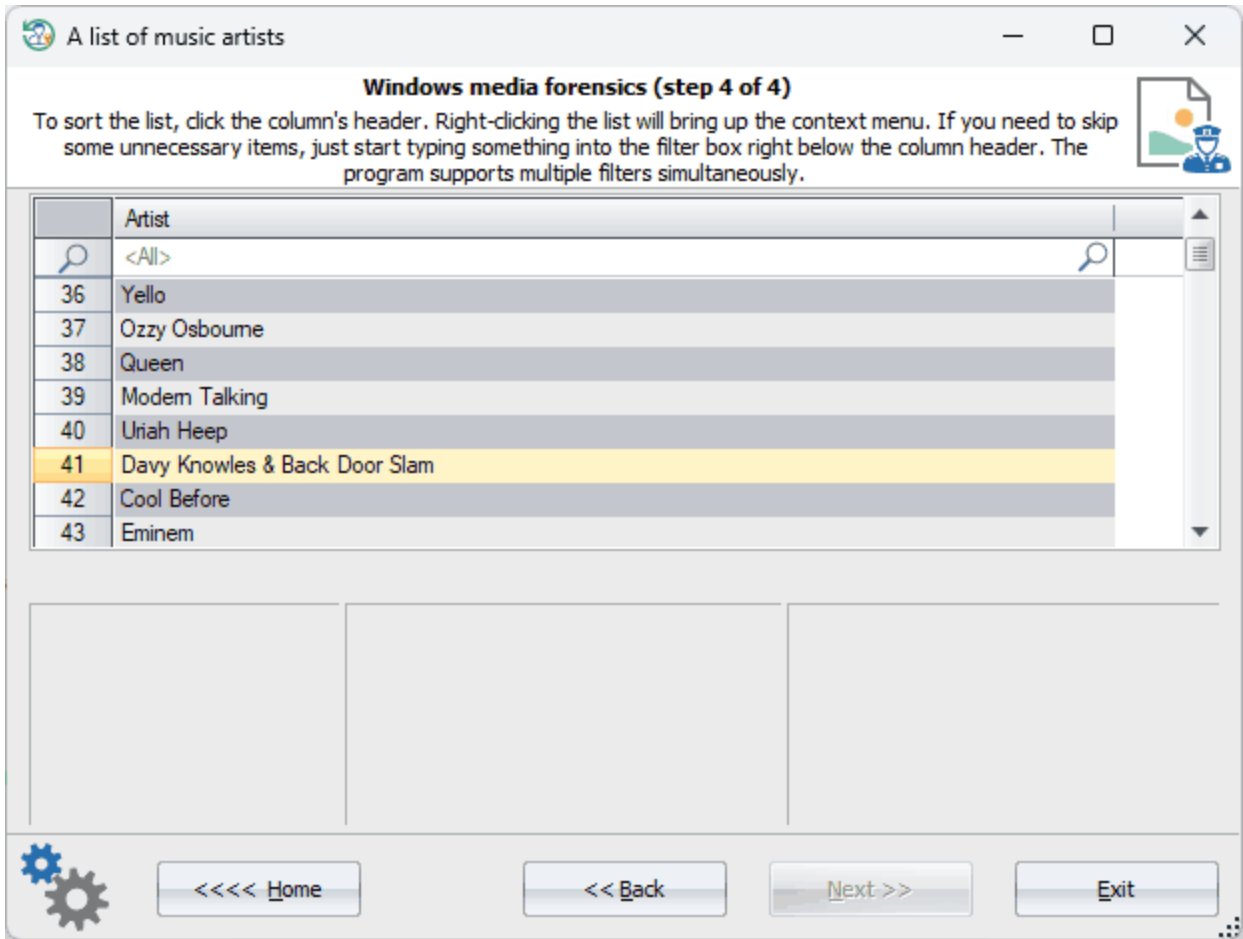
3.7.4.5.1



Photos.

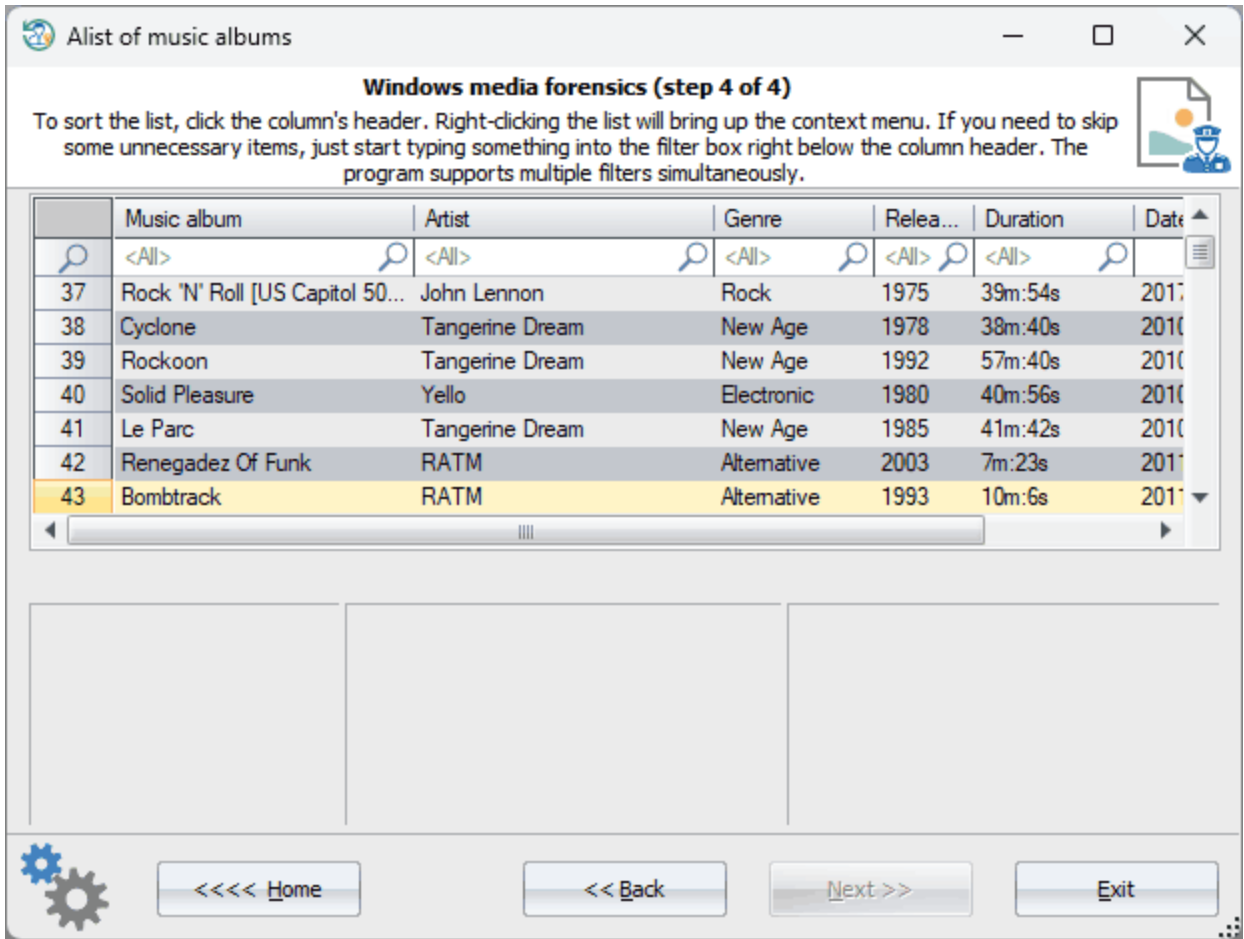
3.7.4.6

3.7.4.6.1



(Media Player, Windows Media Player !).

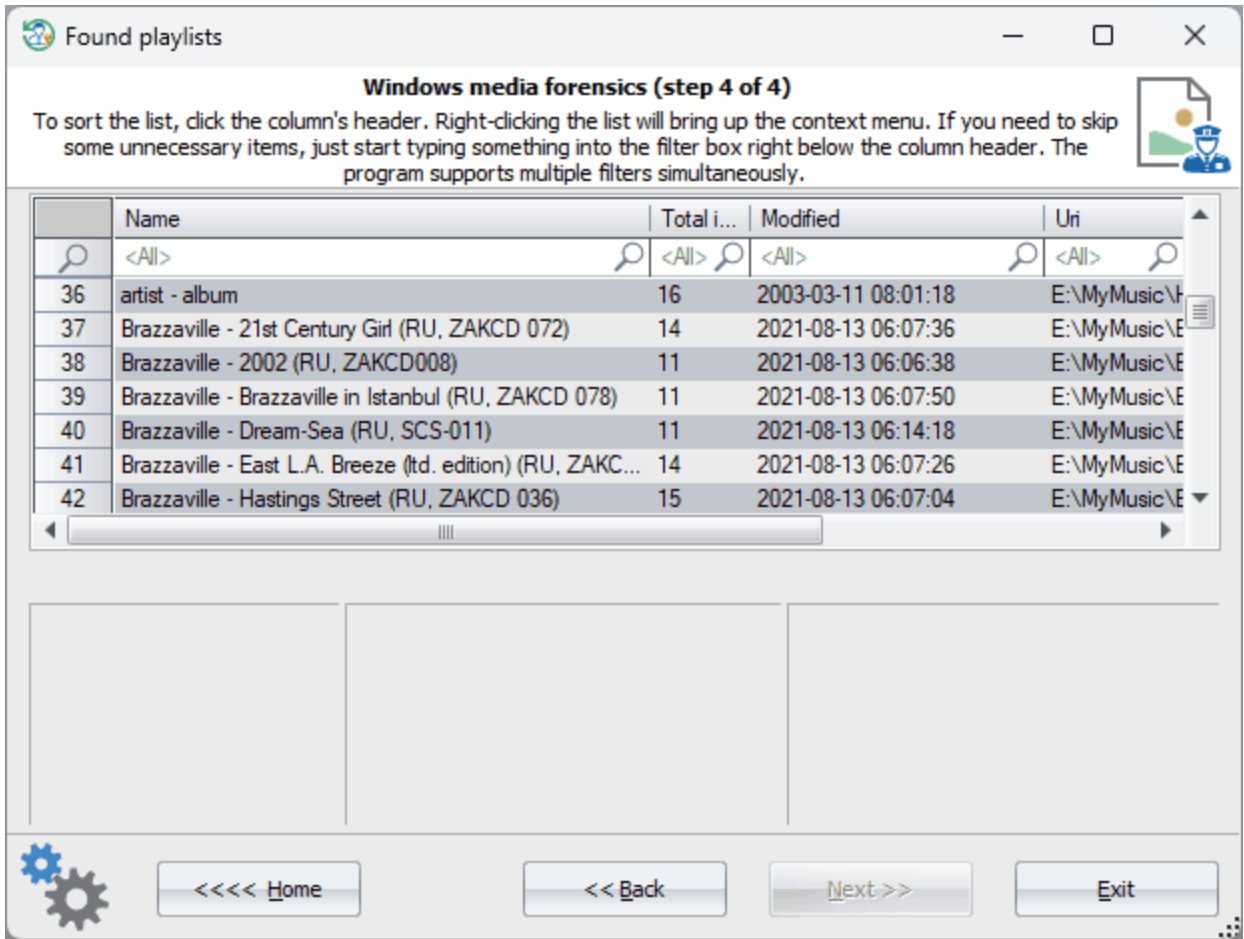
3.7.4.6.2



Media Player.

-
-
-
-
-
-

3.7.4.6.3



Media Player.

3.7.4.6.4

A list of 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.

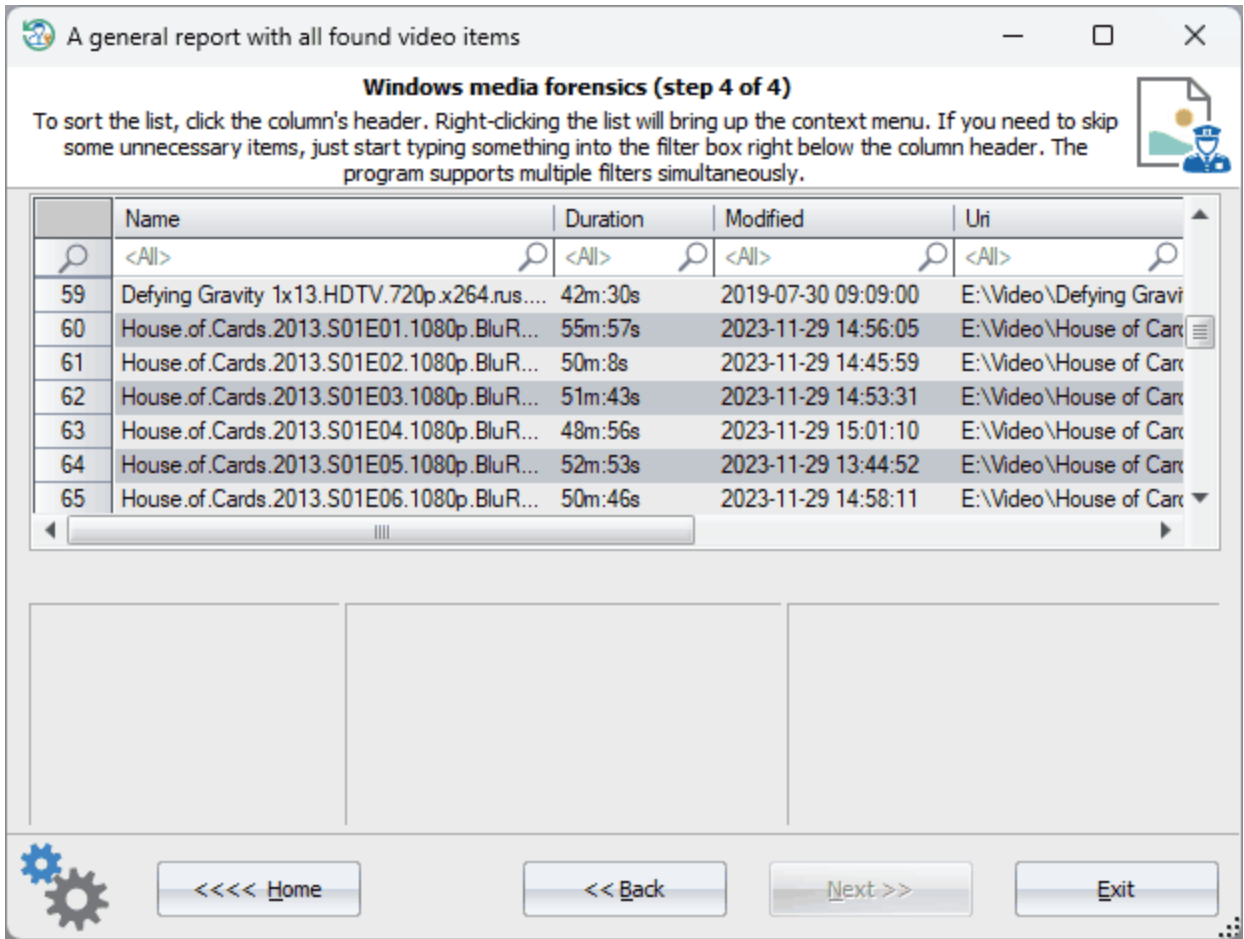
	Name	Music album	Track	Relea...	Duration	Date adde
	<All>	<All>	<All>	<All>	<All>	<All>
50	Knowing Me, Knowing You	Thank You for the Music Di...	1	1995	4m:2s	2008-03-11
51	People Need Love	Thank You for the Music Di...	1	1995	2m:46s	2008-03-11
52	The Winner Takes It All	Thank You for the Music Di...	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

Settings: <<<< Home, << Back, Next >>, Exit

-
-
-
-
-
-
-
-
-
-

:

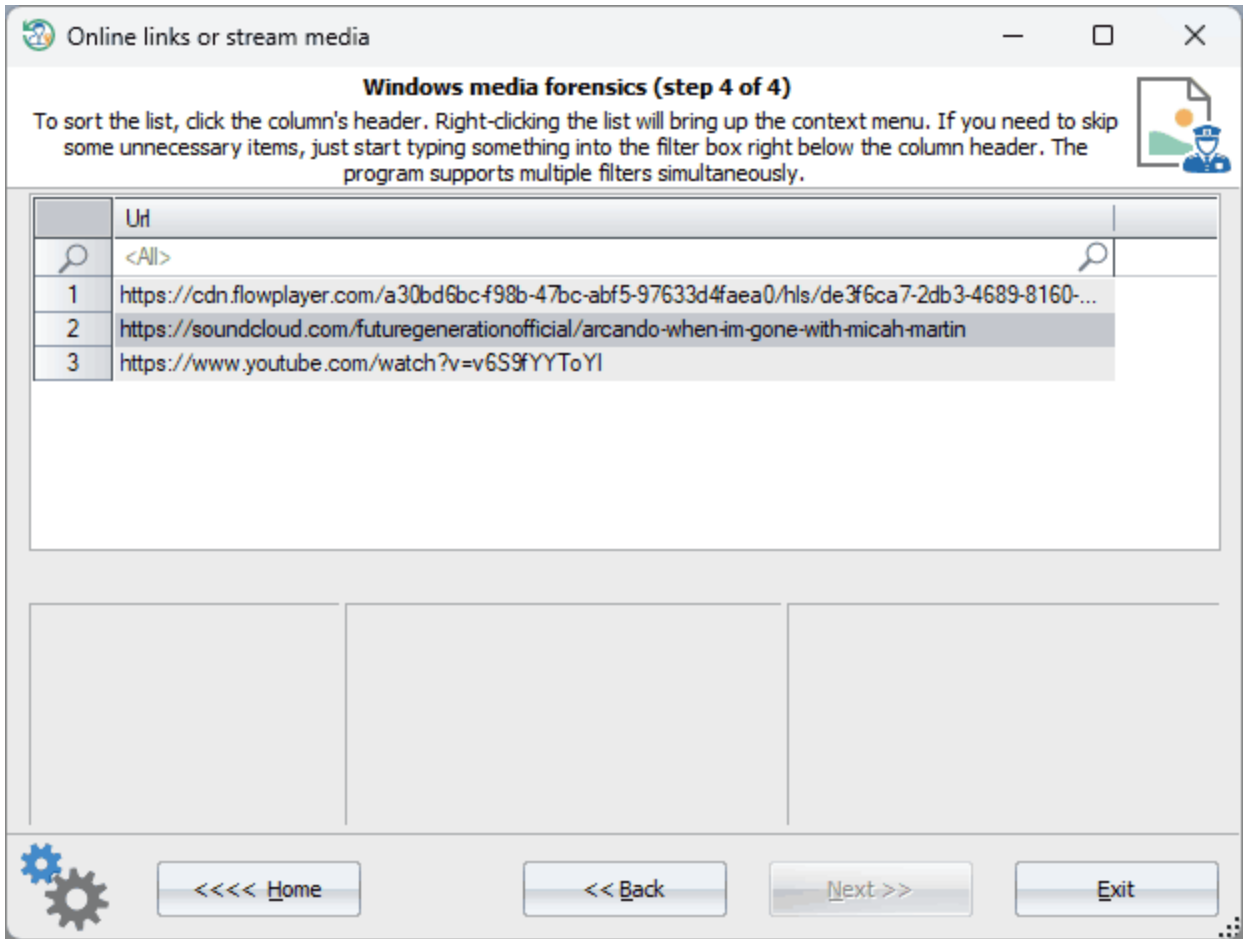
3.7.4.6.5



Media Player.

-
-
-
-

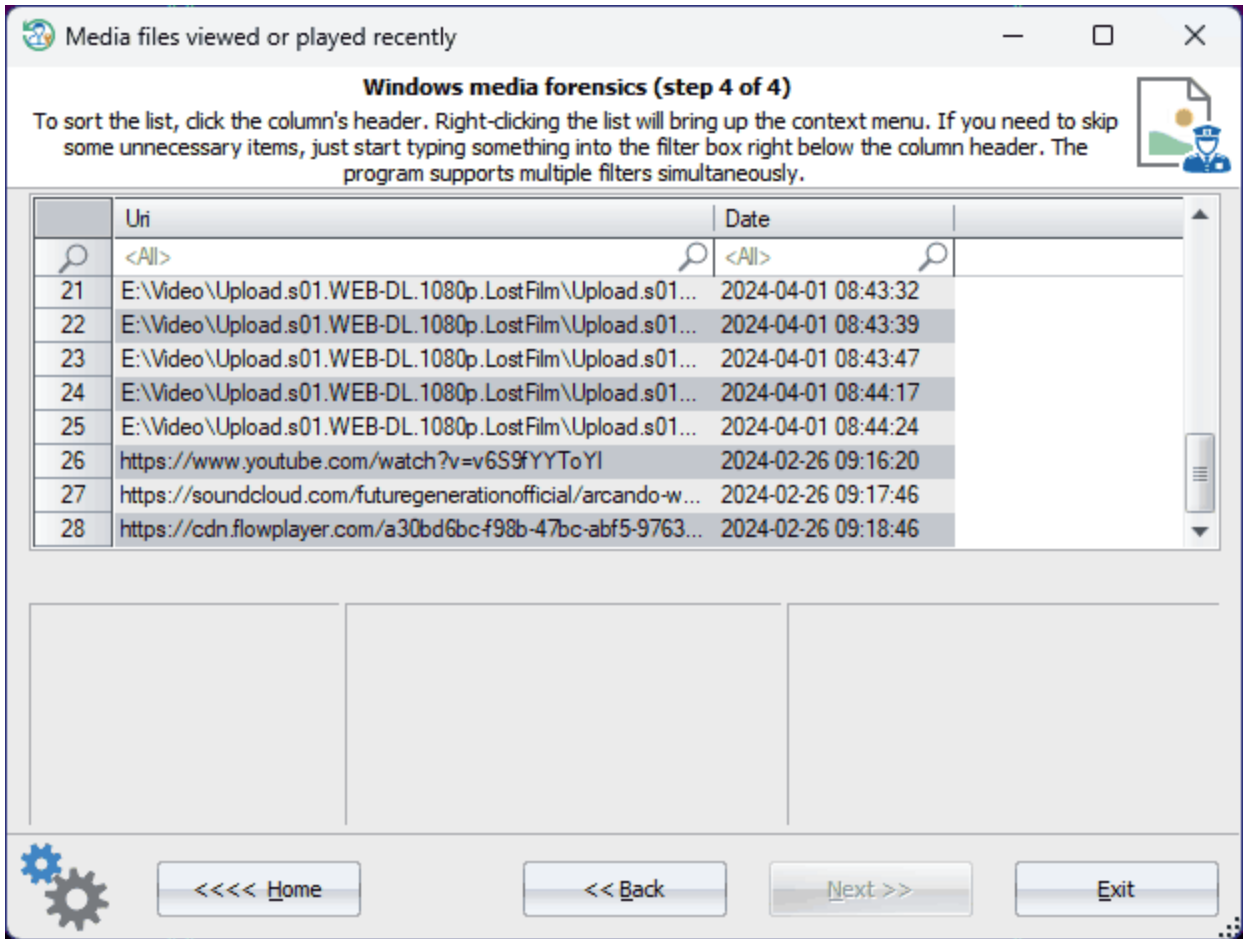
3.7.4.6.6



Media Player.

3.7.4.7

3.7.4.7.1



Media Player.

3.7.5 Windows

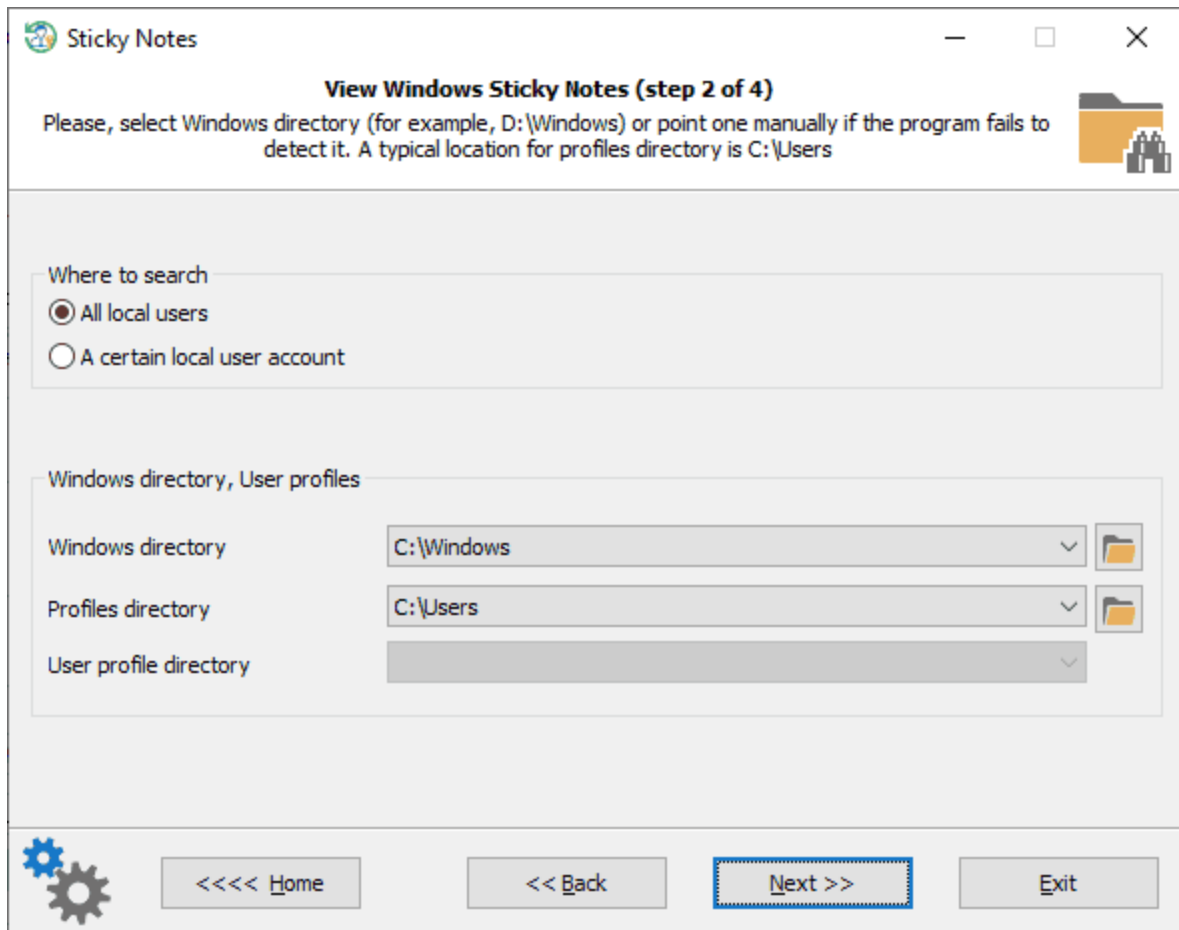
(Sticky Notes) -
Windows, Windows 7.

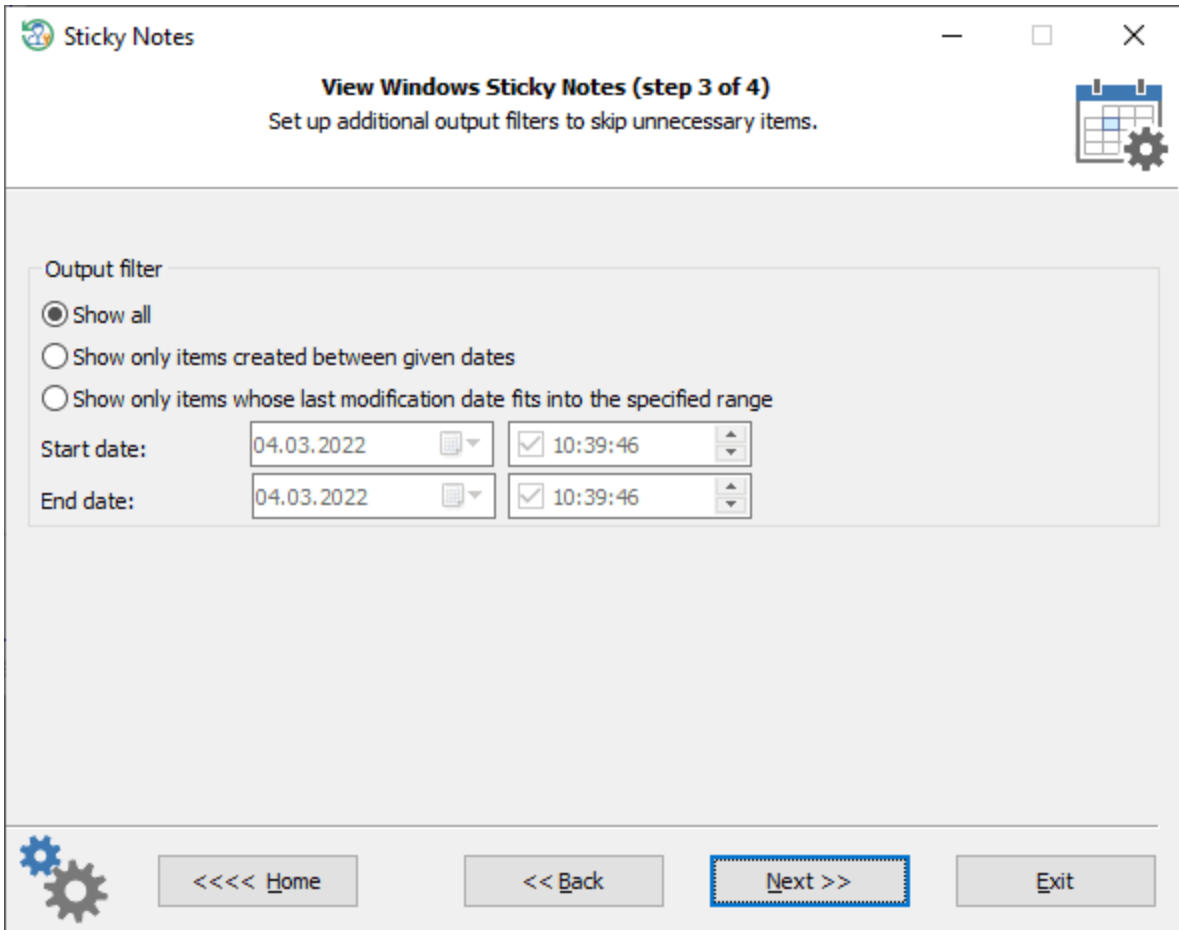
Microsoft

Reset Windows Password
Windows,
Windows

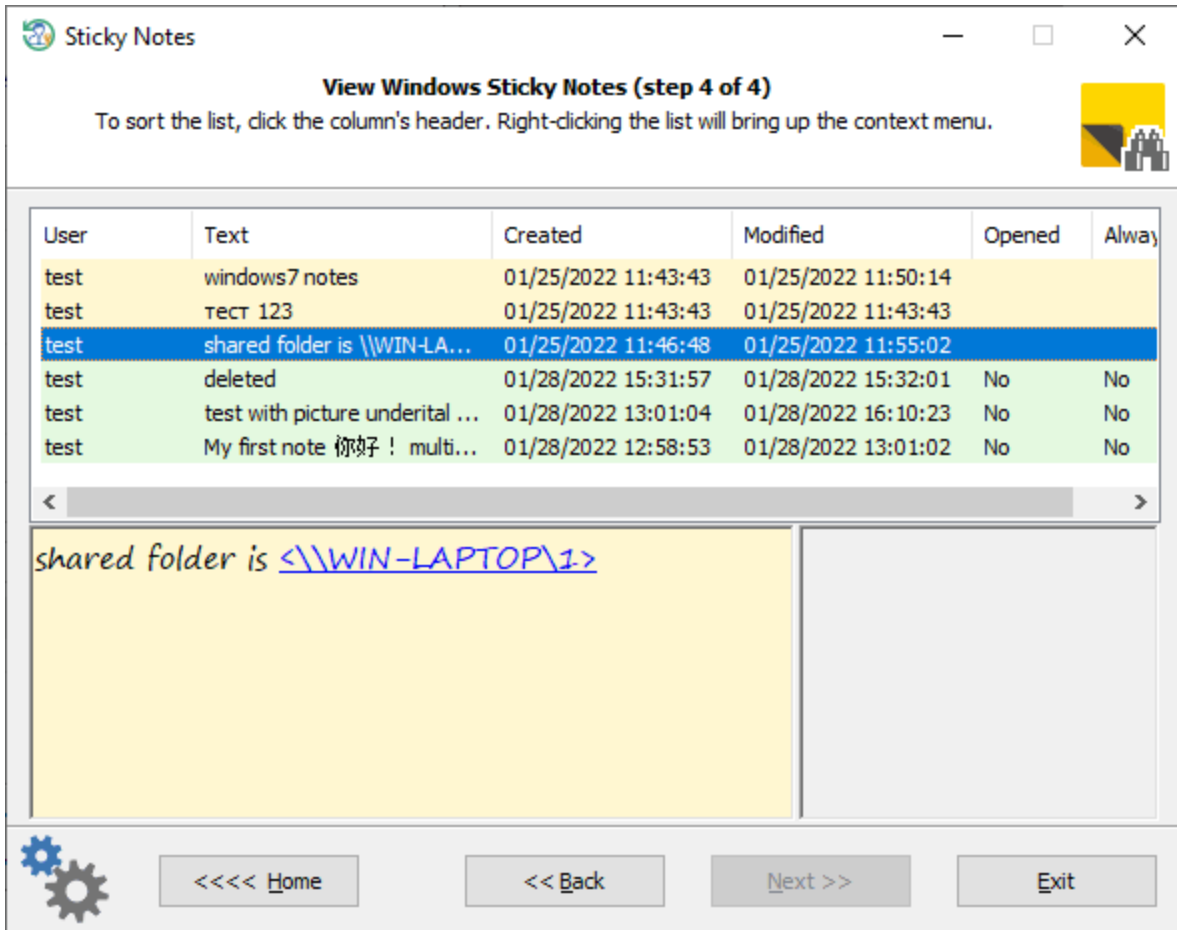
()
()

).





Windows



Windows 10

3.7.6

Reset Windows Password

(Windows),

Windows

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\microphone`

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\webcam`

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	▼	

⚙️ <<<< Home << Back **Next >>** Exit

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

<<<< Home << Back **Next >>** Exit

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

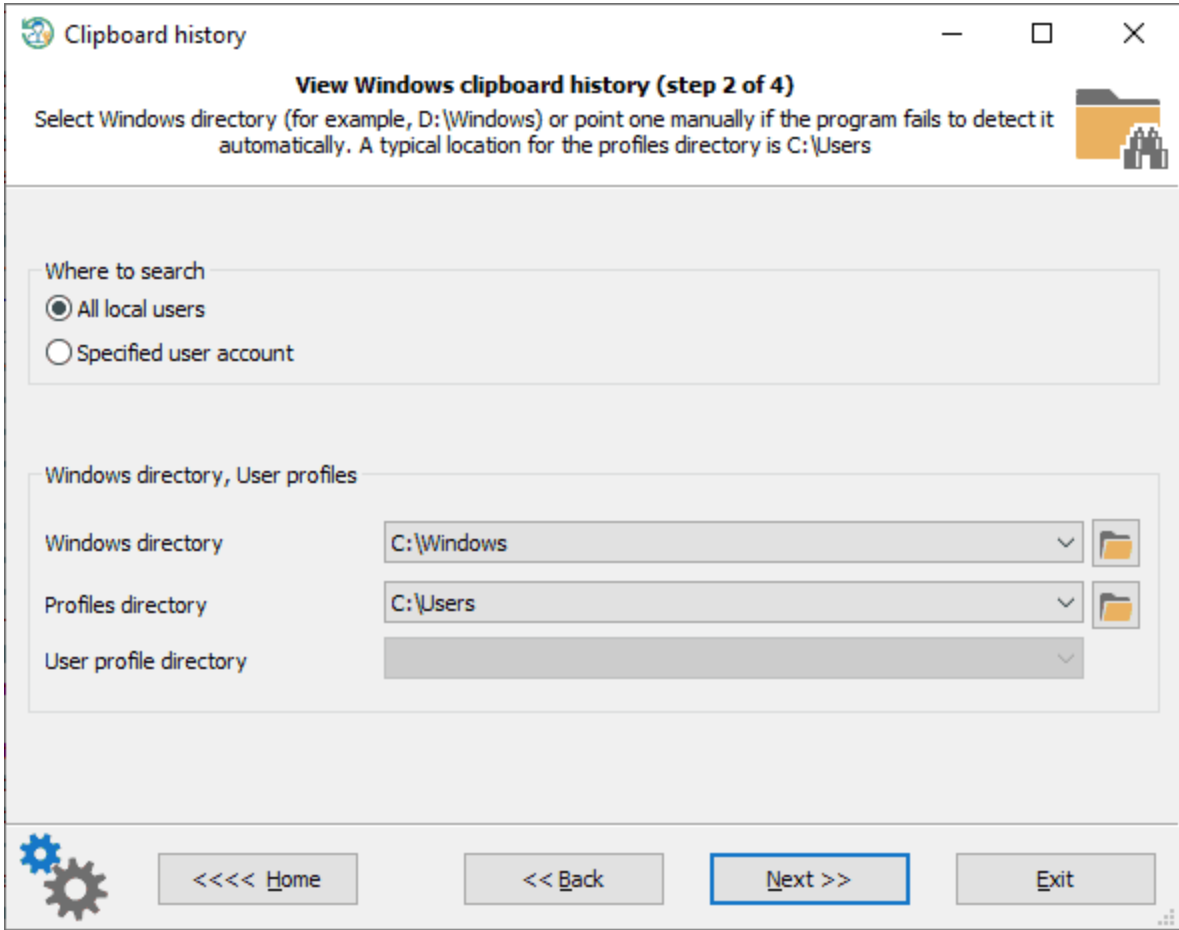
Navigation: <<<< Home << Back Next >> Exit

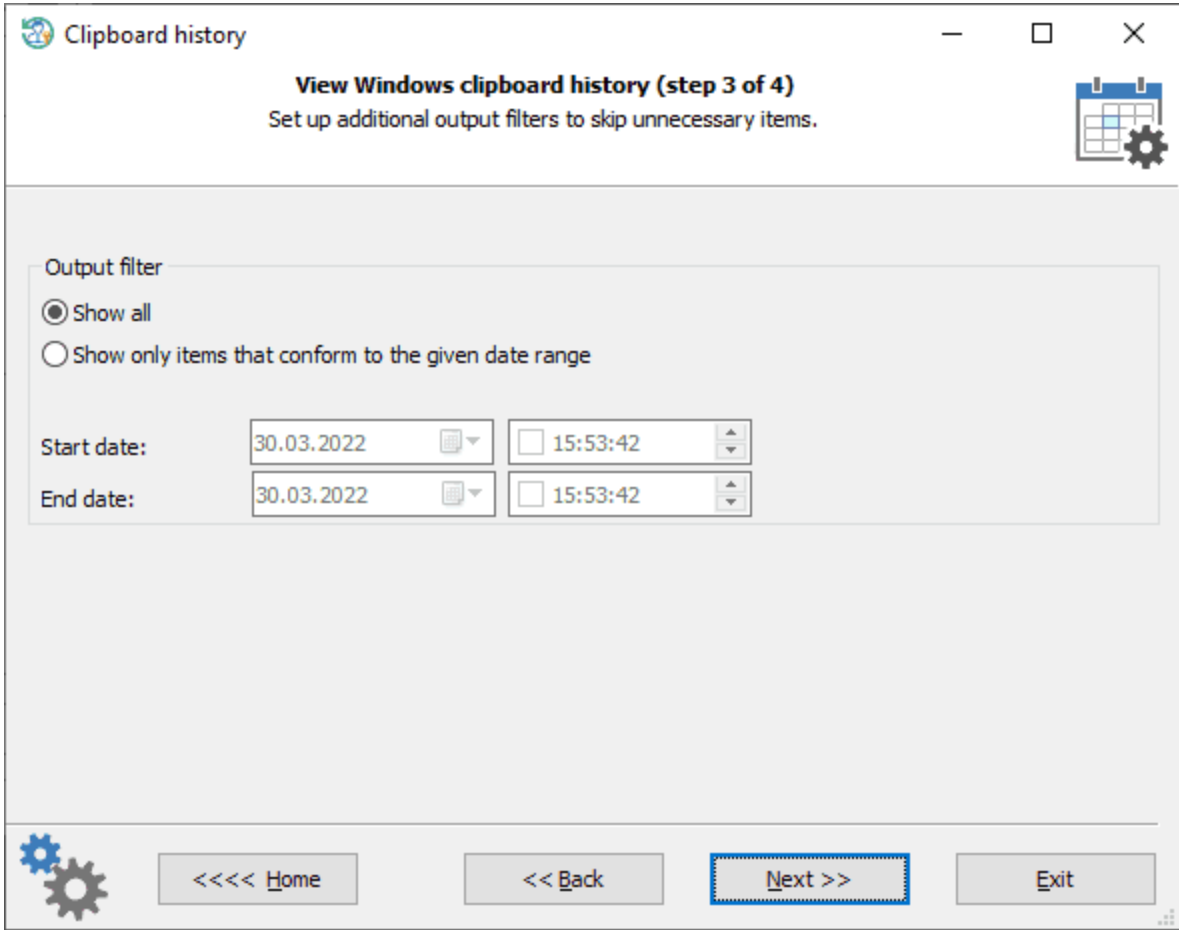
Bluetooth.

3.7.7

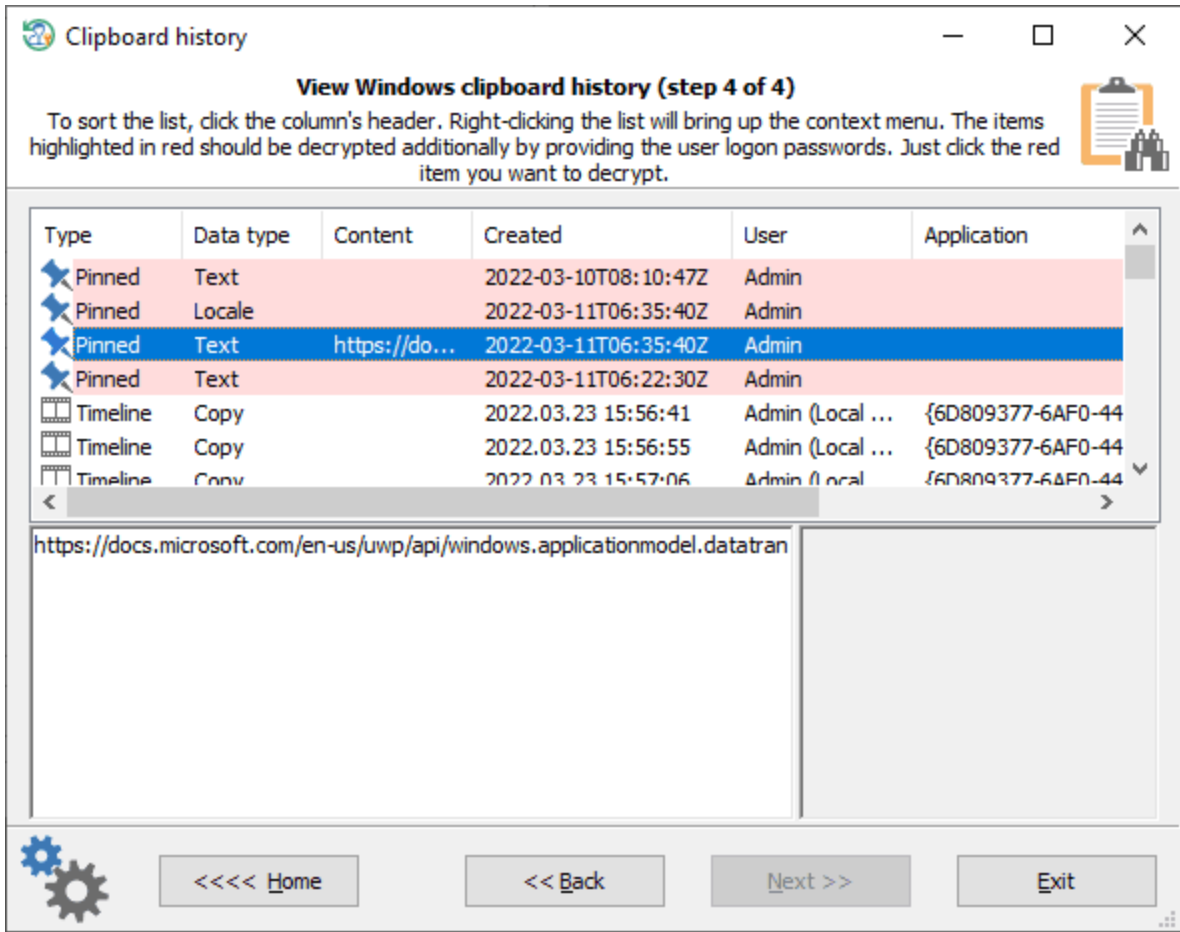
Windows.

Windows





Windows



1. Windows.
2. () Windows
3. Copy/Paste (

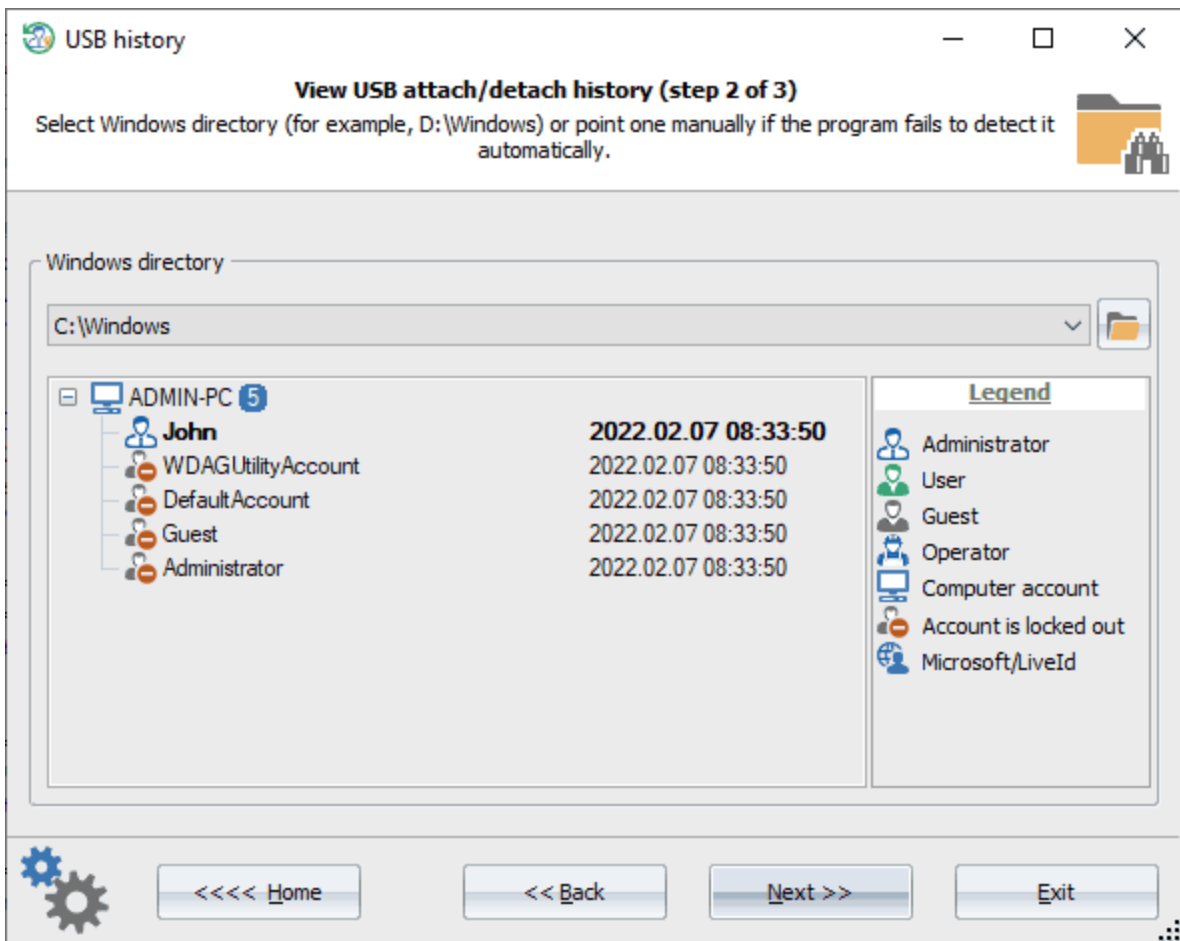
3.7.8

USB

Windows

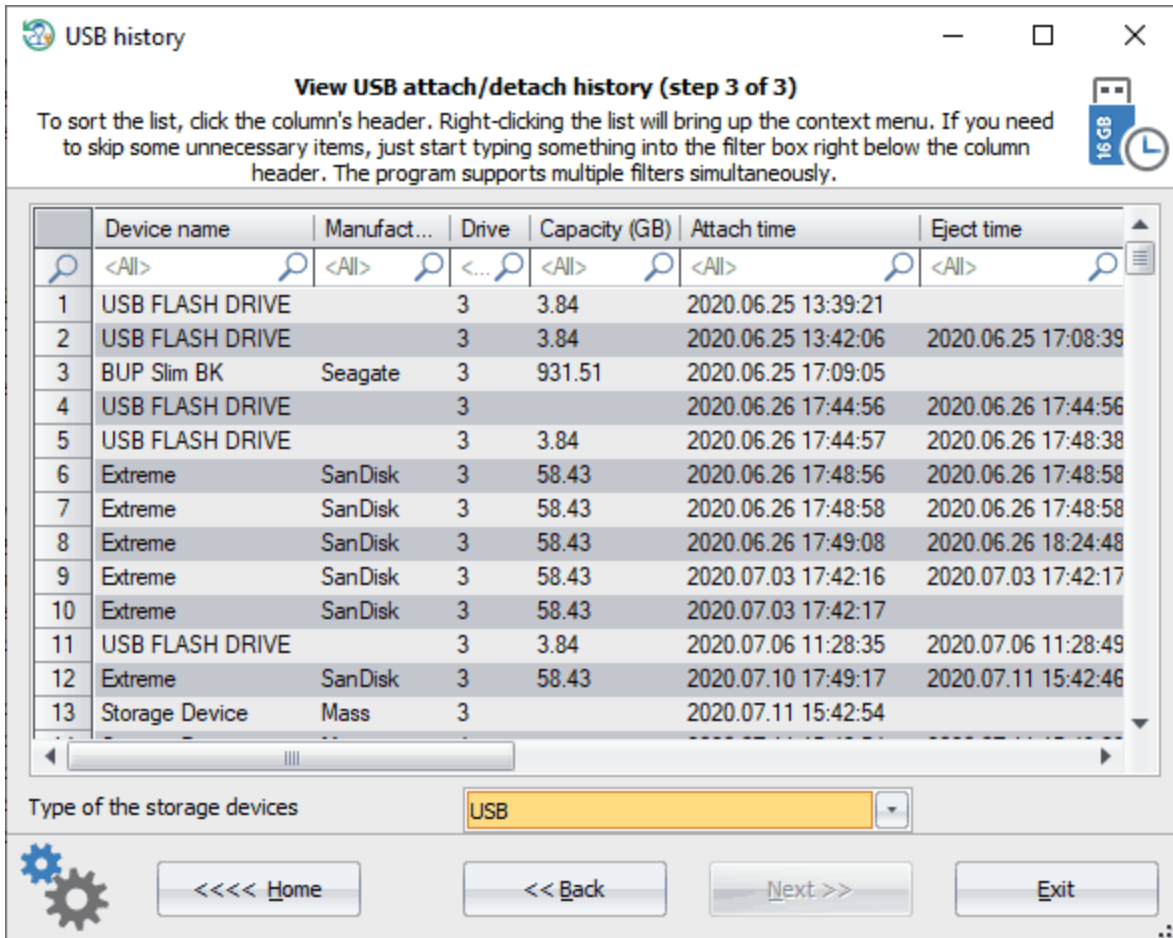
USB

USB



Windows

USB



USB, : 1394, ATA, ATAPI, FIBRE, Virtual File Backup Storages, ISCSI, MMC, RAID, SAS, SATA, SCSI, SD, SSA, Storage Spaces, Virtual Storages.

3.7.9

(SRUM)

. SRUM (, ,)

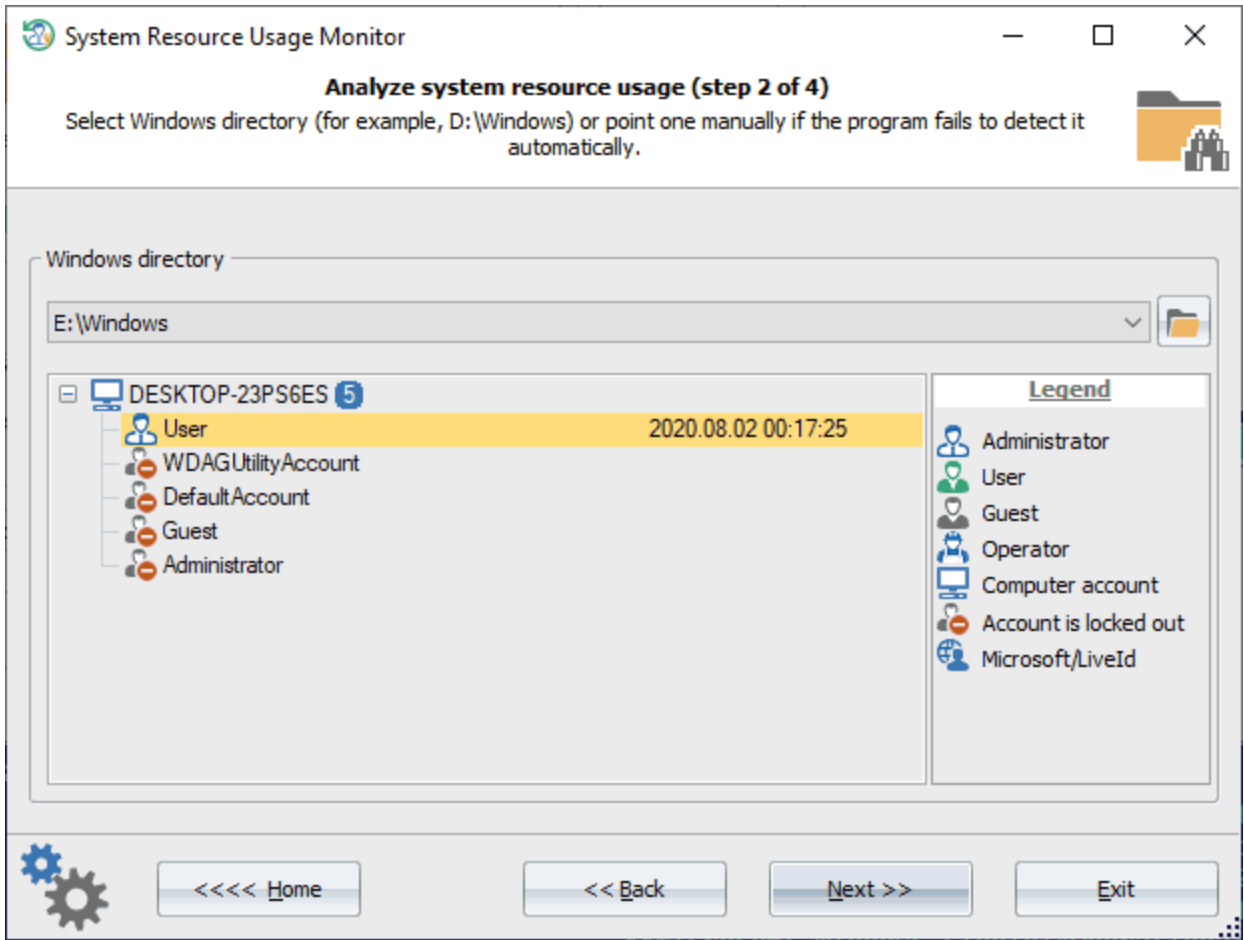
SRUM

SRUMDB.DAT,

Extensible Storage Engine.

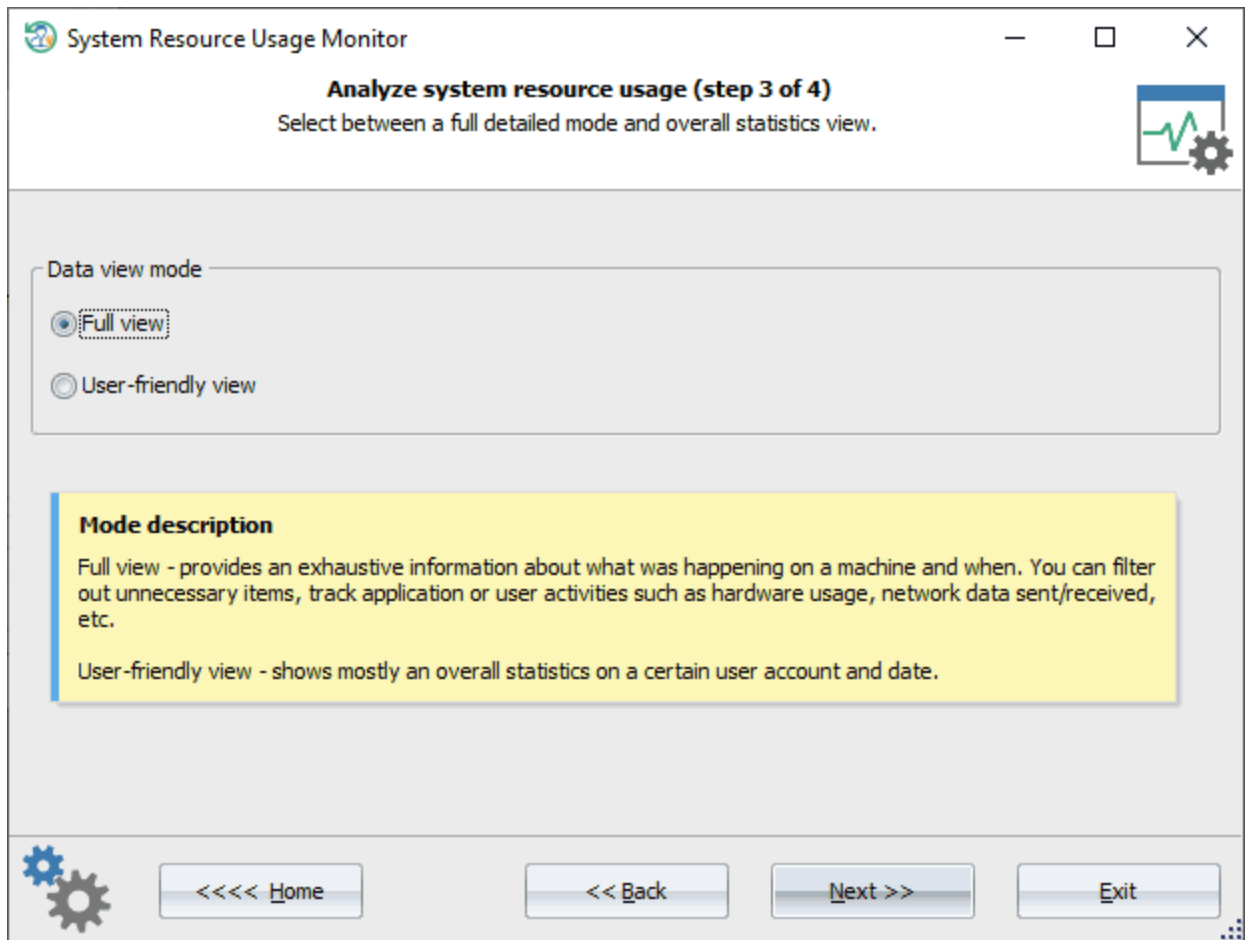
Windows 8.

%WINDIR%\System32\sru



SRUM

Windows.



SRUM -

': 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.

size. 'Push- Windows': notification type, network type, payload

interface, interface type, profile ID, profile flags. ': connection started, connection time, network

type, profile ID, profile flags. ': bytes sent, bytes received, network interface, interface

SRUM -

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 time
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

Navigation: <<<< Home, << Back, Next >>, Exit

3.7.10

Windows Search

Windows Search -

. Windows Search

Windows Search

Extensible Storage Engine

%SYSTEMDRIVE%\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

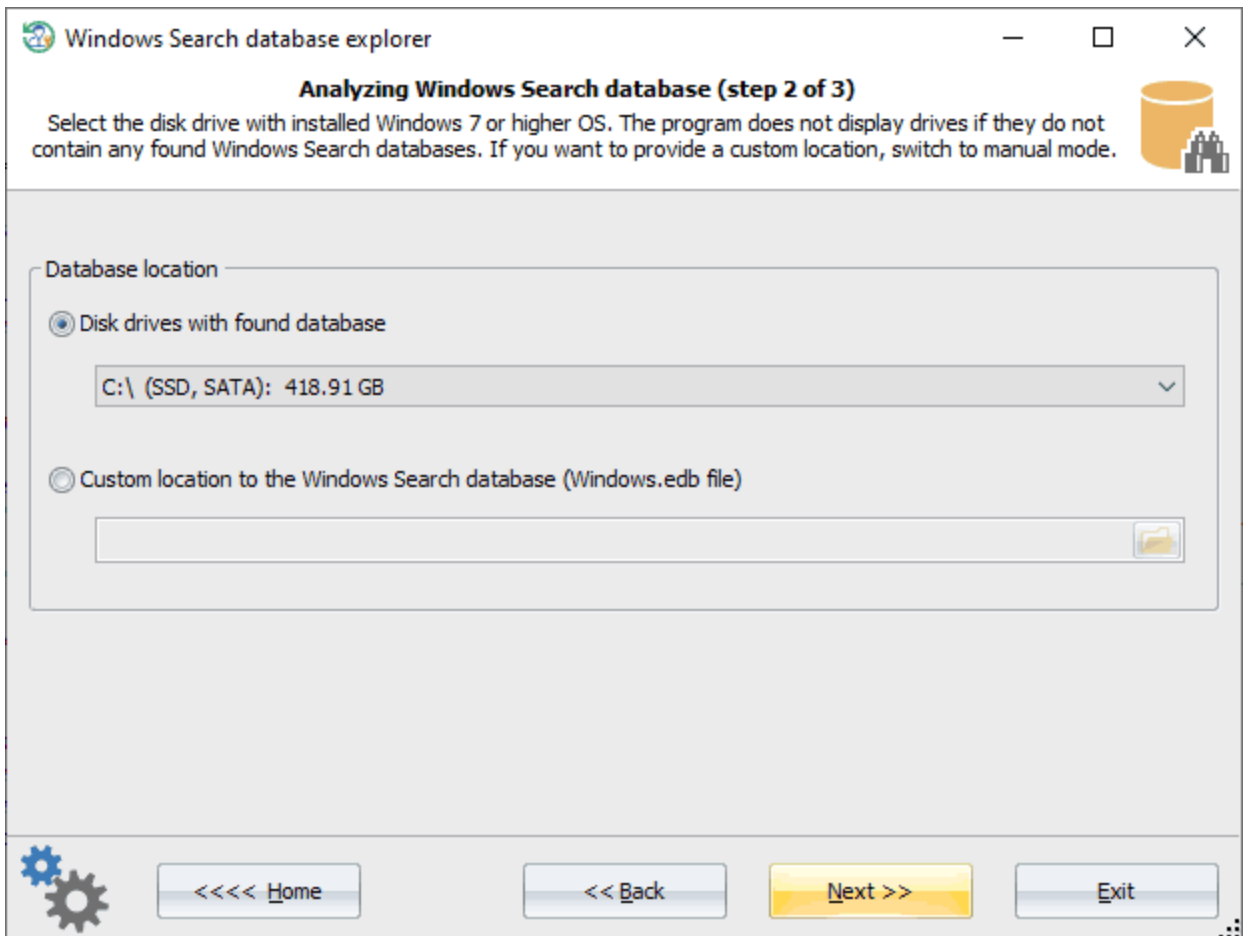
Windows 11

SQLite

Windows.db

Windows 10

Windows Search -



(, , , ,) ,

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.

The interface is divided into three main sections:

- Directory tree:** Shows a hierarchical view of the search database. The selected path is:
 - Windows 10 Enterprise LTSC 2019 177
 - file:
 - iehistory:
 - csc:
 - mapi15:
 - {S-1-5-21-2425377081-3129-...}
 - iaman.infomant@nist.gov
 - 0/
 - Inbox/
- File list:** Displays the contents of the selected folder. The selected file is "Watch out!". Other files include "It's me", "Good job, buddy.", "Last request", and "Hello, laman".
- Property name / Property value table:**

Property name	Property value
MIMETYPE	MAPI/IPM.Note....
IsDeleted	False
Search_Access...	0
ItemFolderPathD...	/iaman.infomant...
ItemPathDisplay	/iaman.infomant...
Search_LastInd...	0.000000
Communication_...	iaman.infomant...
ItemUrl	mapi15://{S-1-5-...
IsRead	True
Importance	3
ItemParticipants	spy
FlagStatus	0
Message_FromA...	16DEB821A6D2...
Message_FromN...	spy

At the bottom, there are navigation buttons: Home, Back, Next, and Exit.

3.7.11

Windows

Windows

Recycle bin history

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	Full path
2327	John	C:\	File	adler-soriya.ru.txt	2022.05.22 12:37:01	5236	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	sonyNessus88.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_part 1.zip	2022.05.20 16:27:10	5456336	C:\

Navigation buttons: <<<< Home, << Back, Next >>, Exit

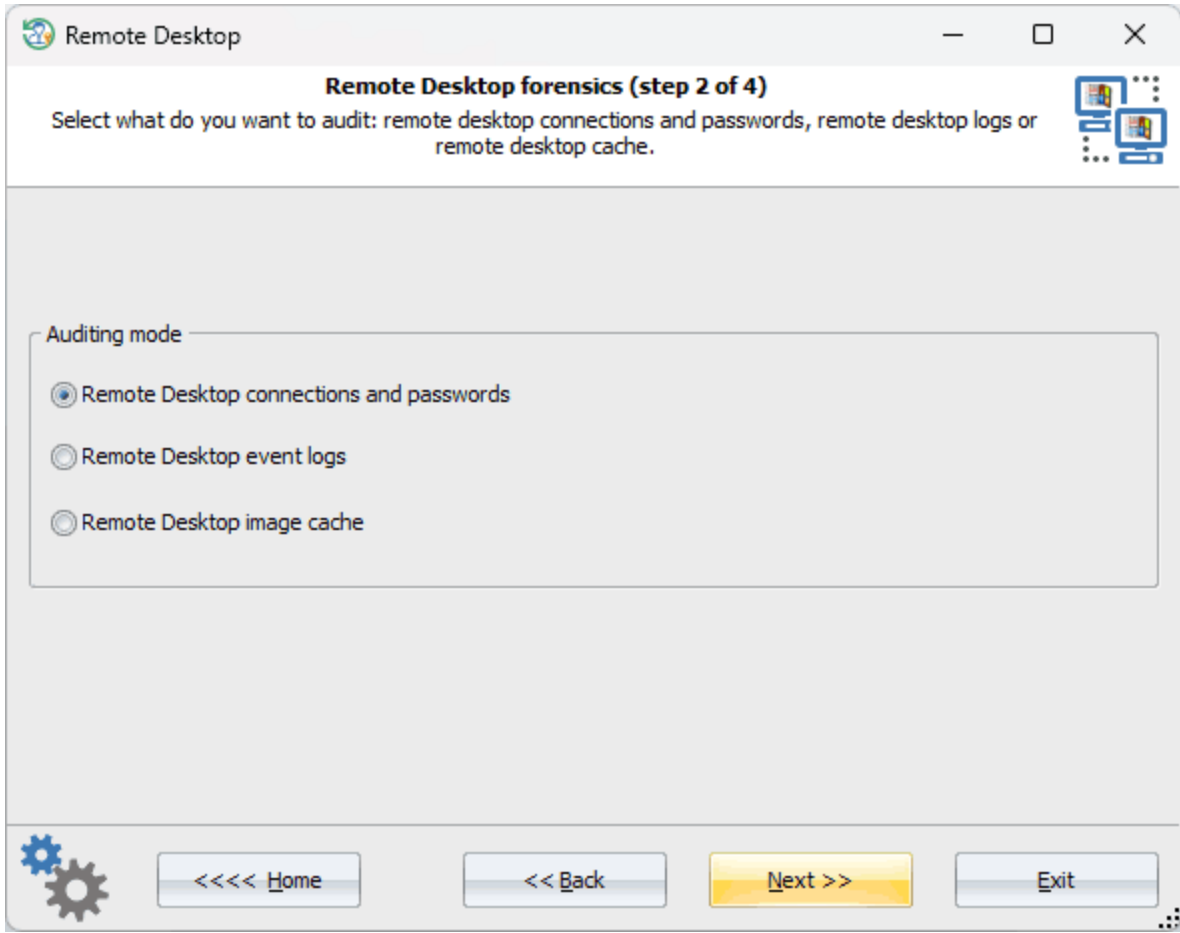
Windows

*.zip 'Ink' ()

3.7.12

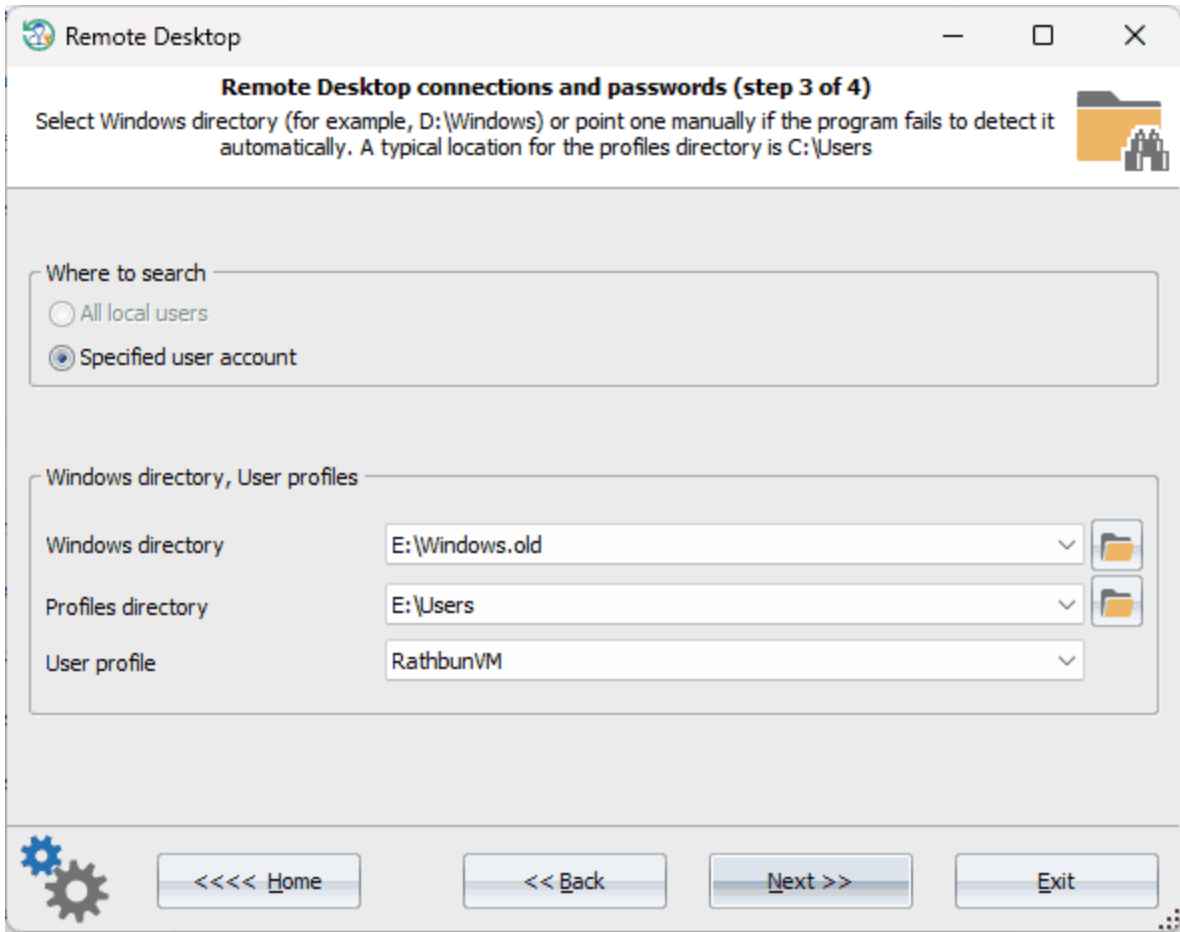
Windows.

Microsoft. (RDP) - Windows RDP

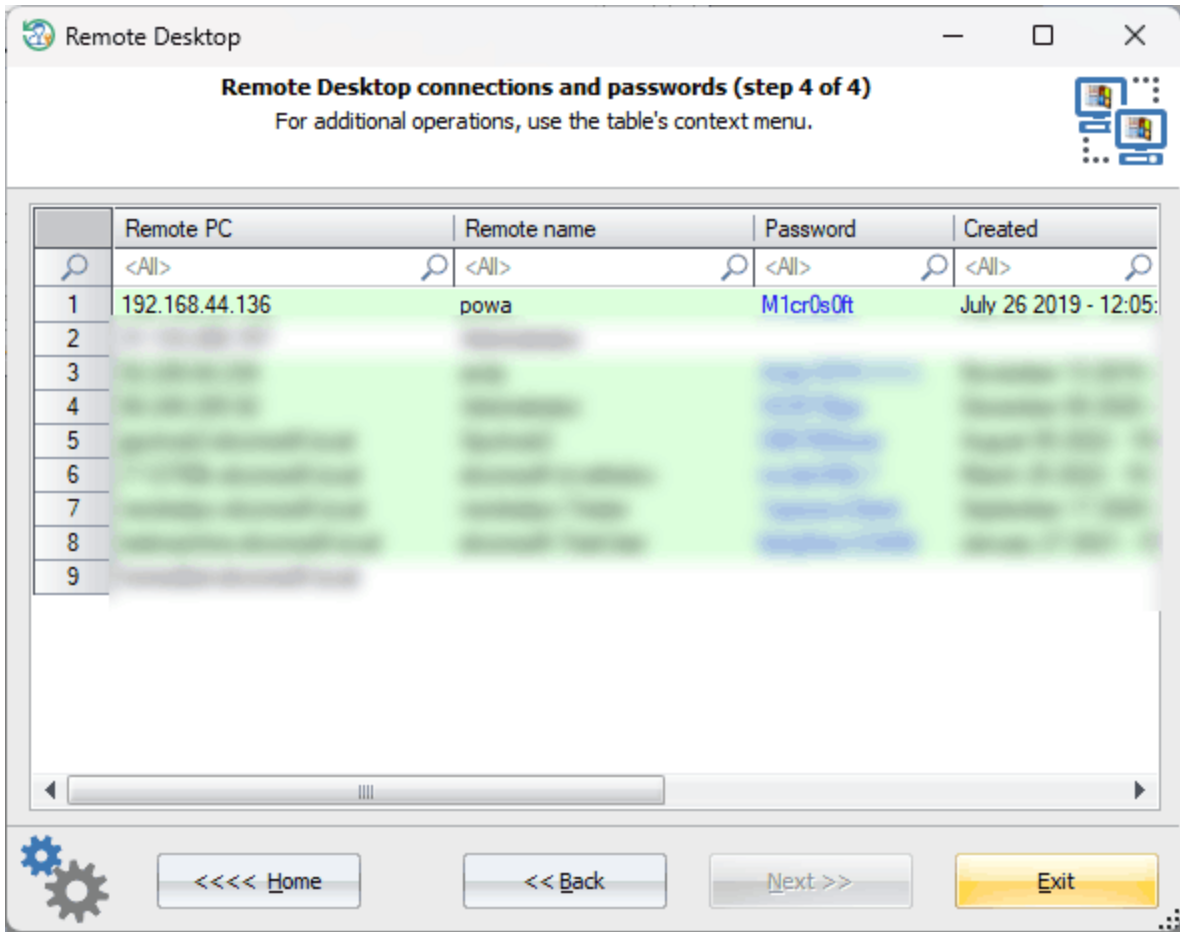


3.7.12.1

Windows,
Reset Windows Password RDP,
Windows,



Windows
RDP.



RDP,

Windows,

3.7.12.2

) Windows (

(Event Viewer).

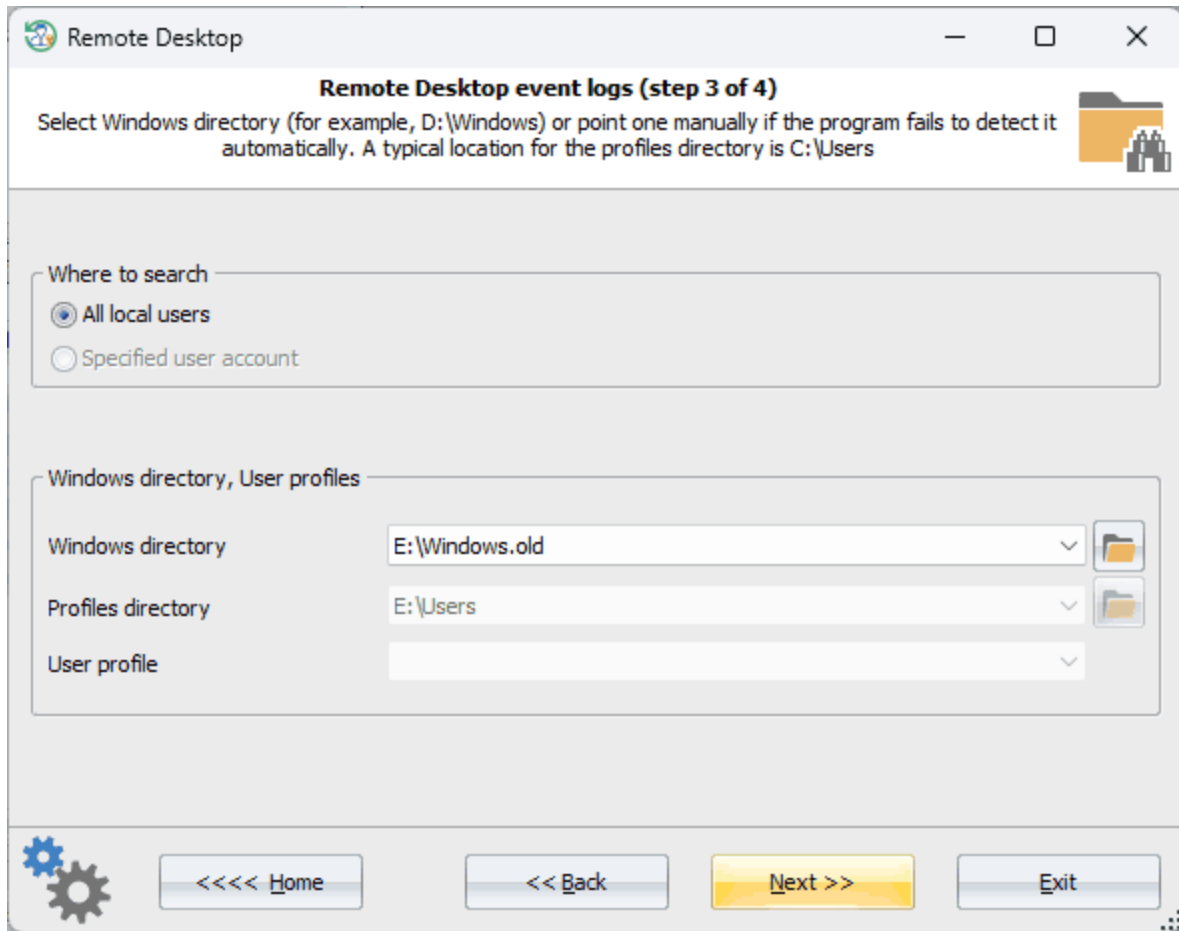
"Microsoft" "TerminalServices-ClientActiveXCore".

Windows,

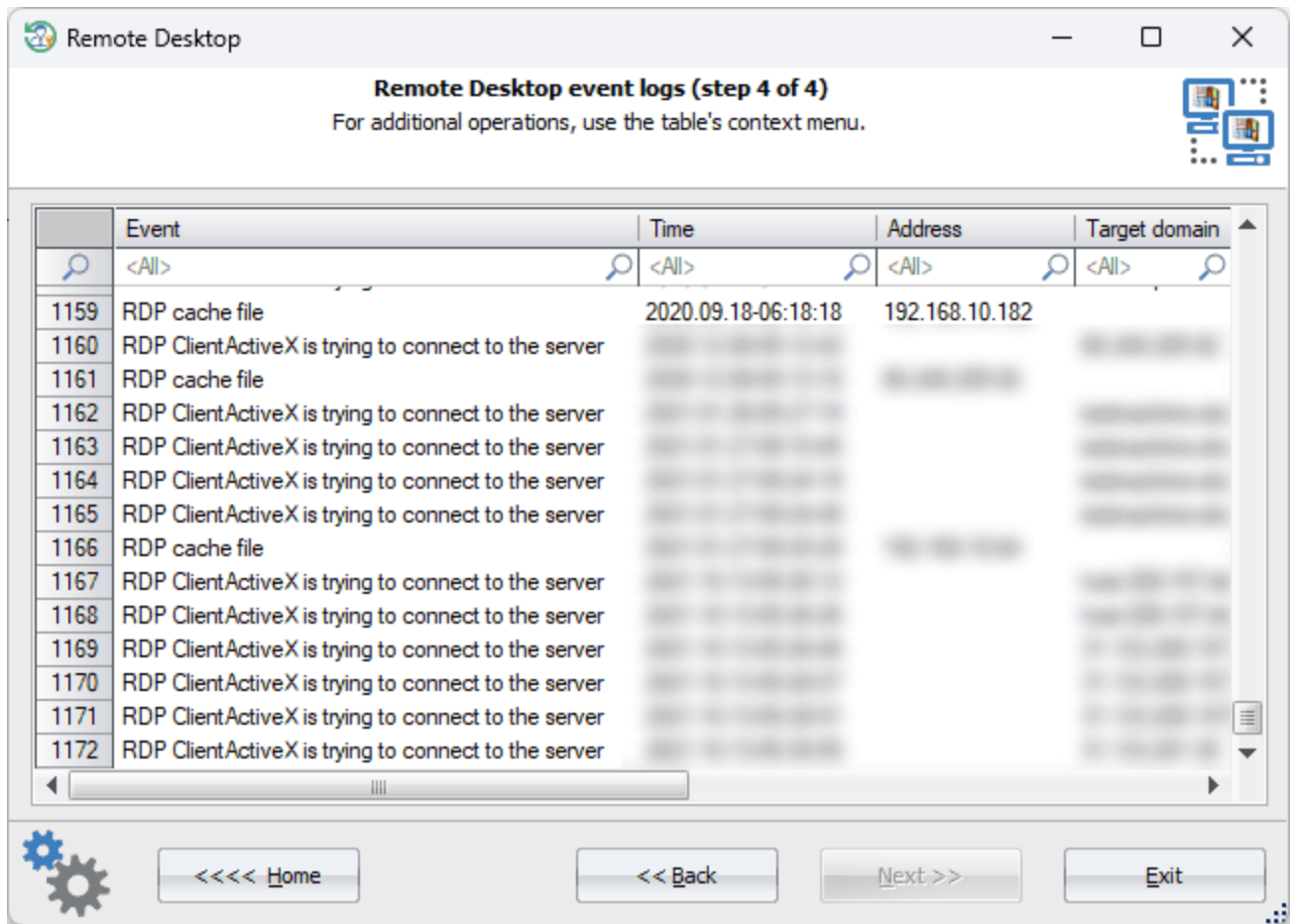
"TerminalServices-ClientActiveXCore".

RDP
 RemoteConnectionManager", "RemoteDesktopServices-RdpCoreTS", "TerminalServices-LocalSessionManager",
 "System" "Security".

Windows



Windows.



HTML. RDP

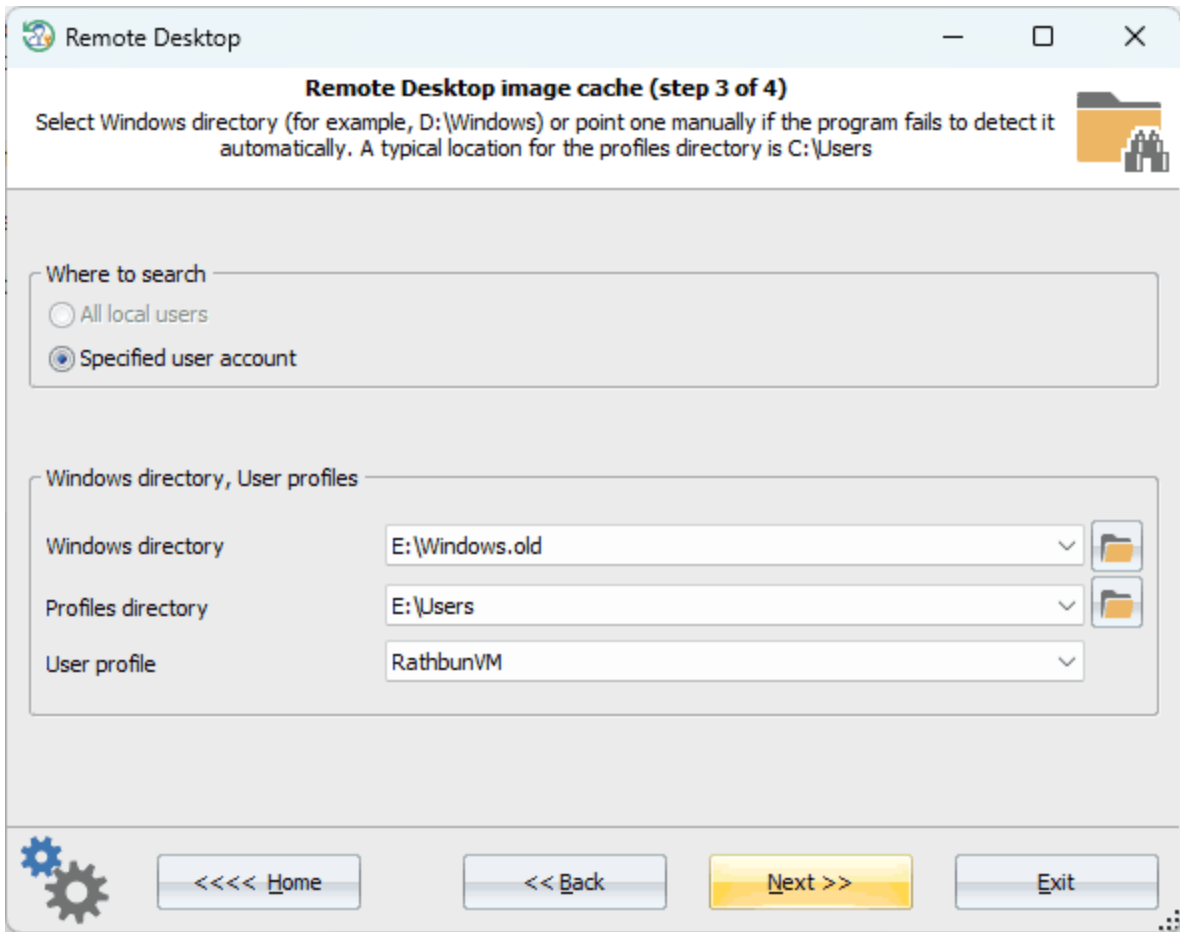
3.7.12.3

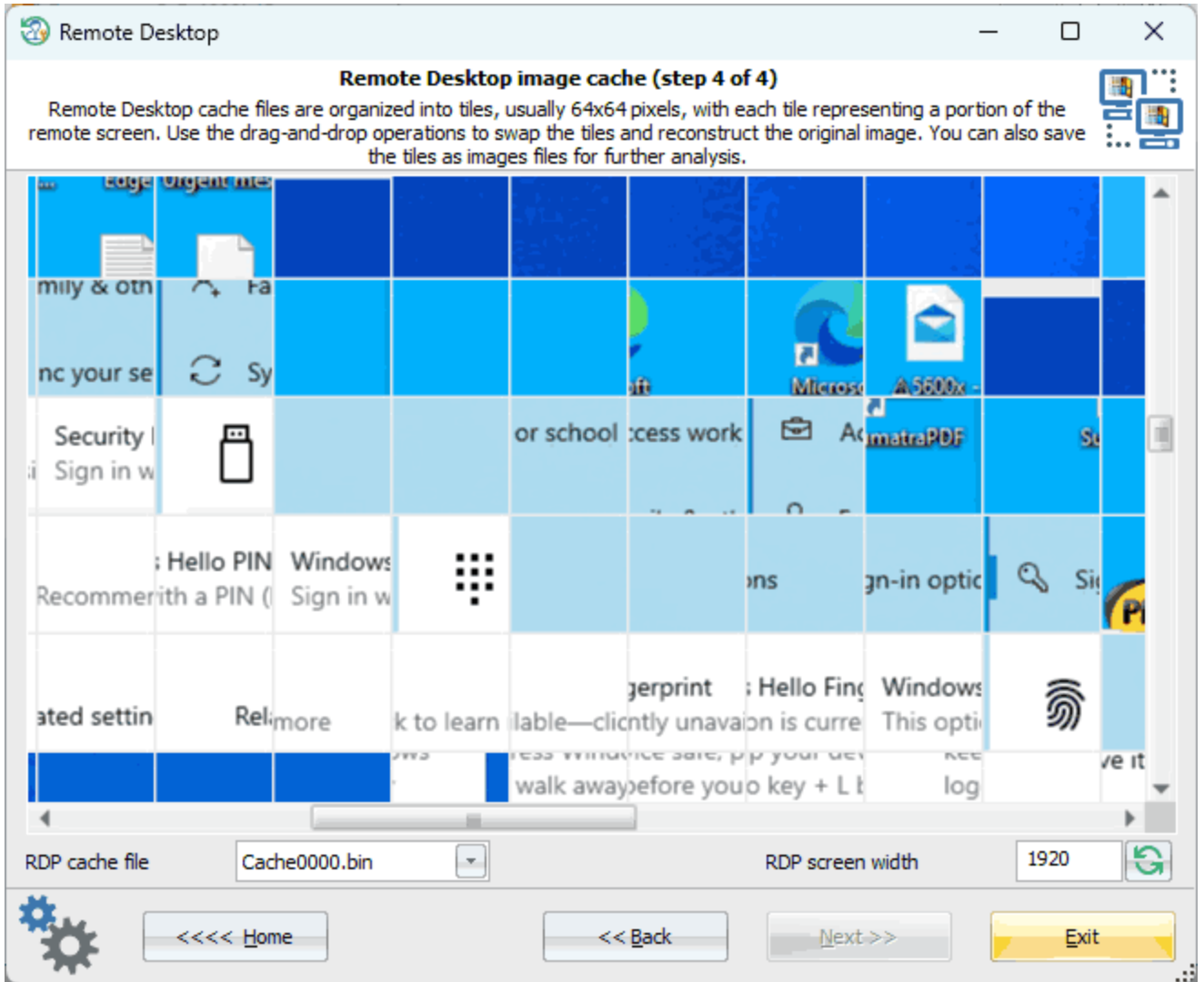
Windows,

RDP

RDP

\Users\\AppData\Local\Microsoft\Terminal Server Client\Cache".
".bin" Microsoft.
".bmc" ".bin" "c:
".bmc"
(), 64 64 ,
".bin"
Reset Windows Password





RDP.

3.7.13

Windows

Windows

*.evtx

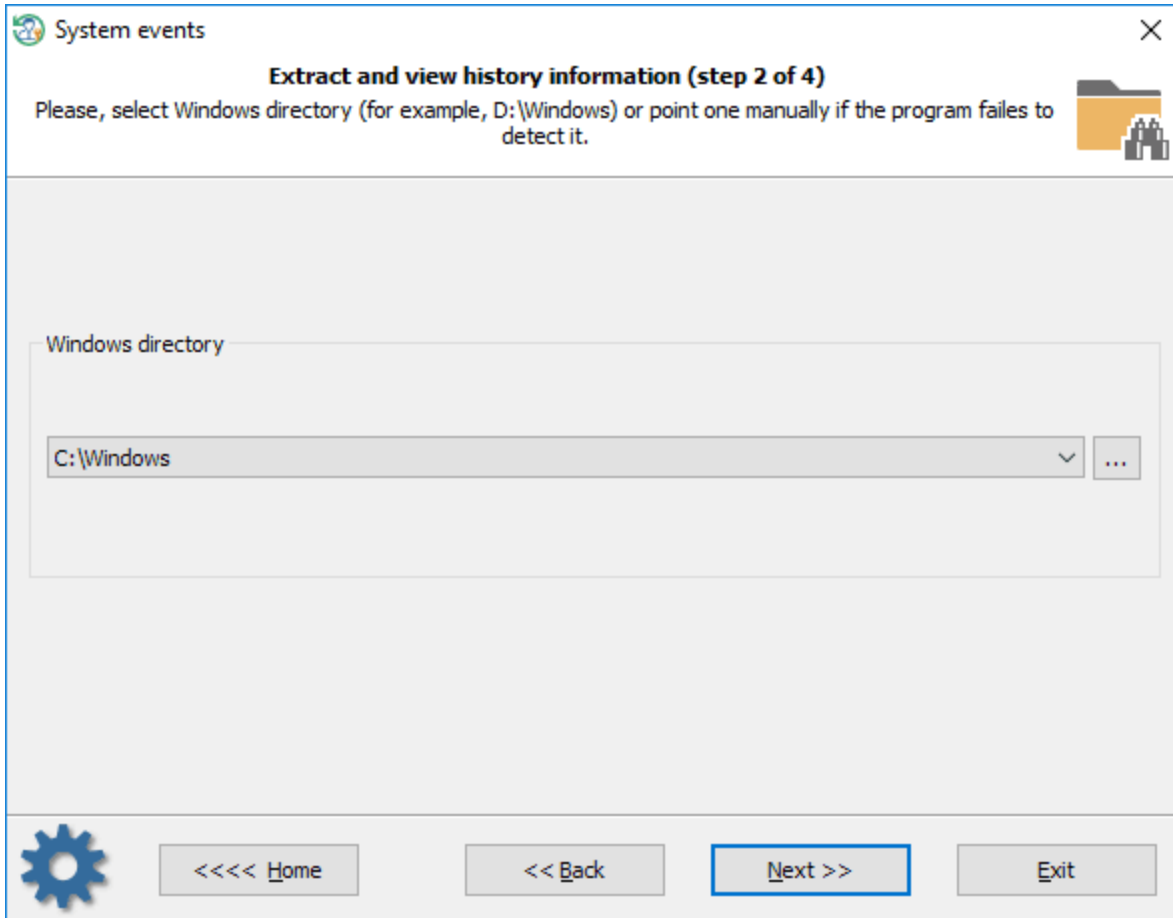
evtx

system.evtx

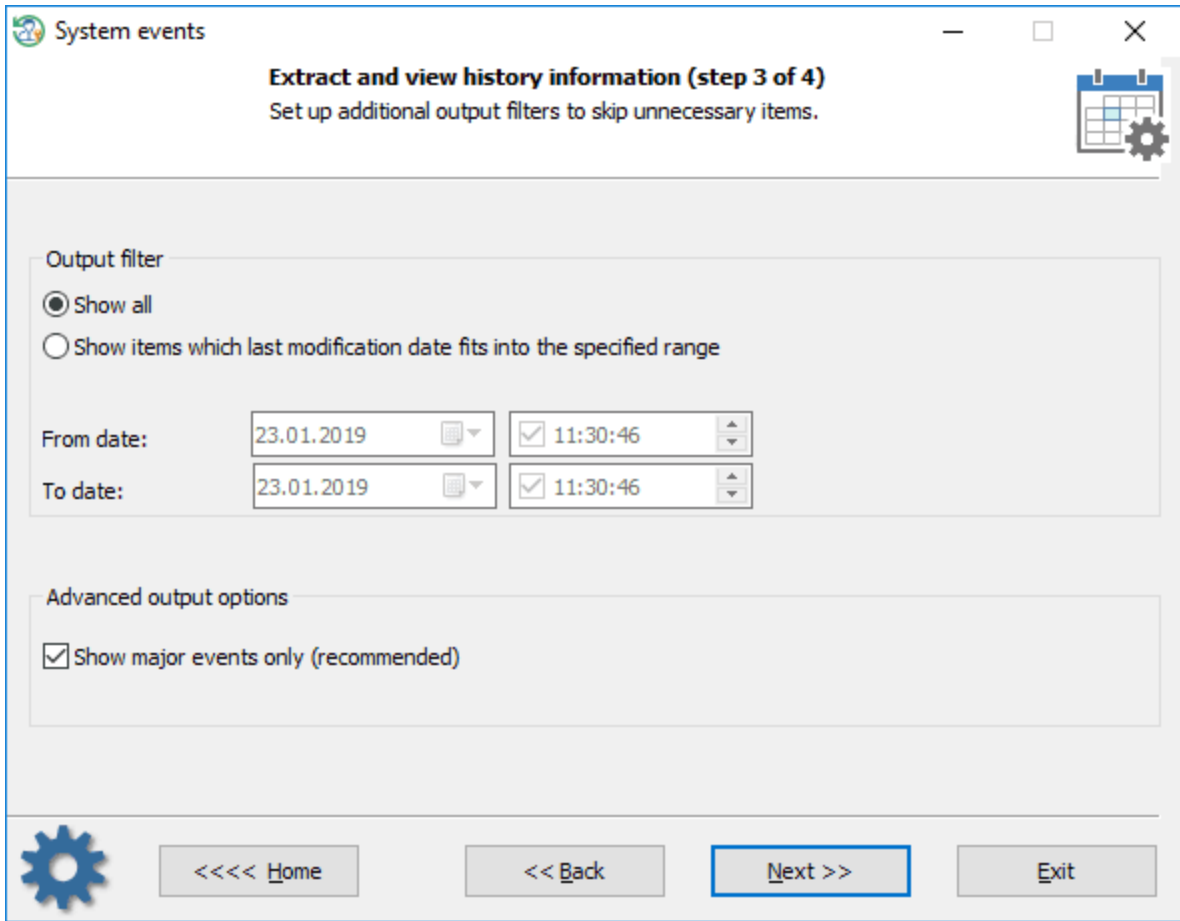
security.evtx

Windows Vista

Windows



Windows,



Windows

System 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	Source
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	ADM:
An account was successfully logged on	John	11.10.2018 14:47:46	ADM:
An account was successfully logged on	John	11.10.2018 14:47:46	ADM:
An account was logged off	John	11.10.2018 14:47:46	ADM:
User initiated logoff	John	11.10.2018 18:30:14	ADM:
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	ADM:
An account was successfully logged on	John	12.10.2018 18:25:18	ADM:
An account was logged off	John	12.10.2018 18:26:05	ADM:
An account was successfully logged on	John	12.10.2018 18:26:05	ADM:
An account was successfully logged on	John	12.10.2018 18:26:05	ADM:
An account was logged off	John	12.10.2018 18:26:05	ADM:

Navigation: <<<< Home << Back Next >> Exit

3.7.14

Telegram

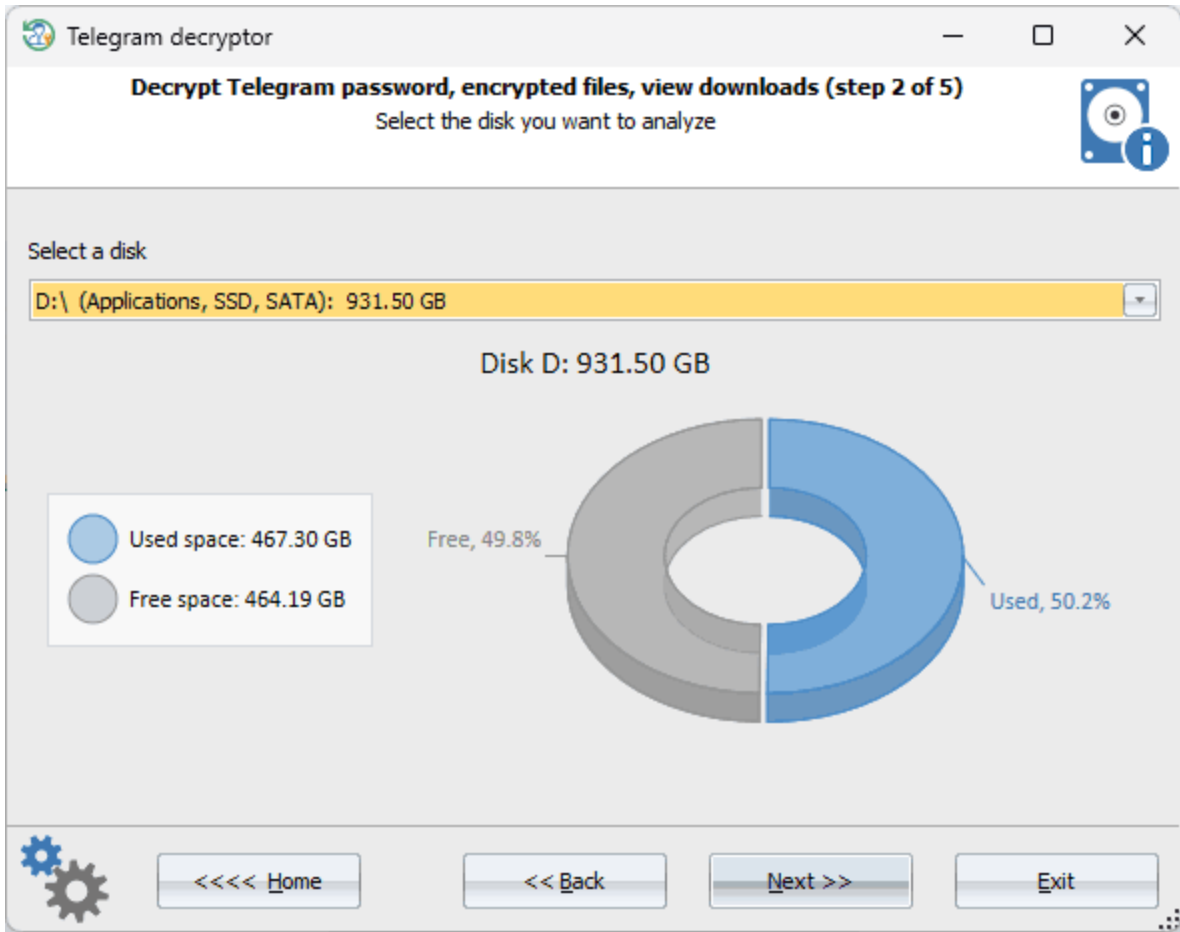
Telegram

Windows,

Telegram Desktop. Telegram

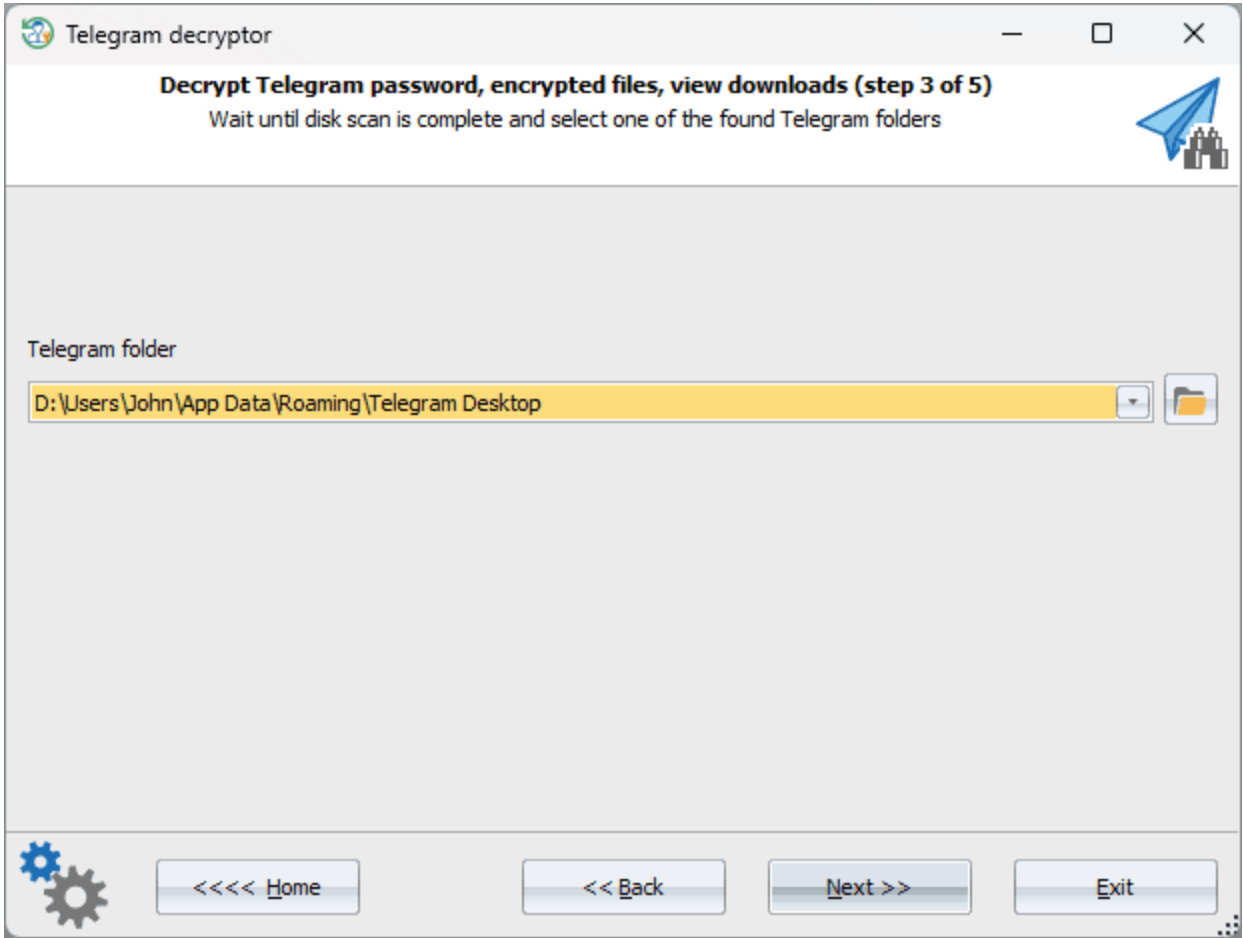
Reset Windows Password

Telegram Desktop.



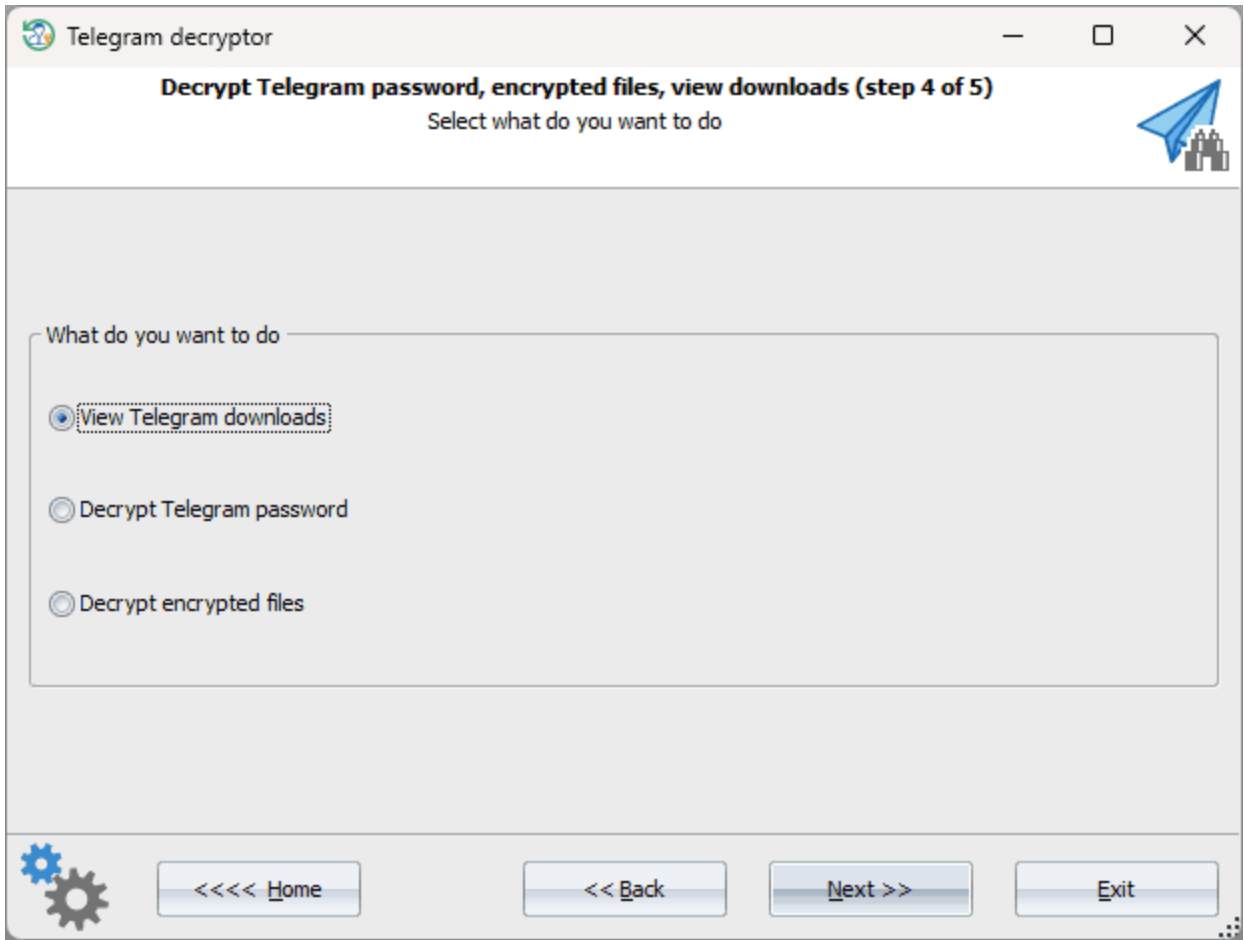
Telegram Desktop.

Telegram



Telegram

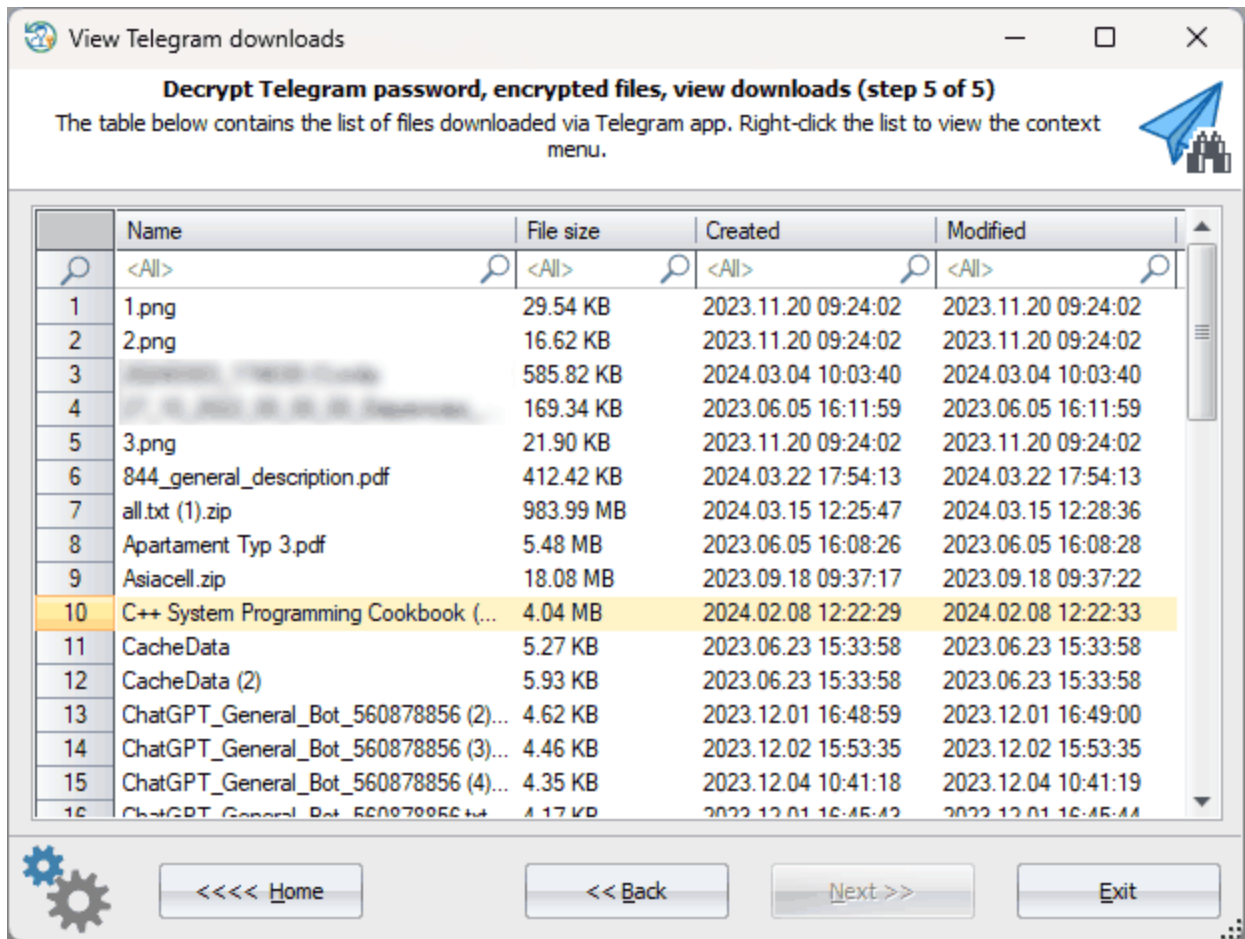
Telegram Desktop
Telegram



- [Telegram](#)
- [Telegram](#)
- [Telegram](#)

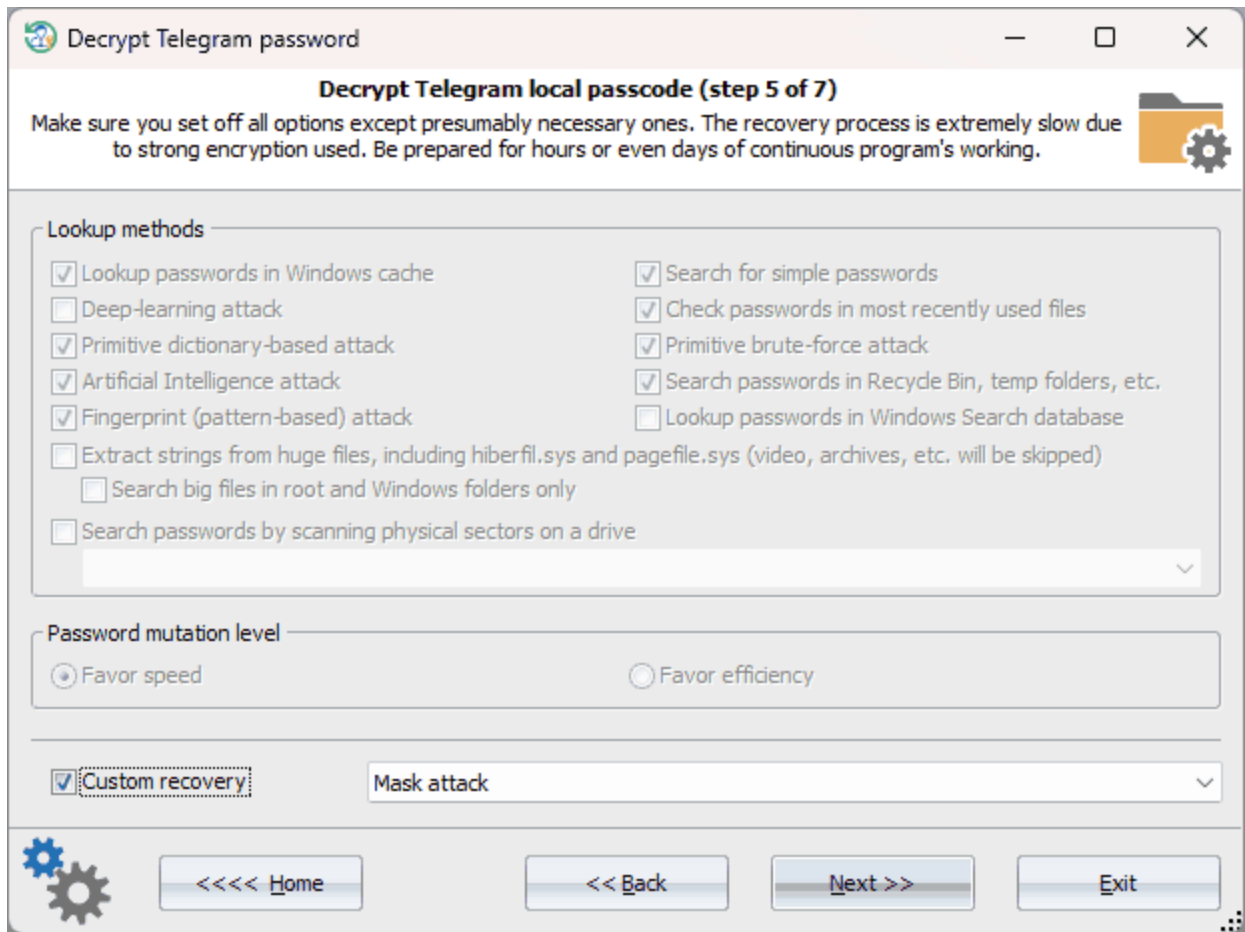
3.7.14.1

Telegram

Telegram
HTML

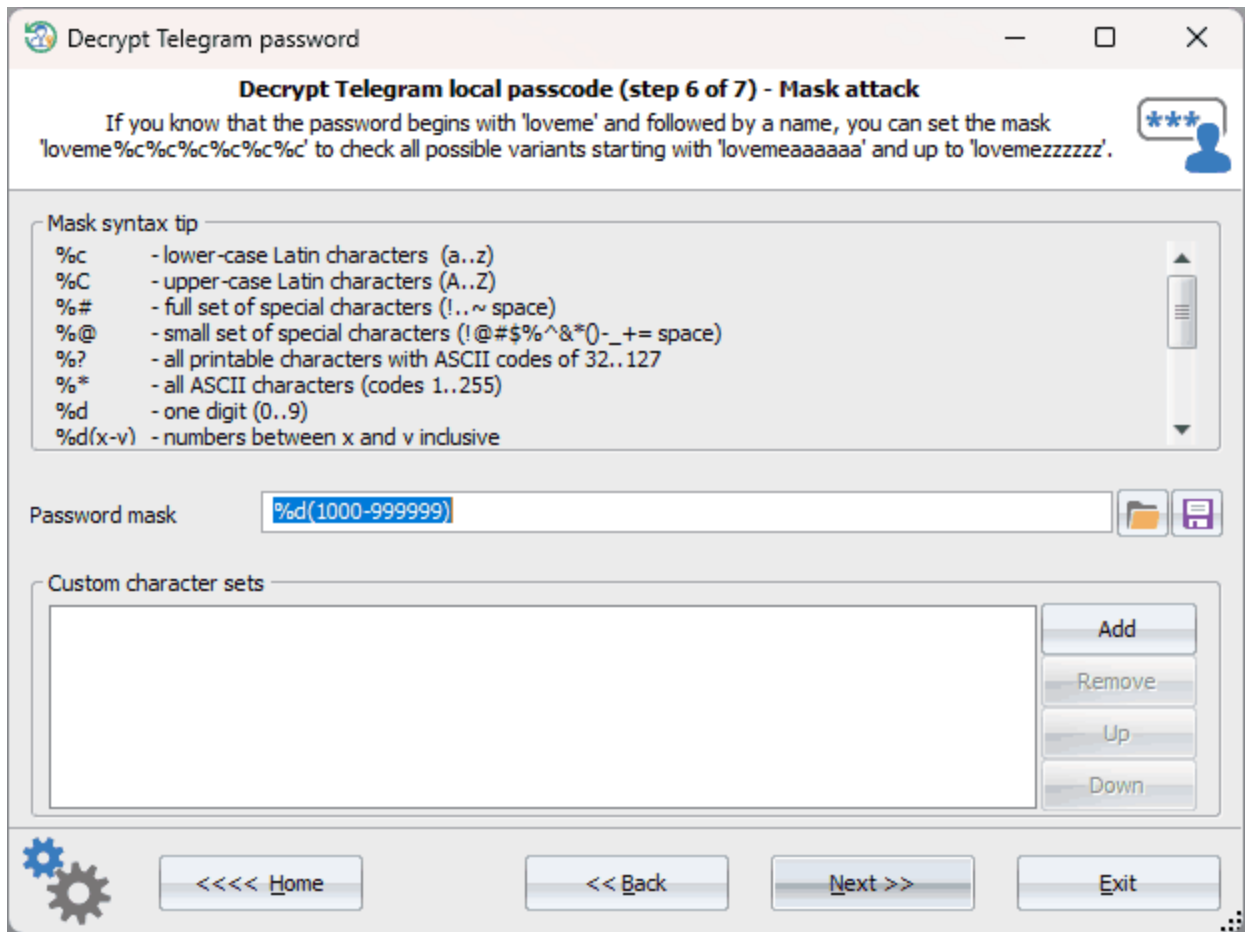
3.7.14.2

Telegram



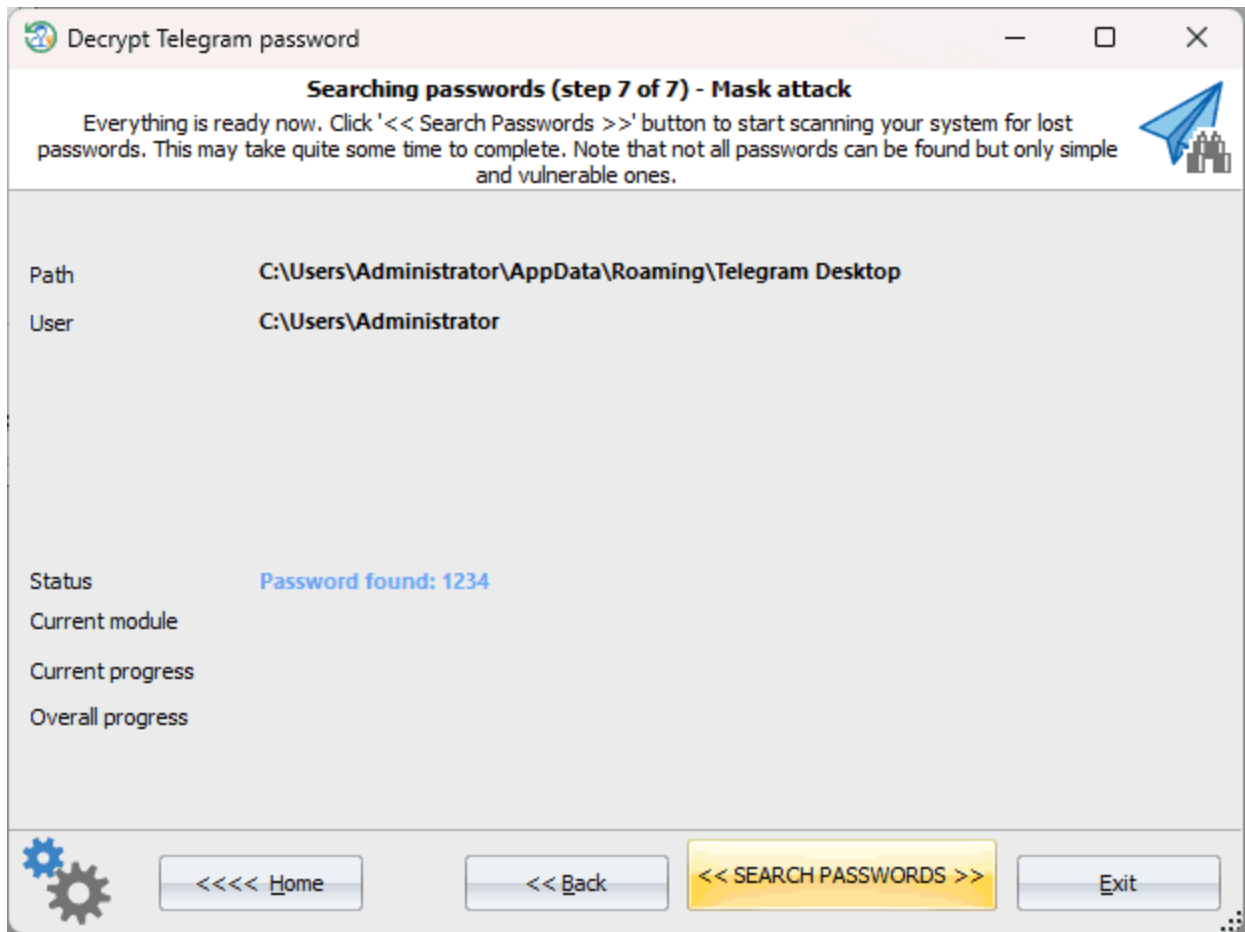
Telegram

Windows



4 6 . . . '0000' '999999'.

Telegram

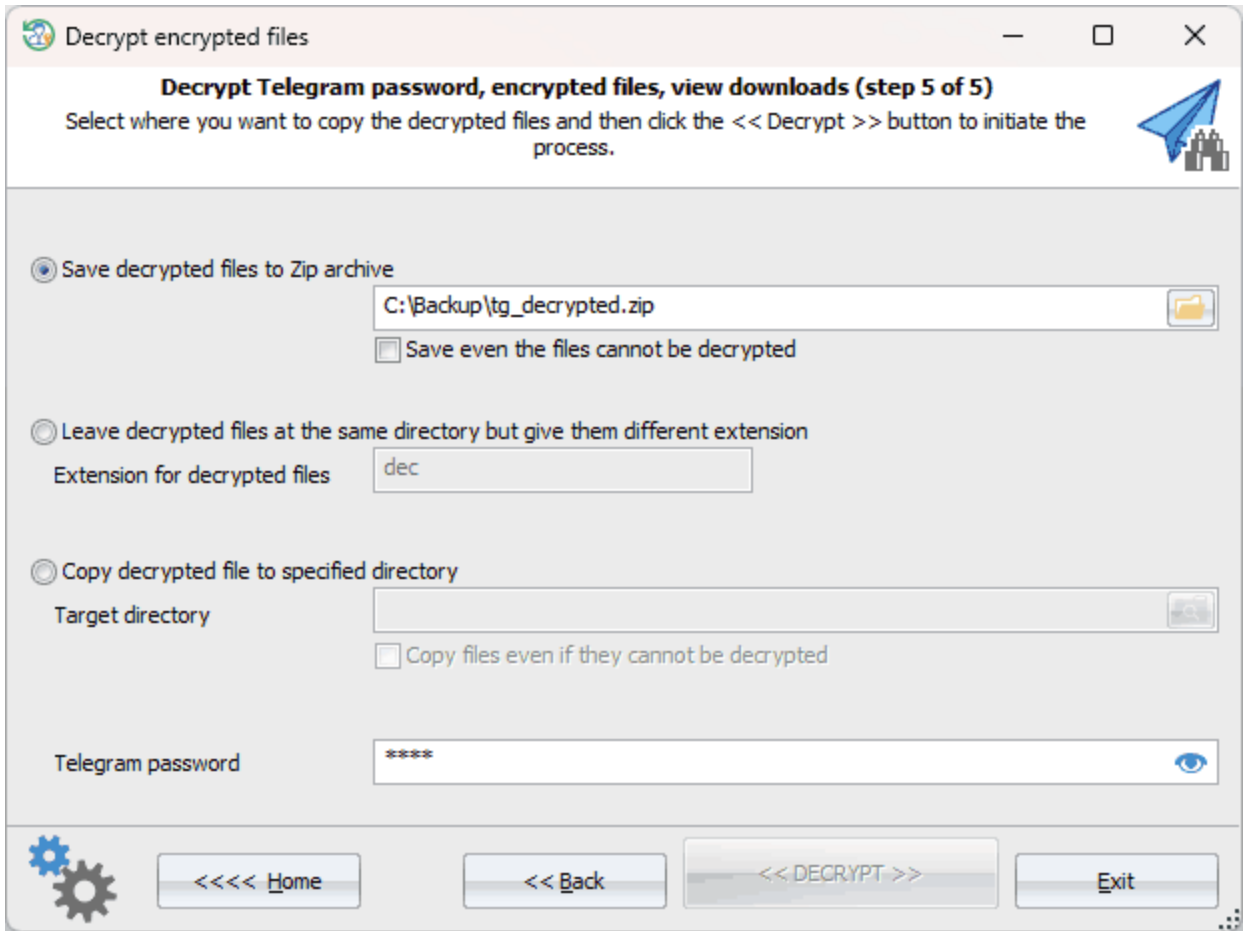


Telegram,

Hashcat.

3.7.14.3

Telegram



Telegram

Telegram.

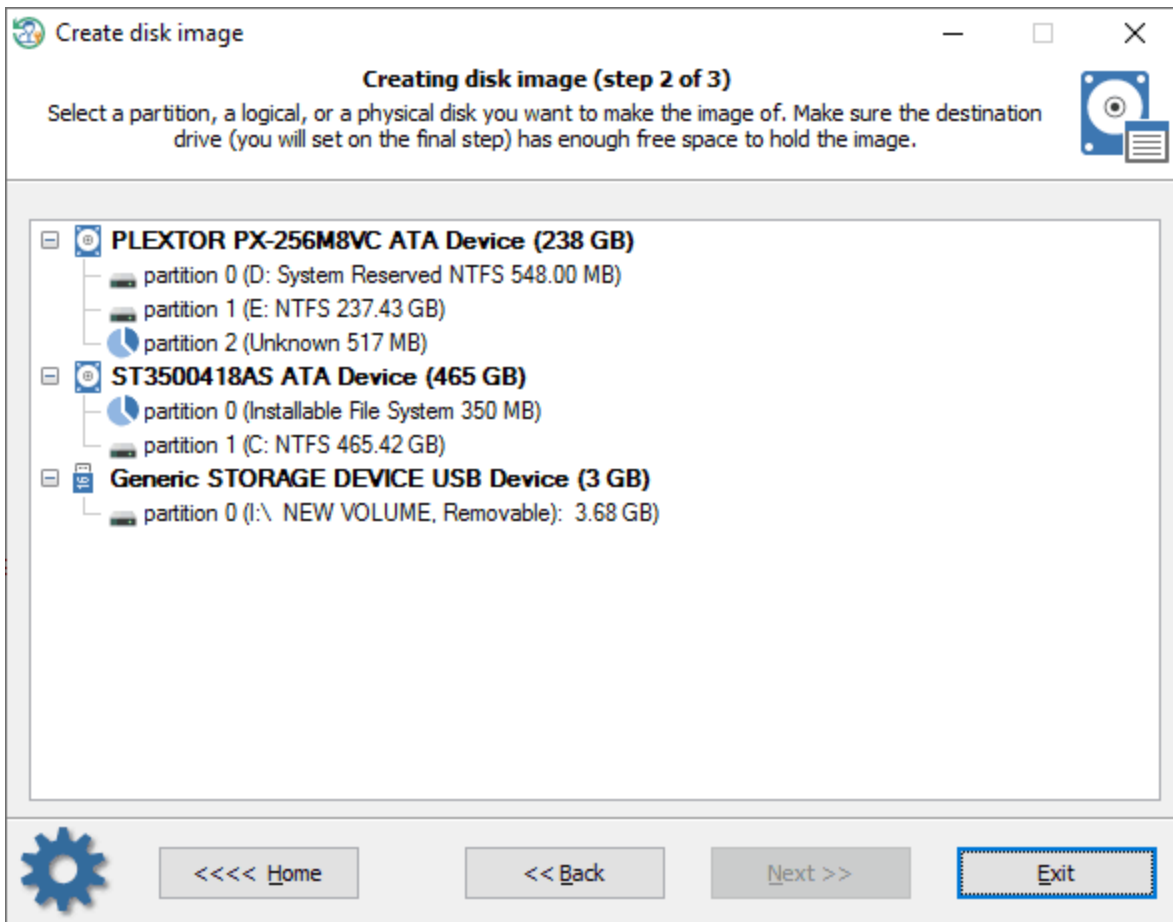
- ZIP
- DEC, XXXXXX.DEC, YYYYYYY.DEC
- maps Telegram.

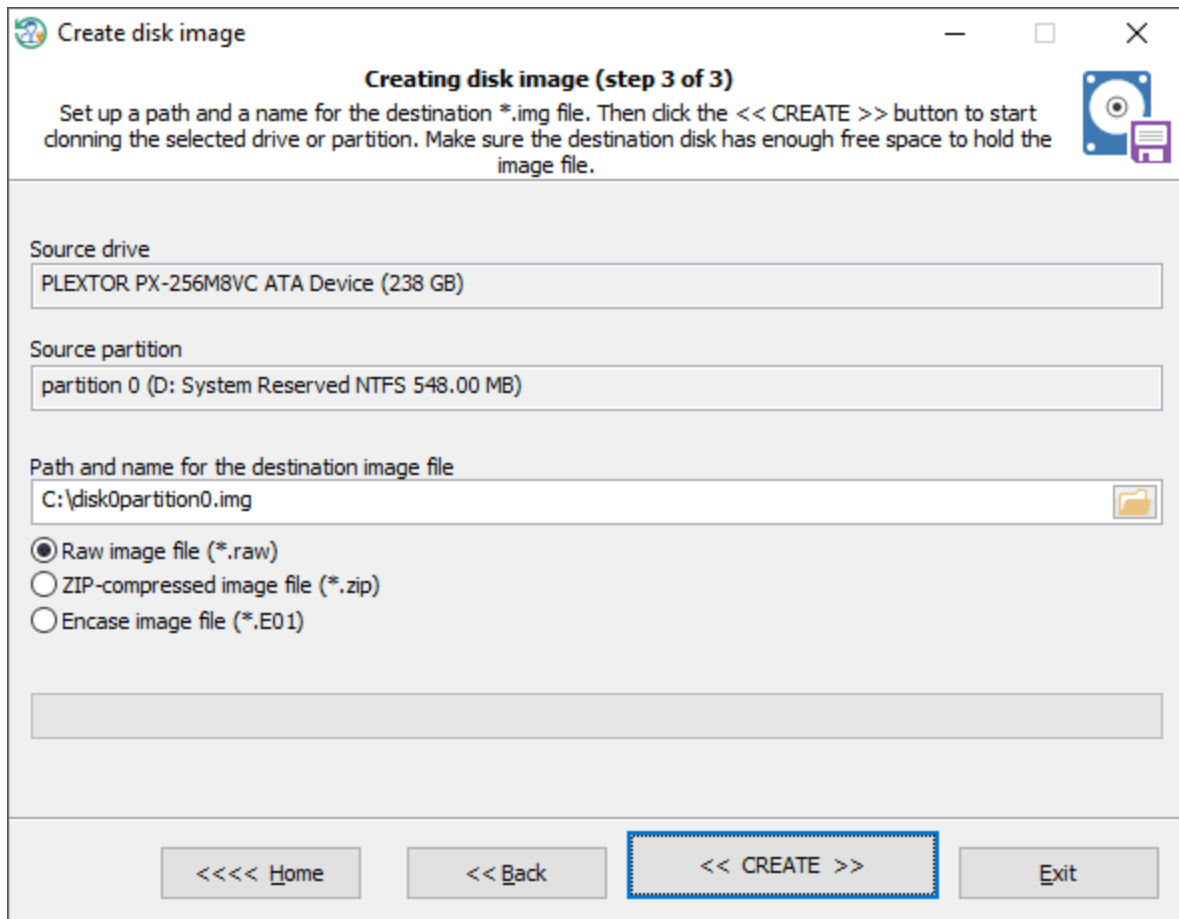
3.8

3.8.1

Windows

RWP



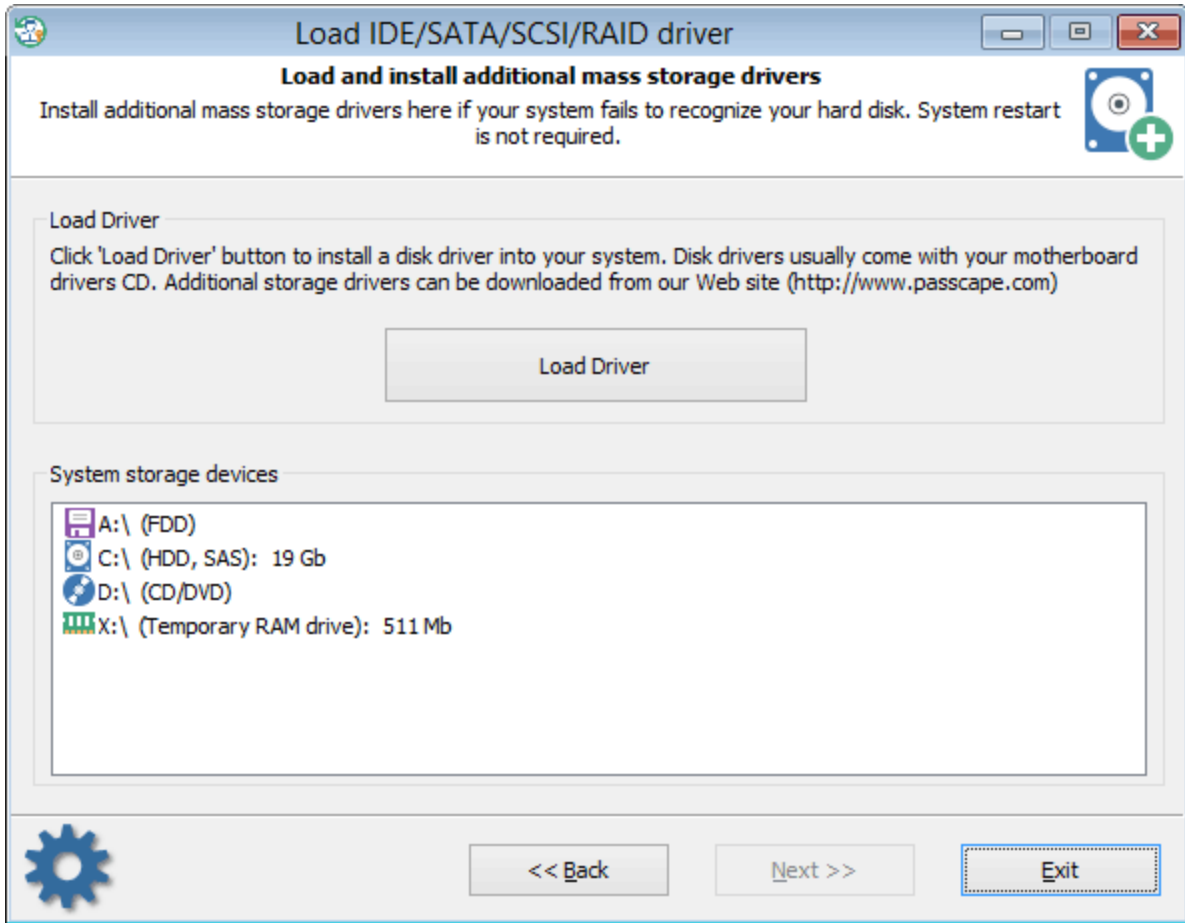


>>"

"<<

zip-

3.8.2



IDE/SATA/SCSI/RAID/NVME

: ATI, Highpoint,
 Intel, Jmicron, Marvell, Nvidia, Silicion Image, Sis, Uli, Via, Vmware. X:
\Apps\Drivers. HDD Nvidia,
 *.INF X:\Apps\Drivers\Nvidia.

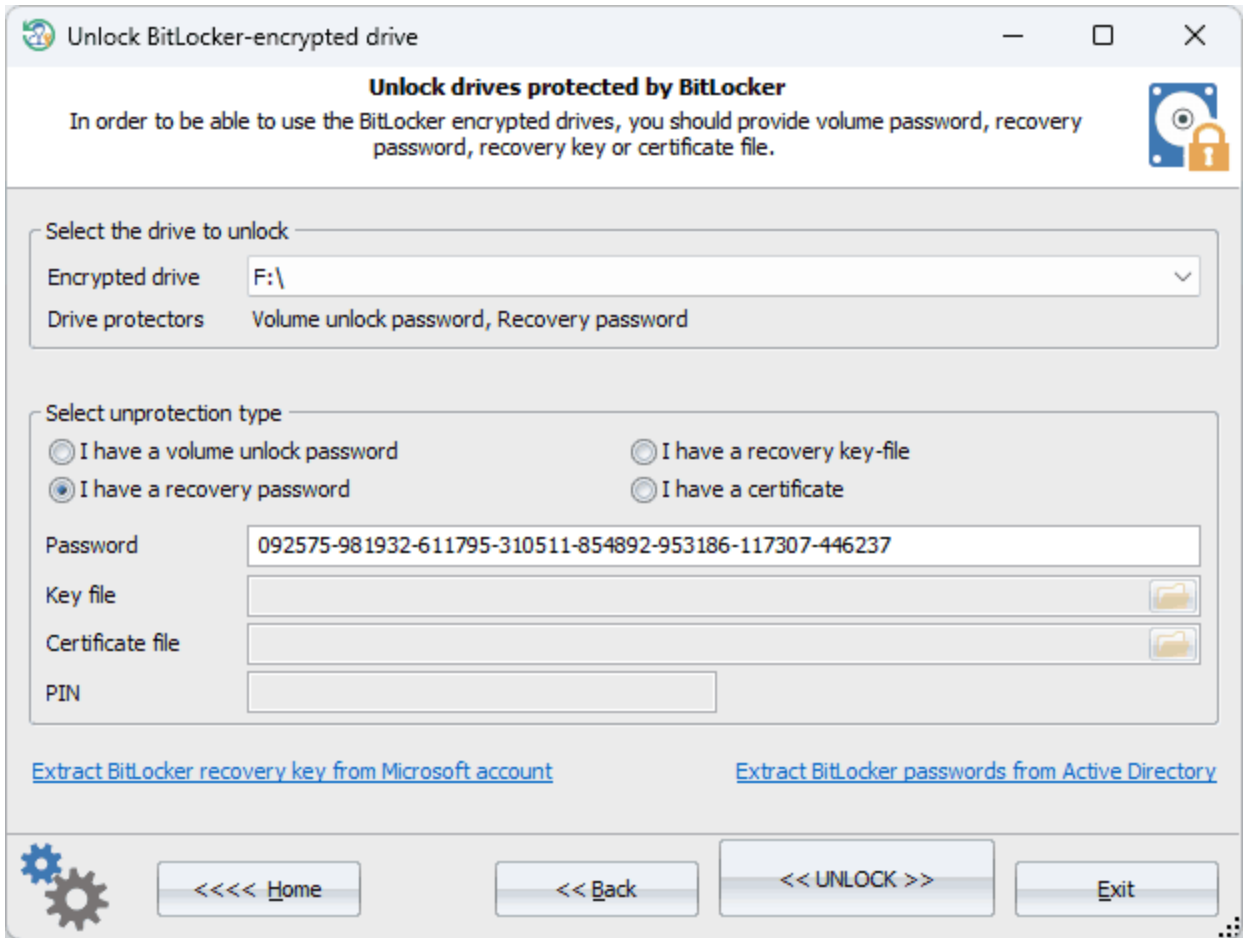
PC

Windows 11 x64.

Reset Windows Password

3.8.3

Bitlocker



Bitlocker,

<< UNLOCK >>

Bitlocker

[Extract BitLocker passwords from Active](#)

[Directory](#)

BitLocker
BitLocker,

-
-
-

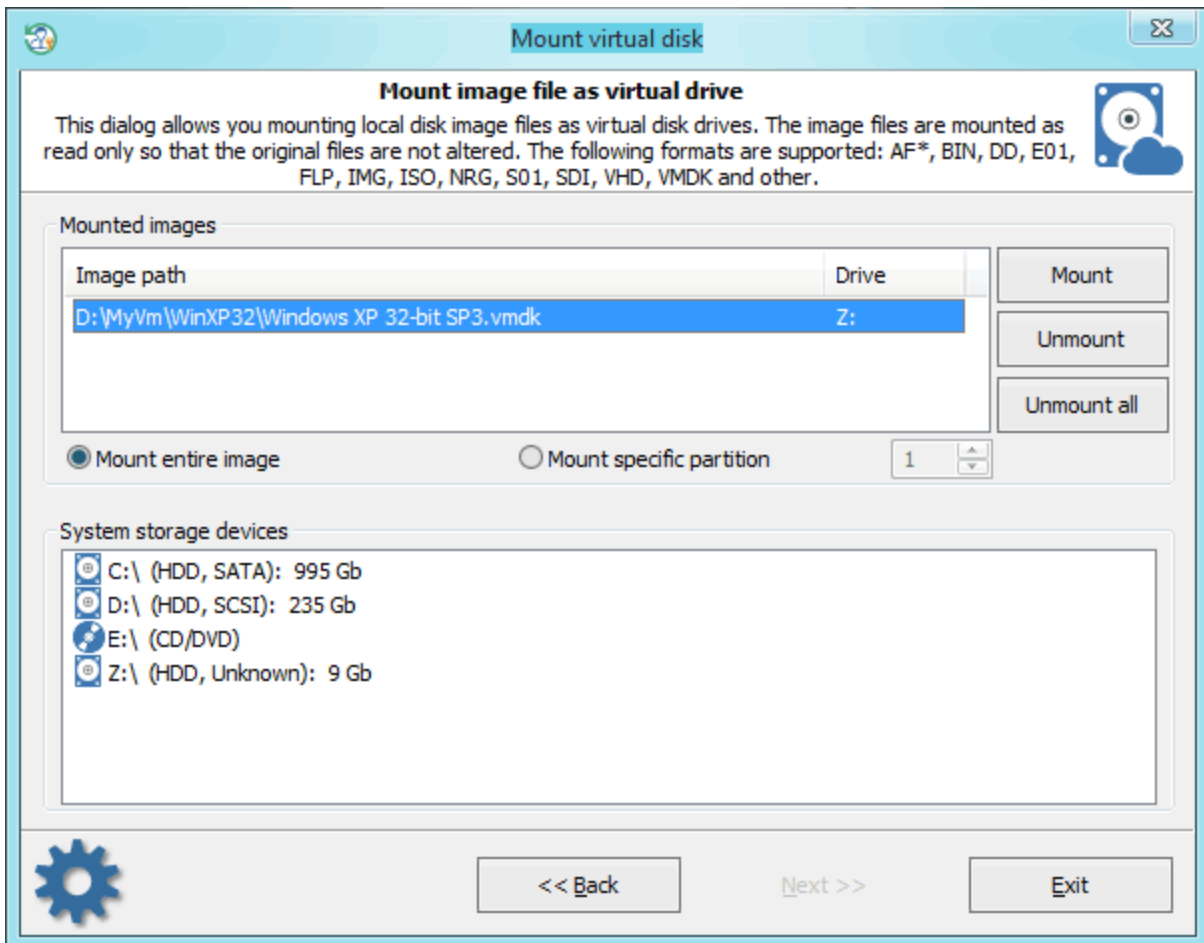
()

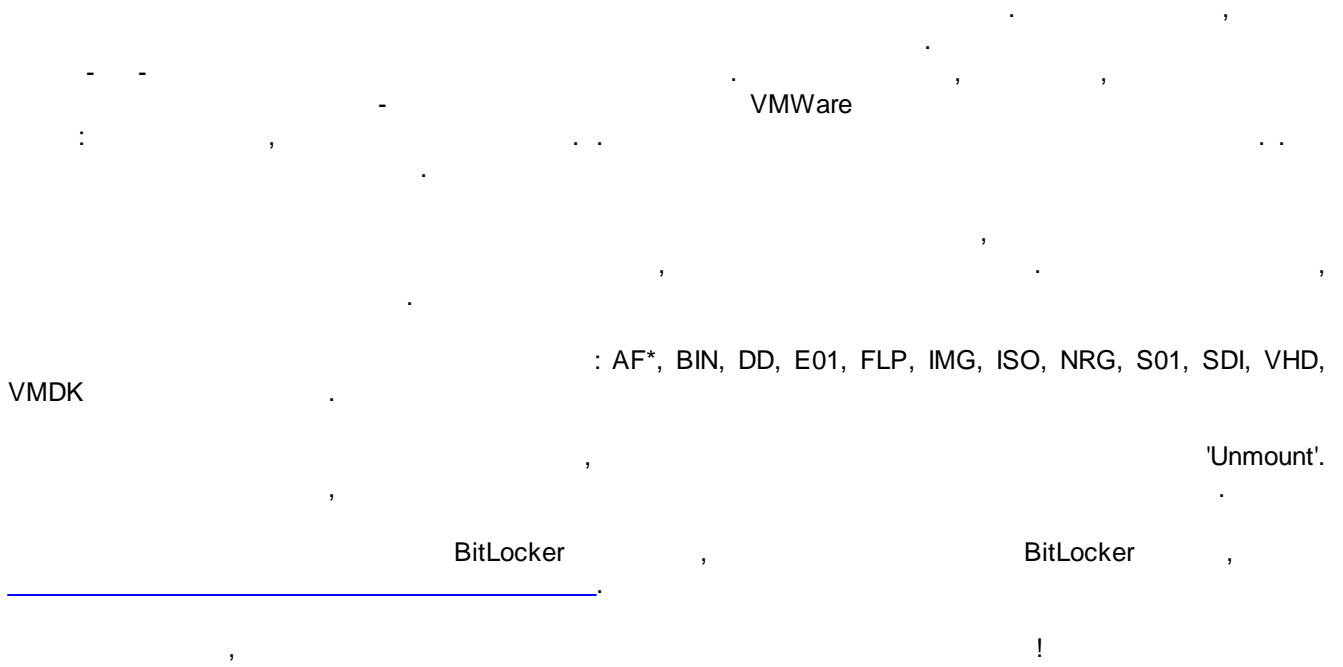
BitLocker

Microsoft'

- Microsoft
- BitLocker. 48-
- RWP,
- << >> BitLocker
- Windows (BIOS, TPM BitLocker)
- BIOS BitLocker.

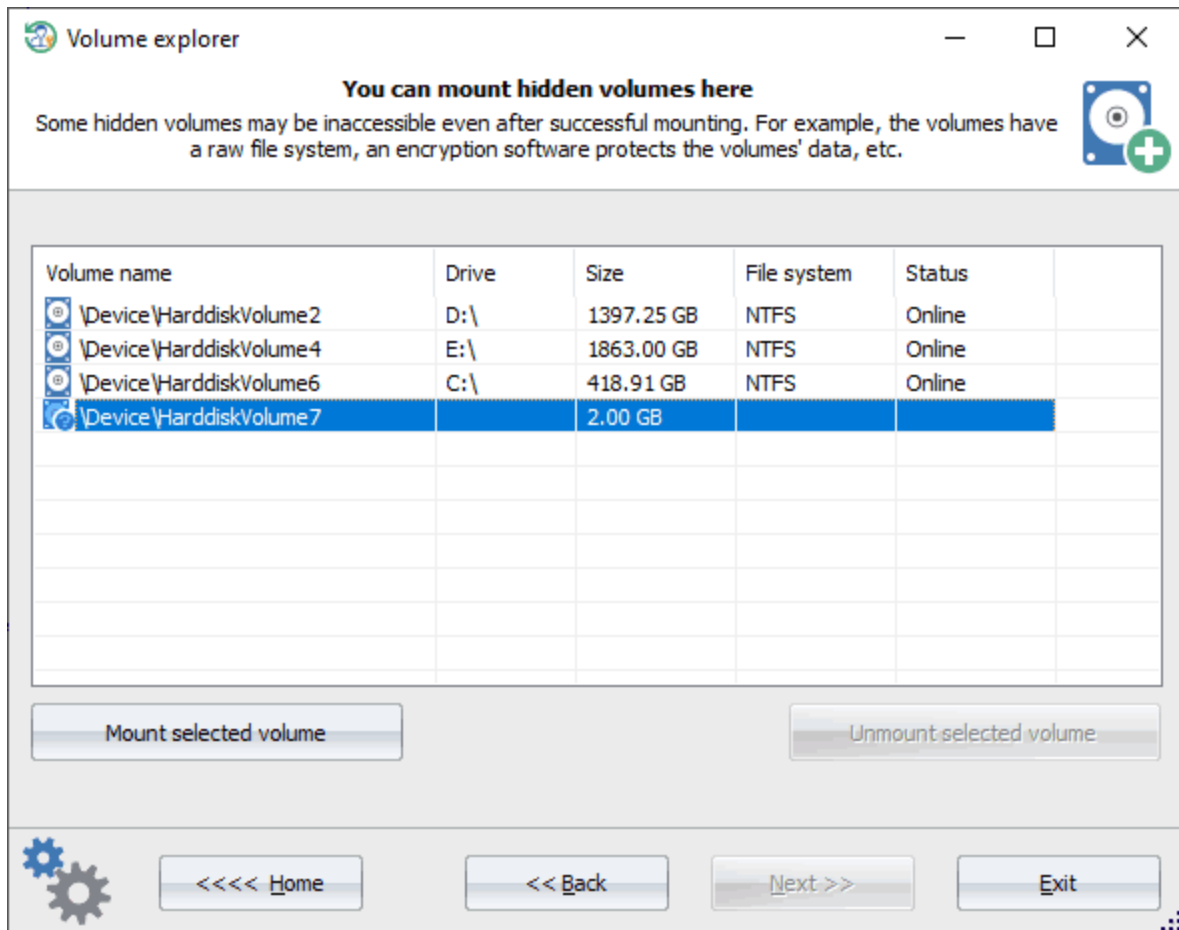
3.8.4

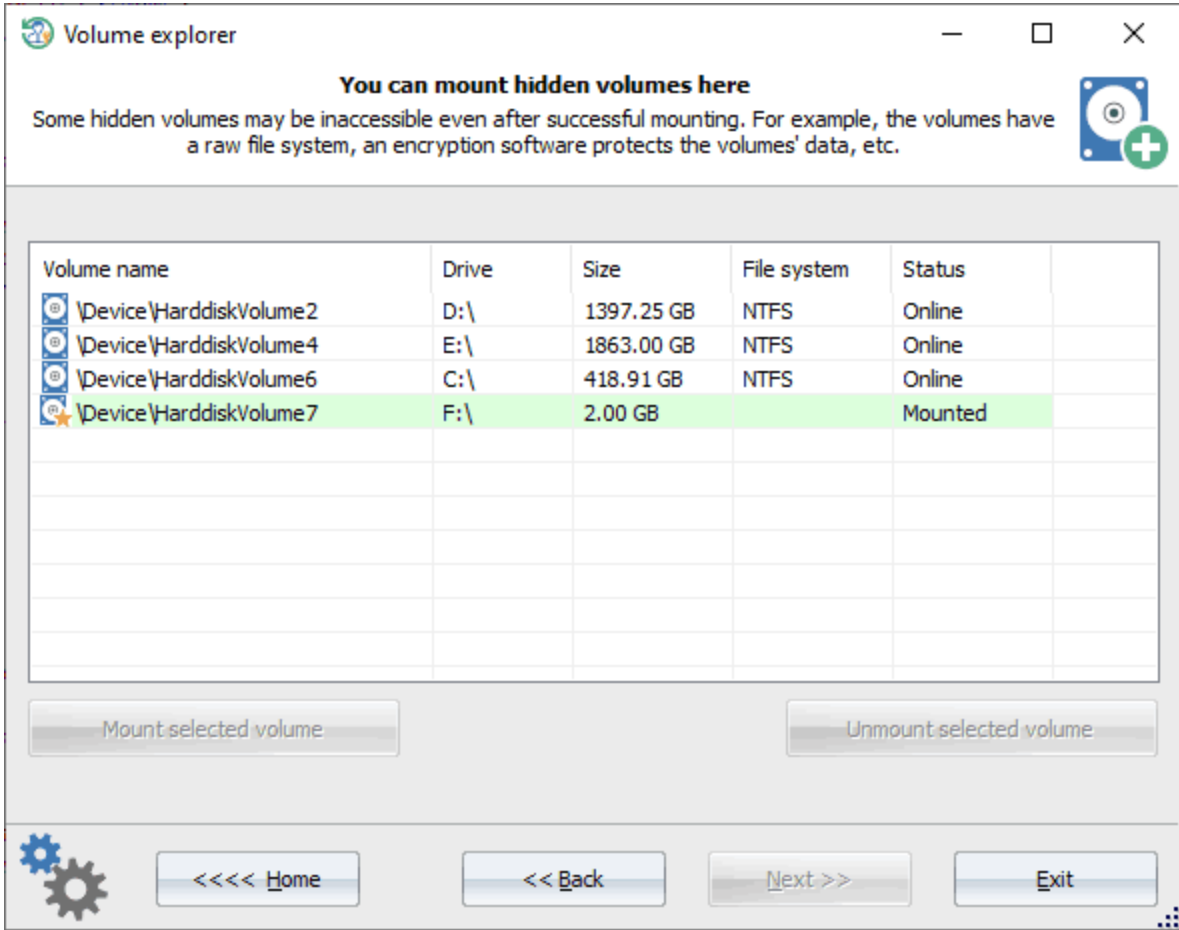




3.8.5

Windows






(BitLocker) raw,

3.8.6

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

<input type="radio"/> All local hard disk drives	<input type="radio"/> Selected drive
<input type="radio"/> 'Documents' folders for every user	<input checked="" type="radio"/> All files and folders for selected account
<input type="radio"/> 'Documents' folder for selected account	<input type="radio"/> Specified location(s)

User profile directory

D:\Users\test ▼

 << Back Next >> Exit

Last modified files [minimize] [maximize] [close]

Extract and view history information (step 3 of 4)
Set up additional output filters to skip unnecessary items.

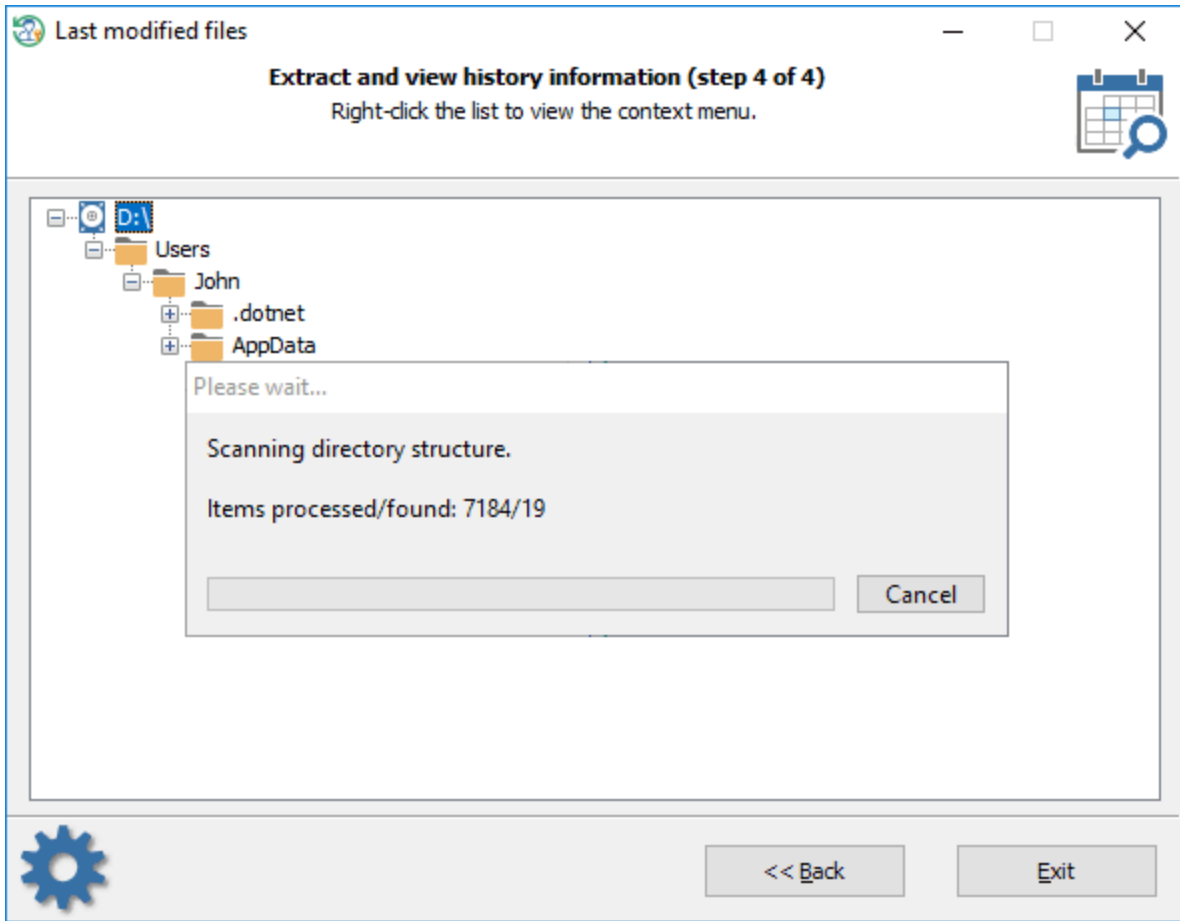
Output filter

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 [calendar icon] [dropdown arrow] 0:00:00 [time spinner]

To date: 05.10.2018 [calendar icon] [dropdown arrow] 23:59:59 [time spinner]

[gear icon] << Back Next >> Exit

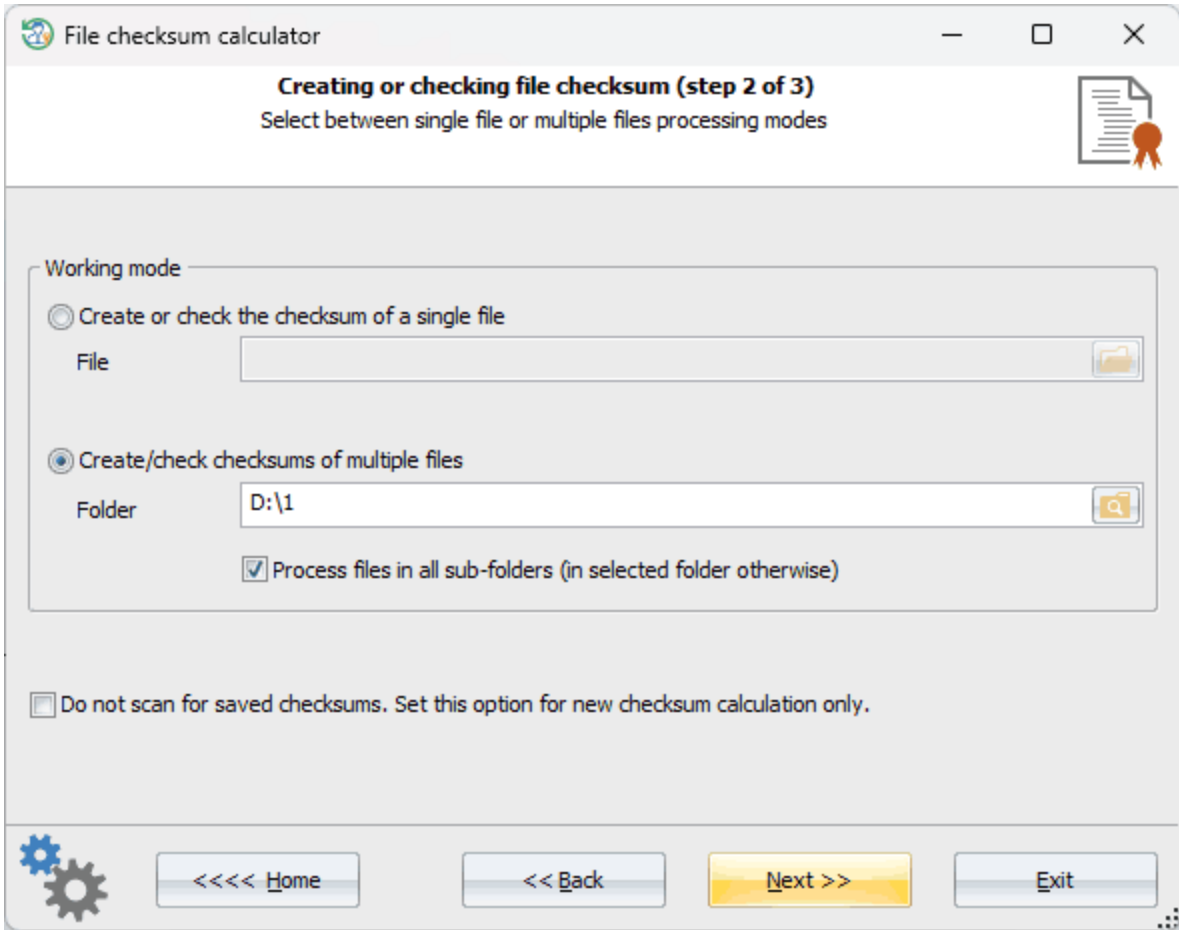


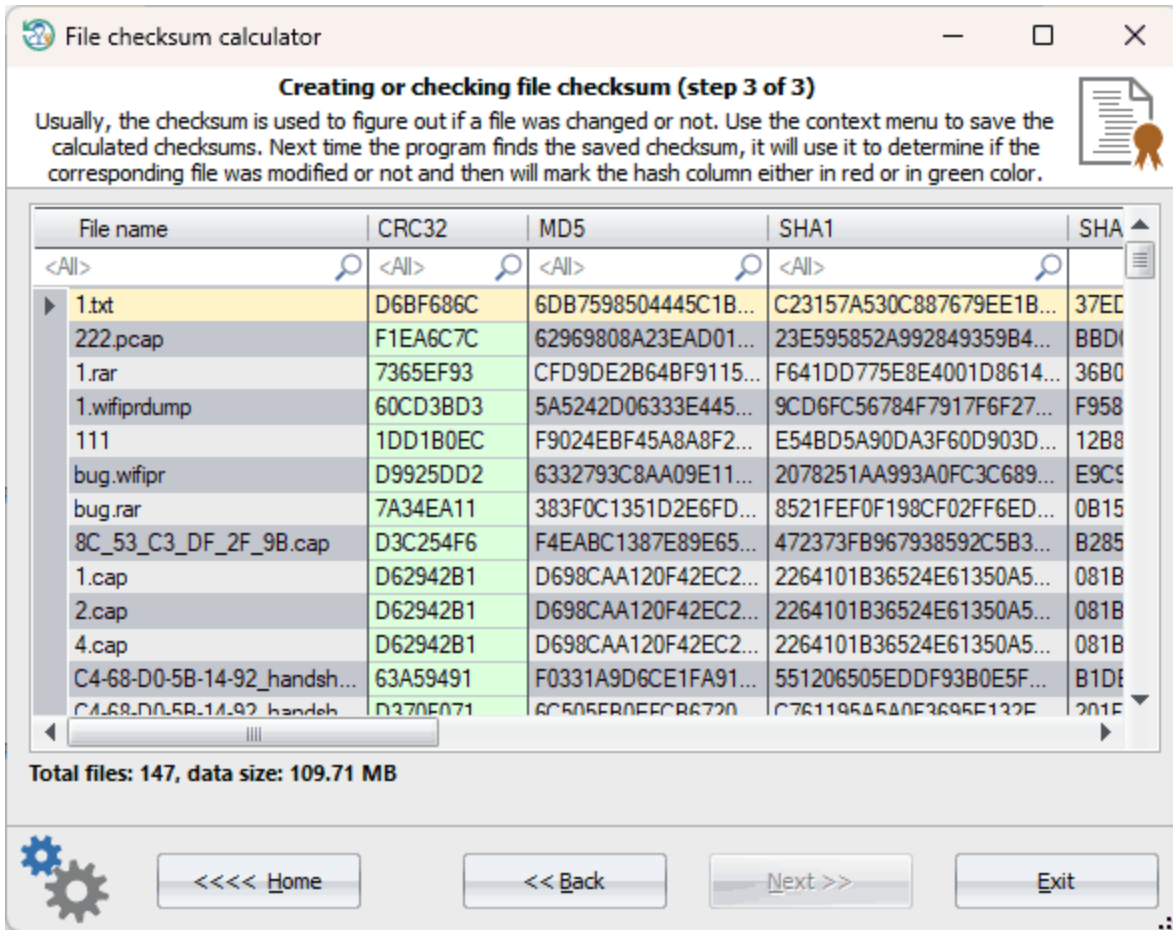
3.8.7

3.8.8

MD5, SHA1, SHA-256 SHA-512.

CRC32,

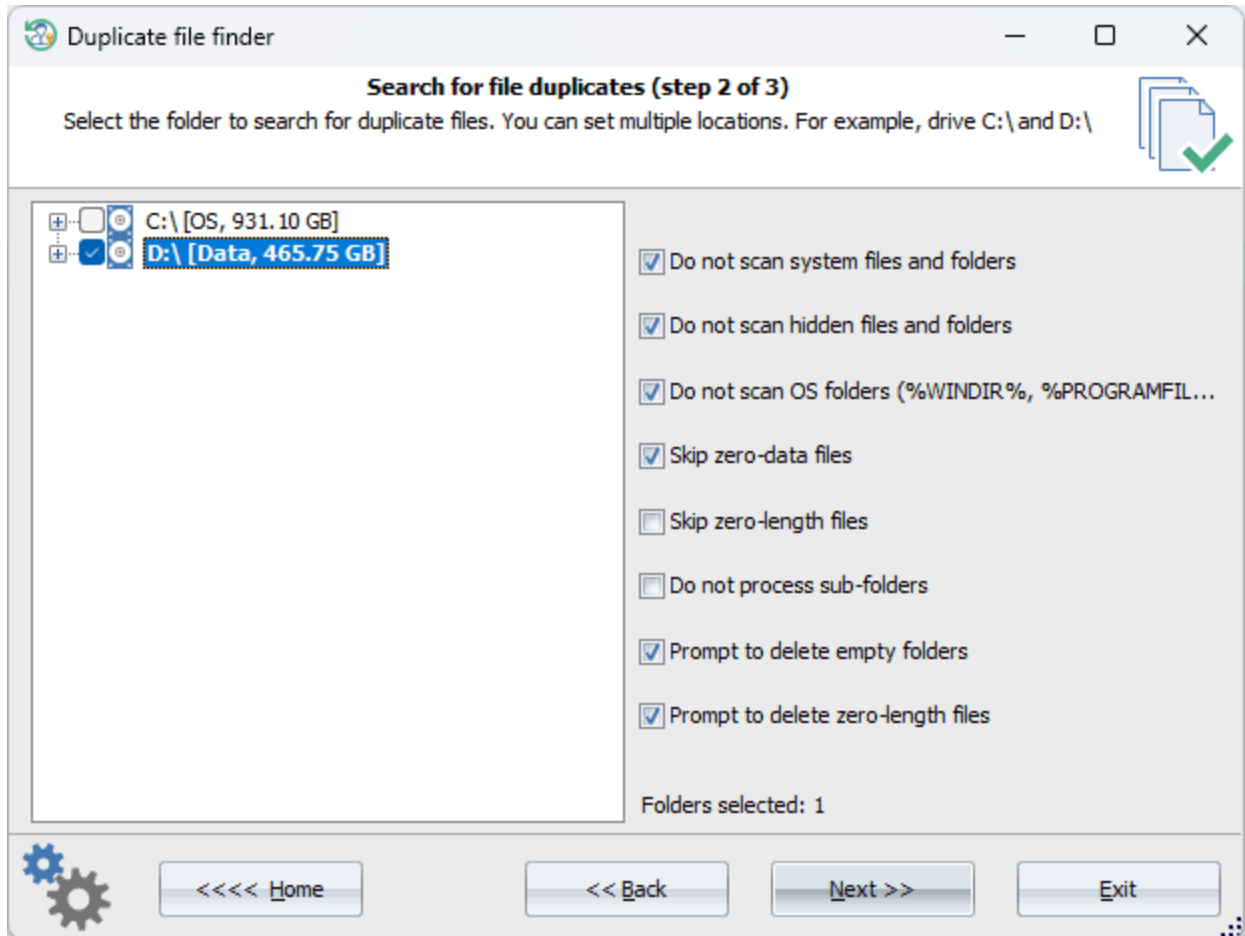




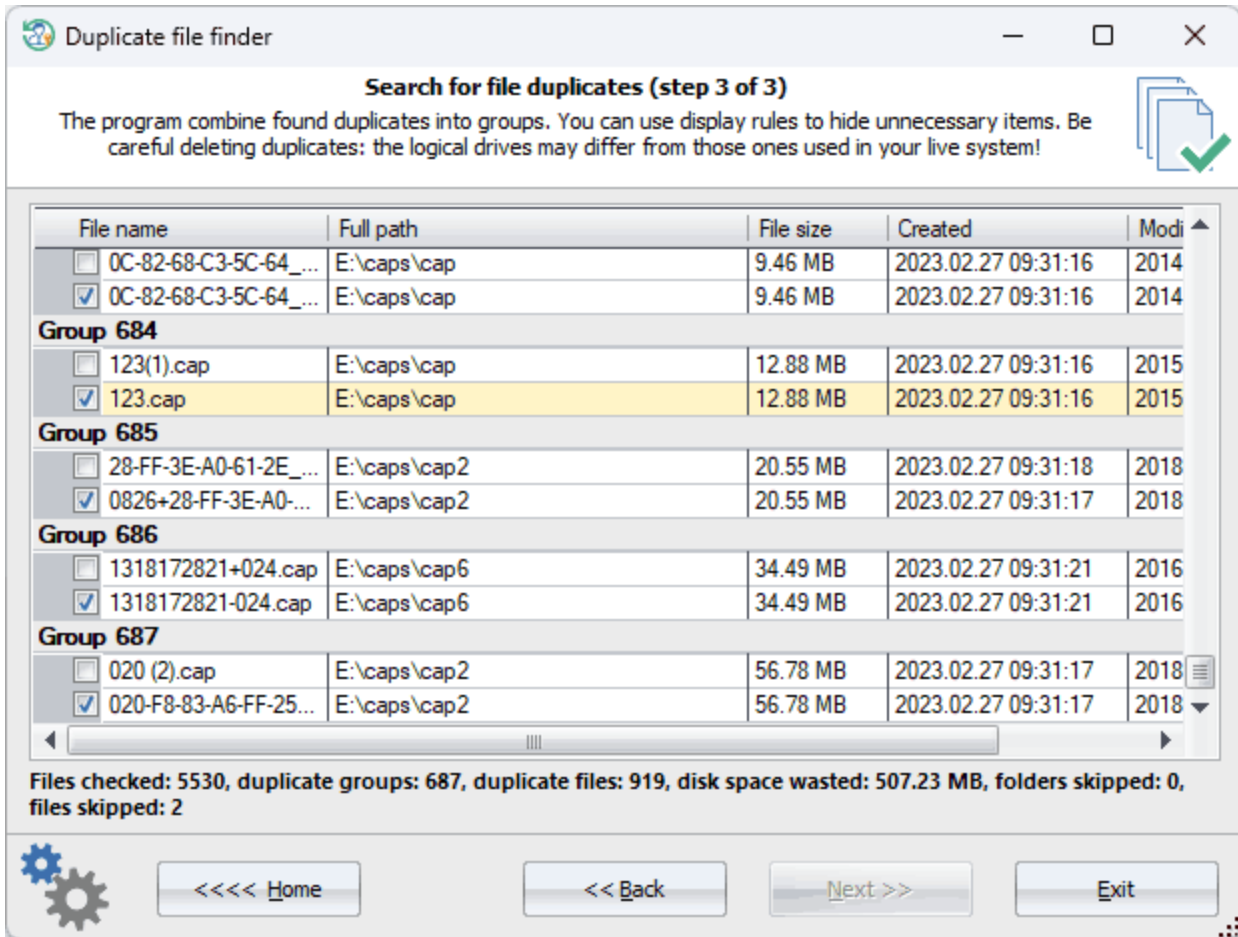
(* .crc, * .md5, * .sha, * .sha256 * .sha512),

readme.txt, CRC32, MD5, SHA1, SHA256, SHA512, readme.txt.crc, readme.txt.md5..., readme.txt.sha512

3.8.9



- **Do not scan system files or folders.** () , SYSTEM.
- **Do not scan hidden files or folders.** () , HIDDEN.
- **Do not scan OS folders.** Windows, %WINDIR%, %PROGRAMFILES%, %PROGRAMDATA%
- **Skip empty-data files.**
- **Skip zero-length files.**
- **Do not process sub-folders.**
- **Prompt to delete empty folders.** Windows
- **Prompt to delete zero-length files.**



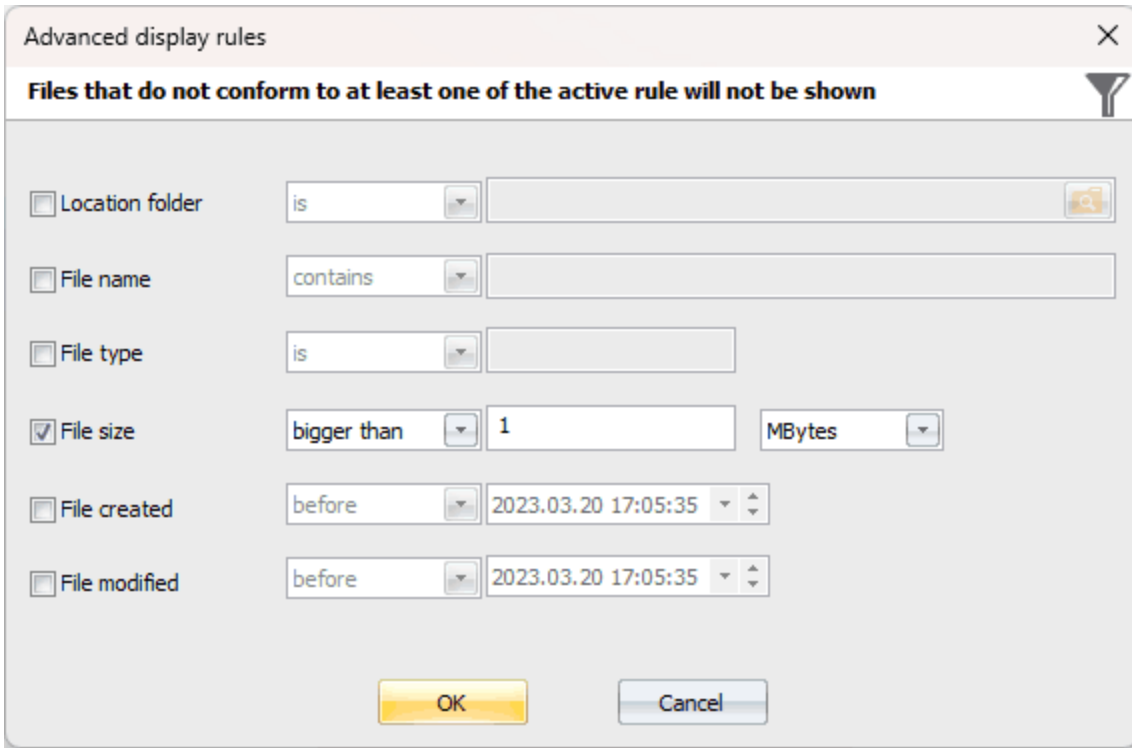
(,) . ,

Windows 10, Windows 11

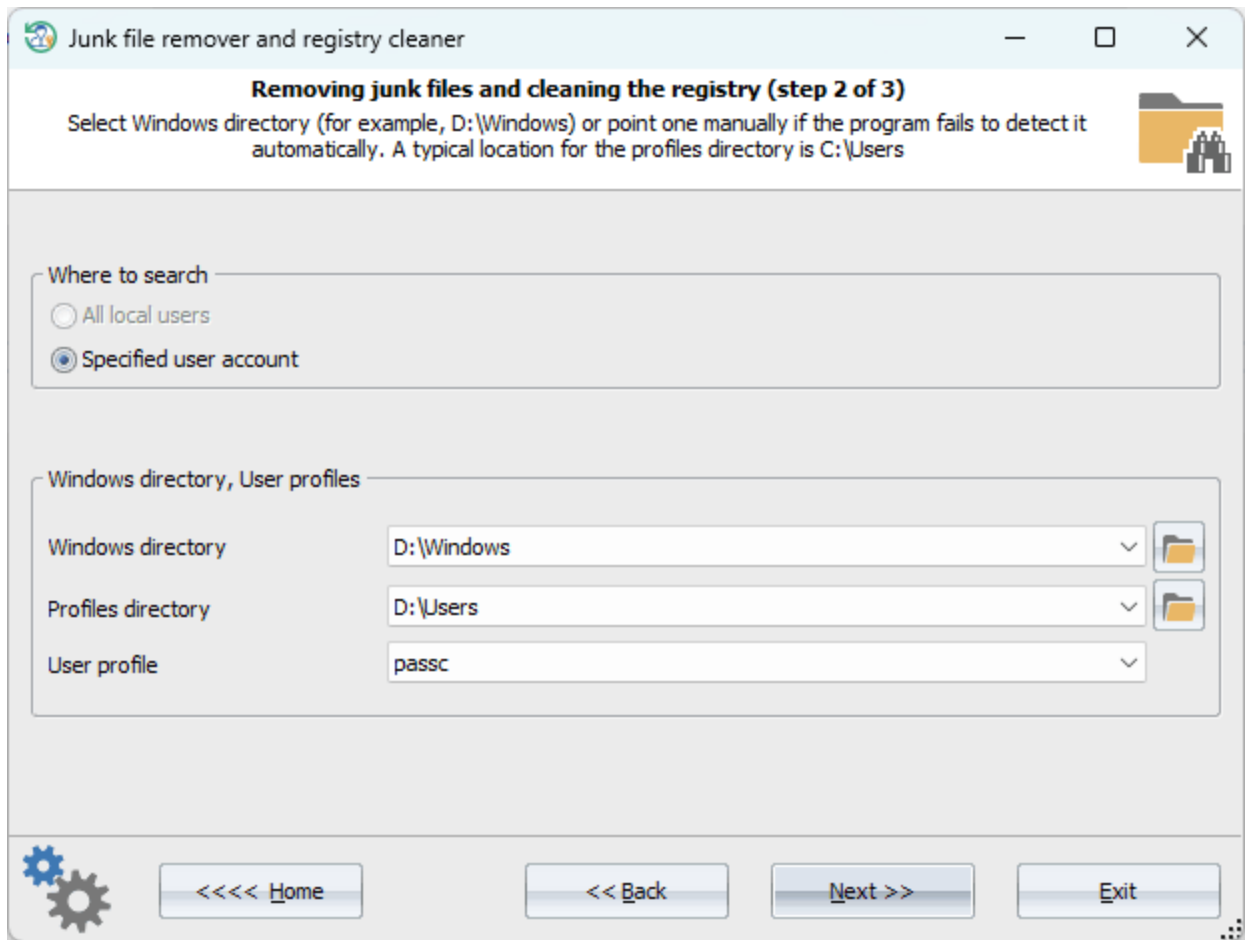
C:\Windows\System32\config\systemprofile\AppData\Local
: tw-XXXXXXXXXXXXXXXXX.tmp, X -

-
-

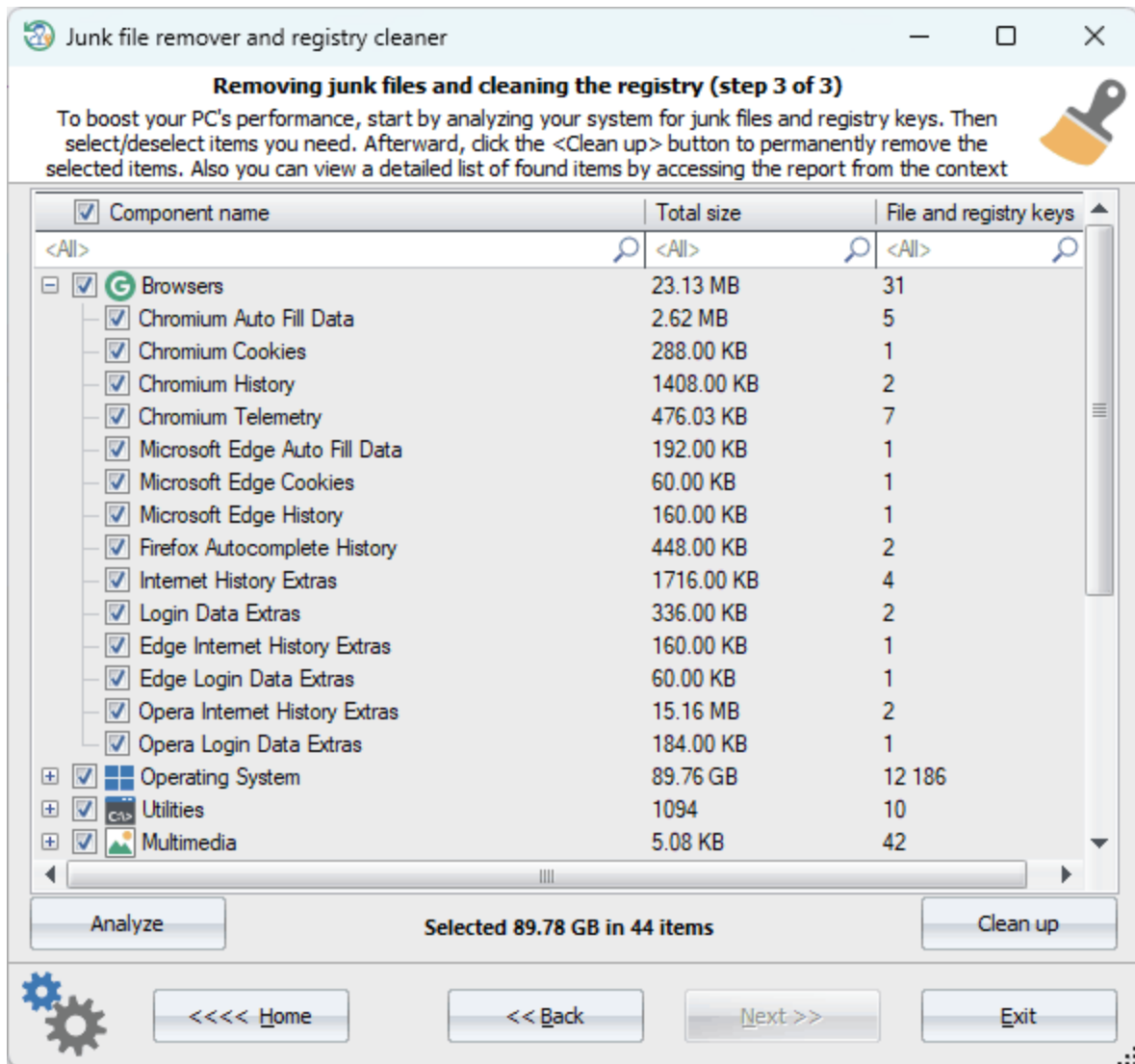
RWP



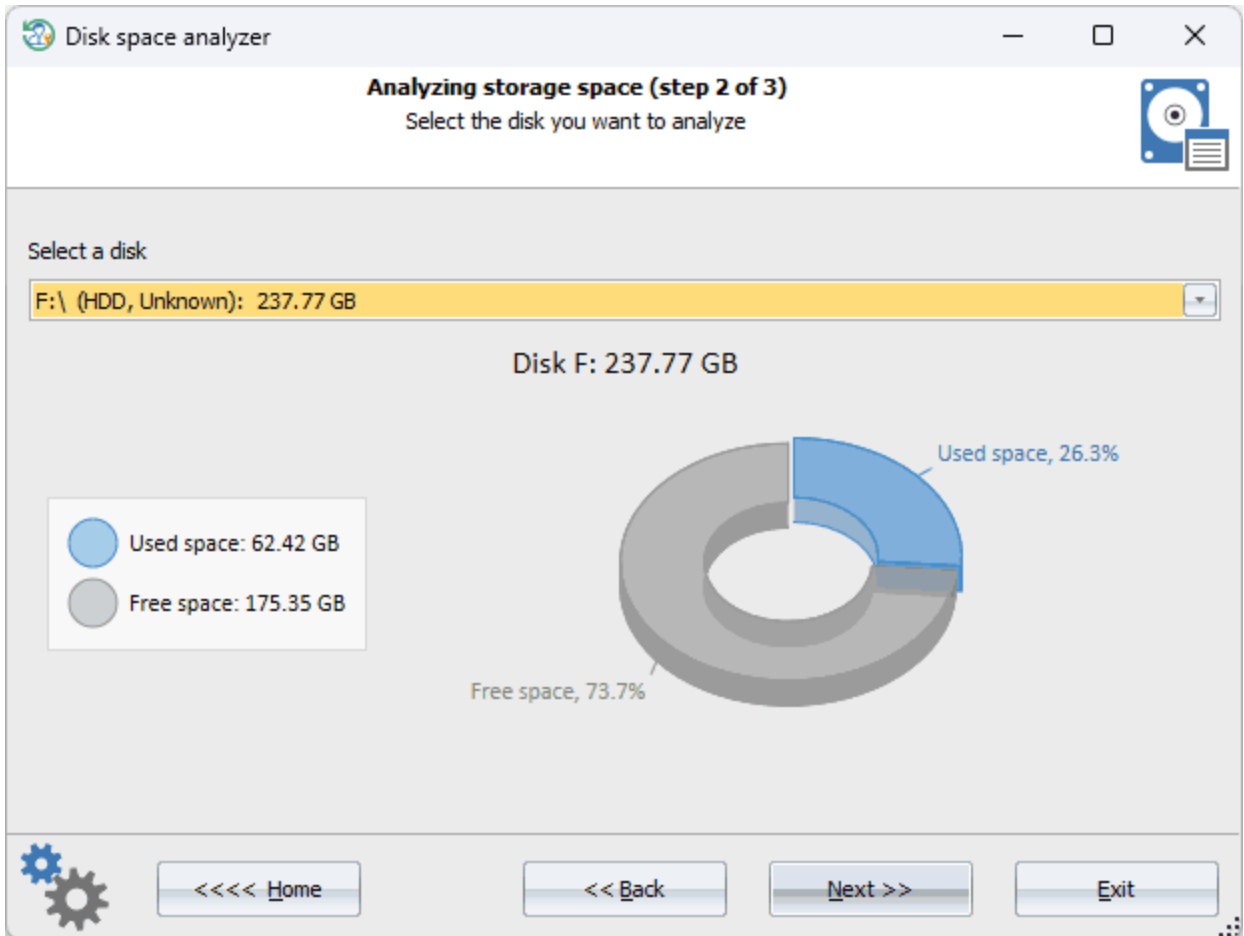
3.8.10

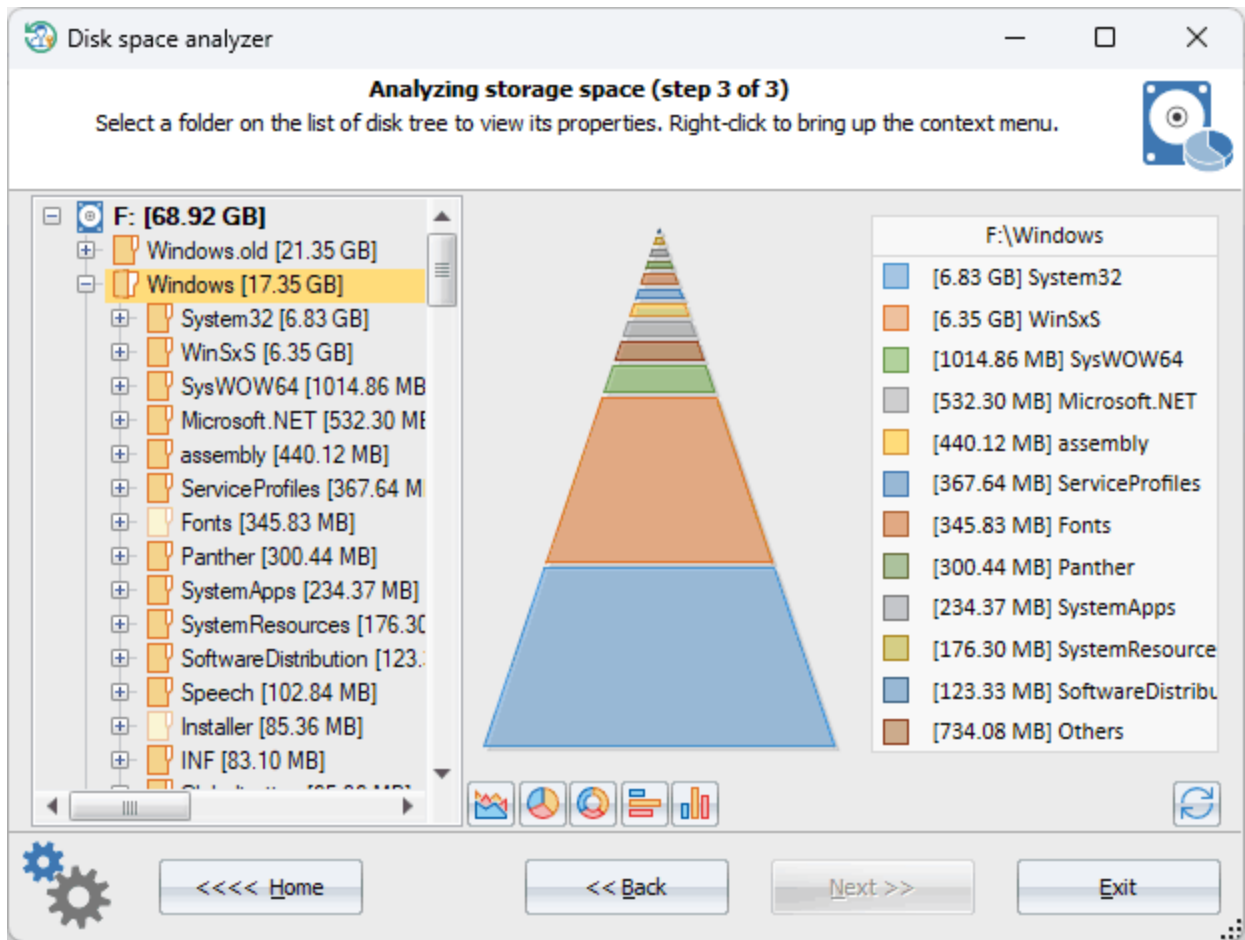


Windows



3.8.11

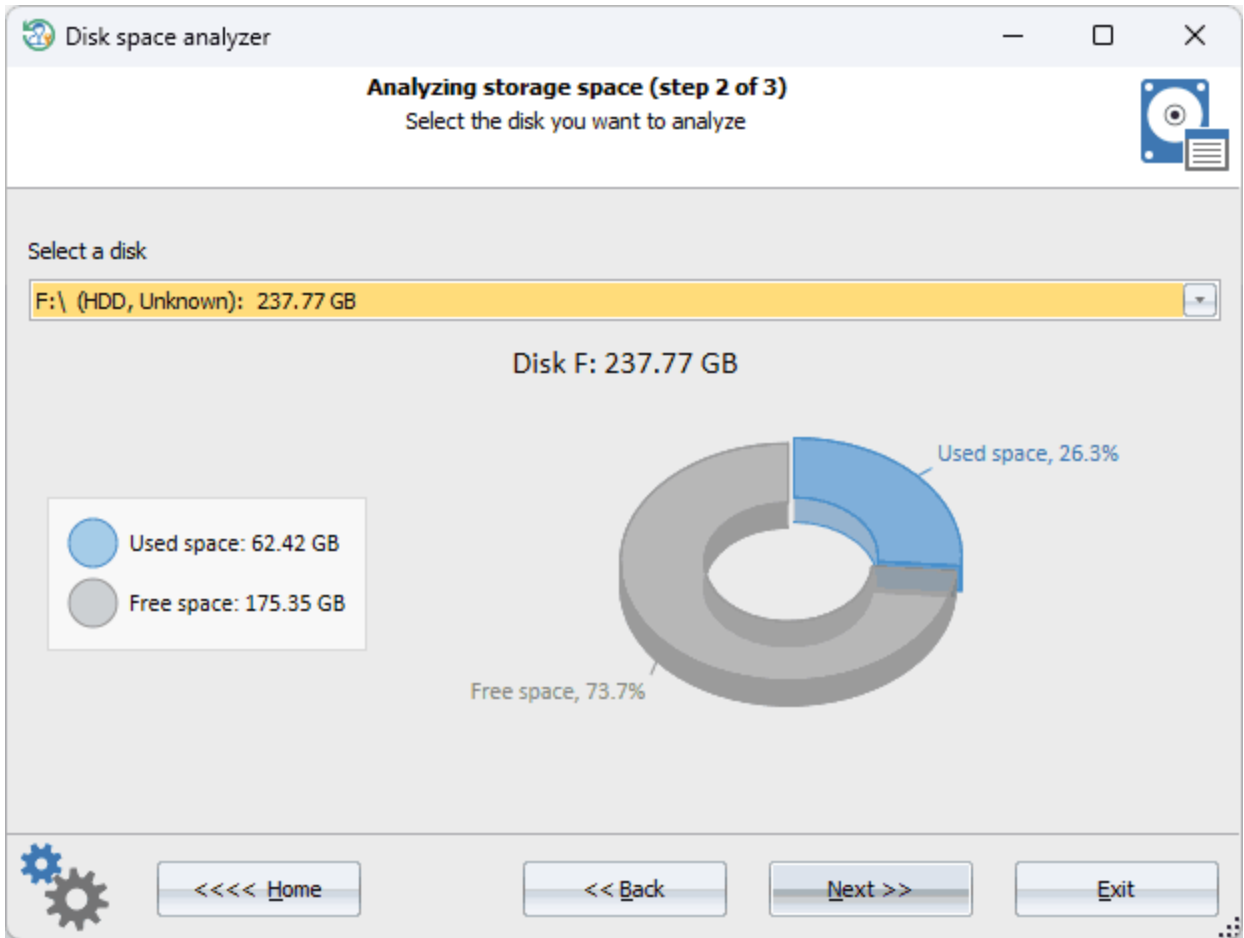


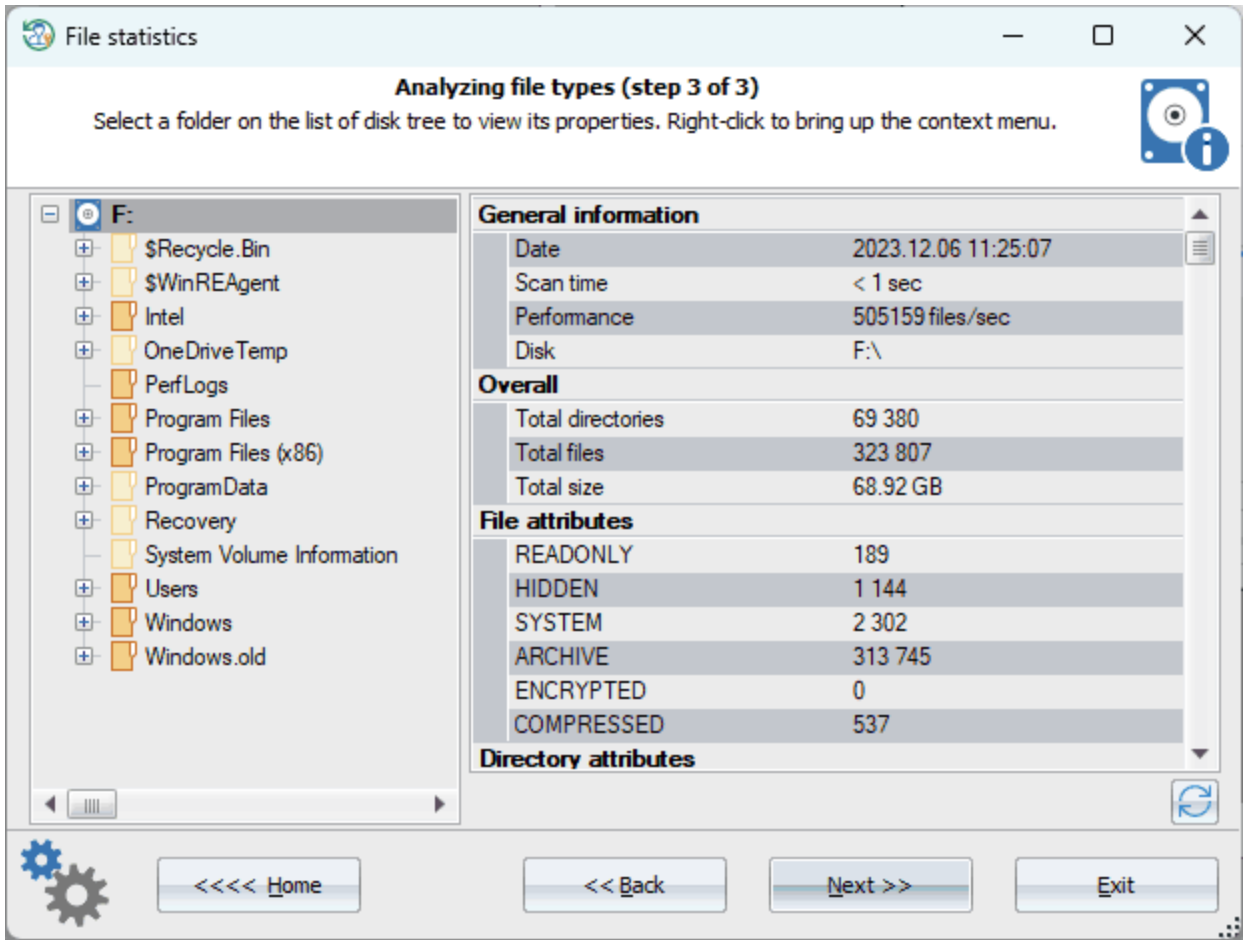


3.8.12

-
-
-
-
-
-

/





HTML,

3.8.13

1

(

1

Windows.
)

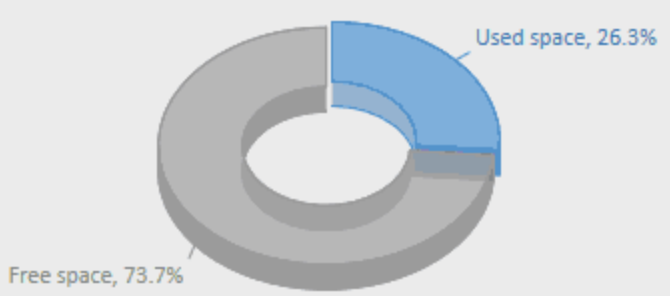
Fast disk search

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



Category	Percentage	Amount
Used space	26.3%	62.42 GB
Free space	73.7%	175.35 GB

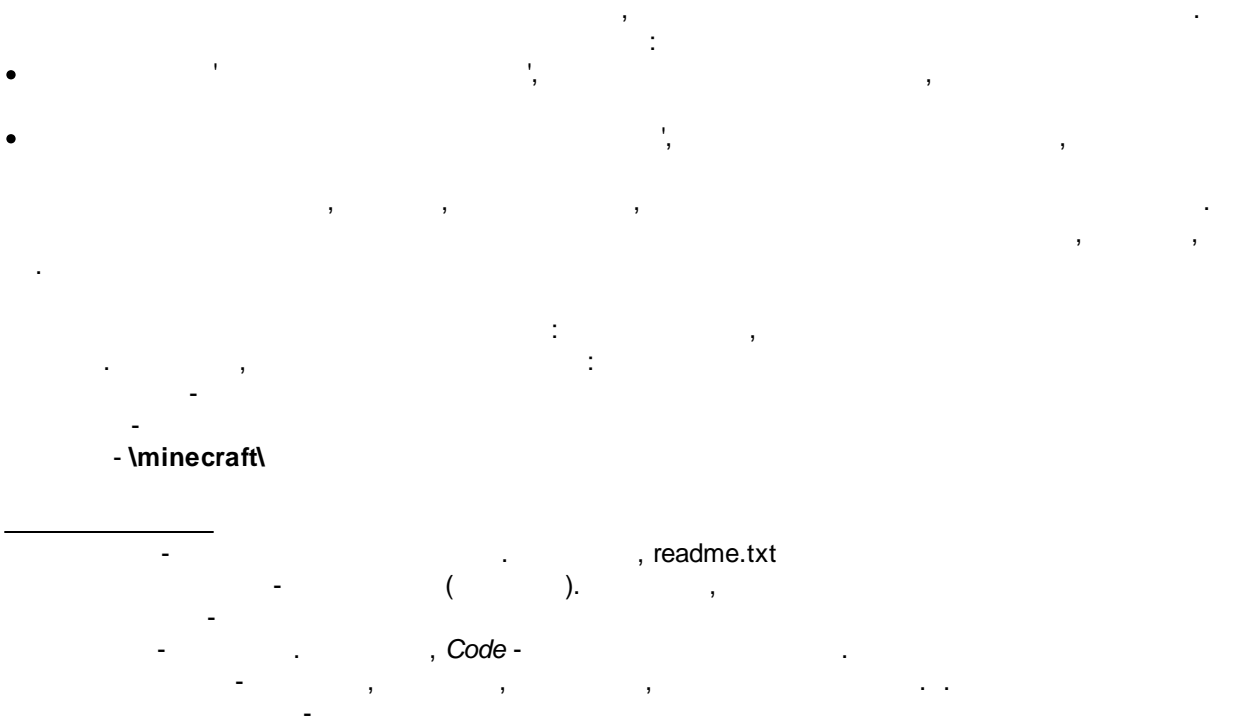
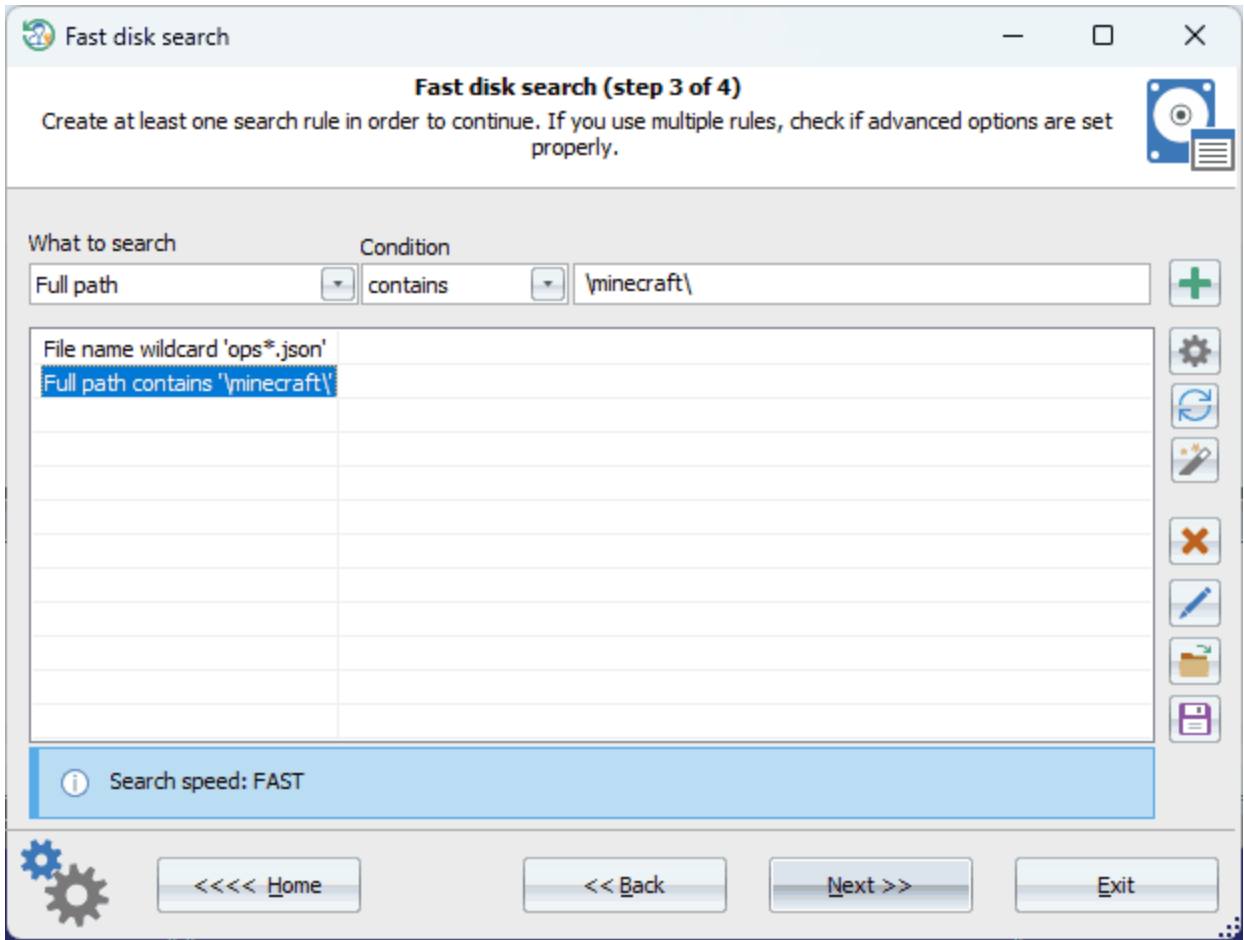
Used space, 26.3%

Free space, 73.7%

Used space: 62.42 GB

Free space: 175.35 GB

Home Back Next Exit

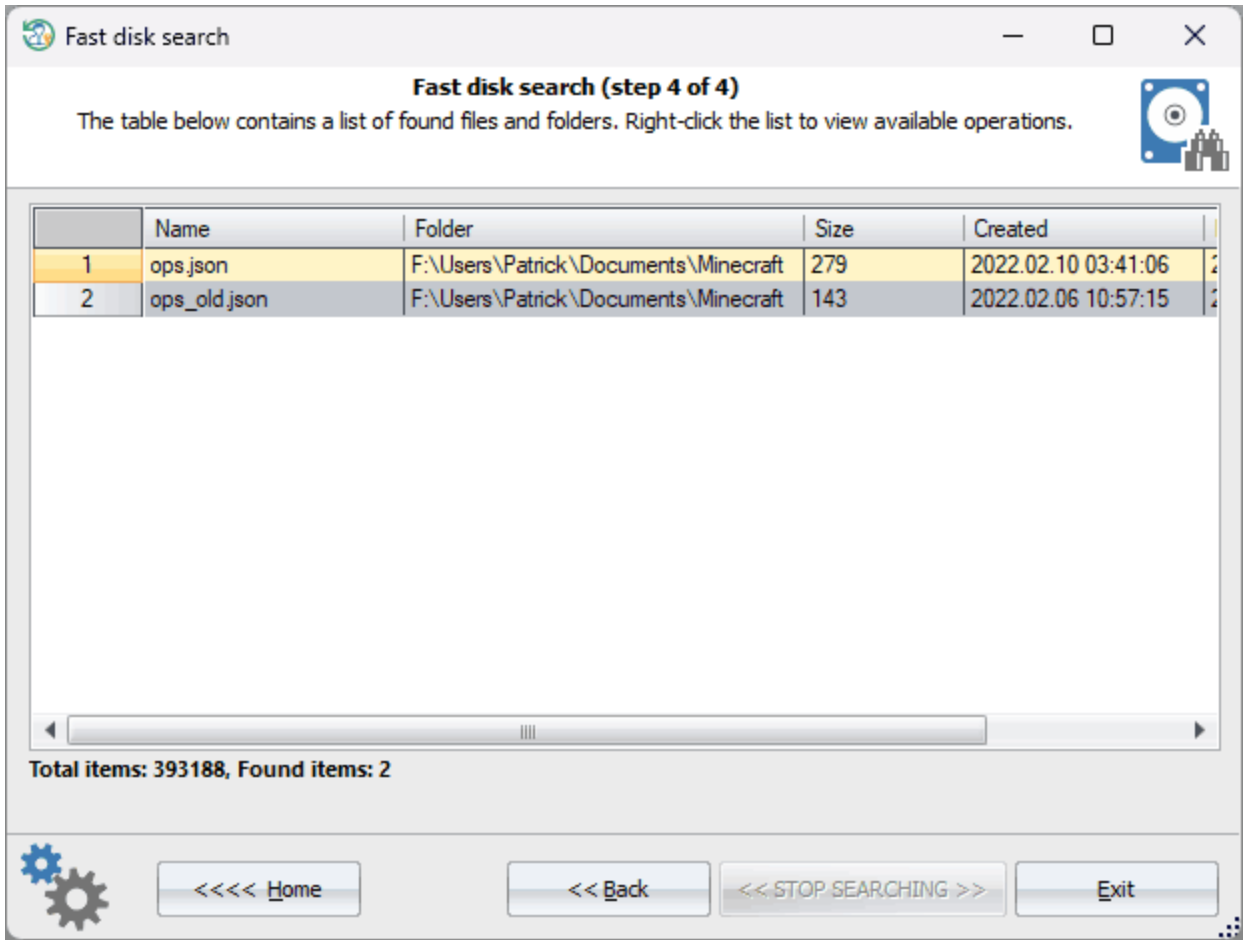


ANSI, UTF8 UTF16

, windows.old

()

-
-
-
-
-
-
-
-



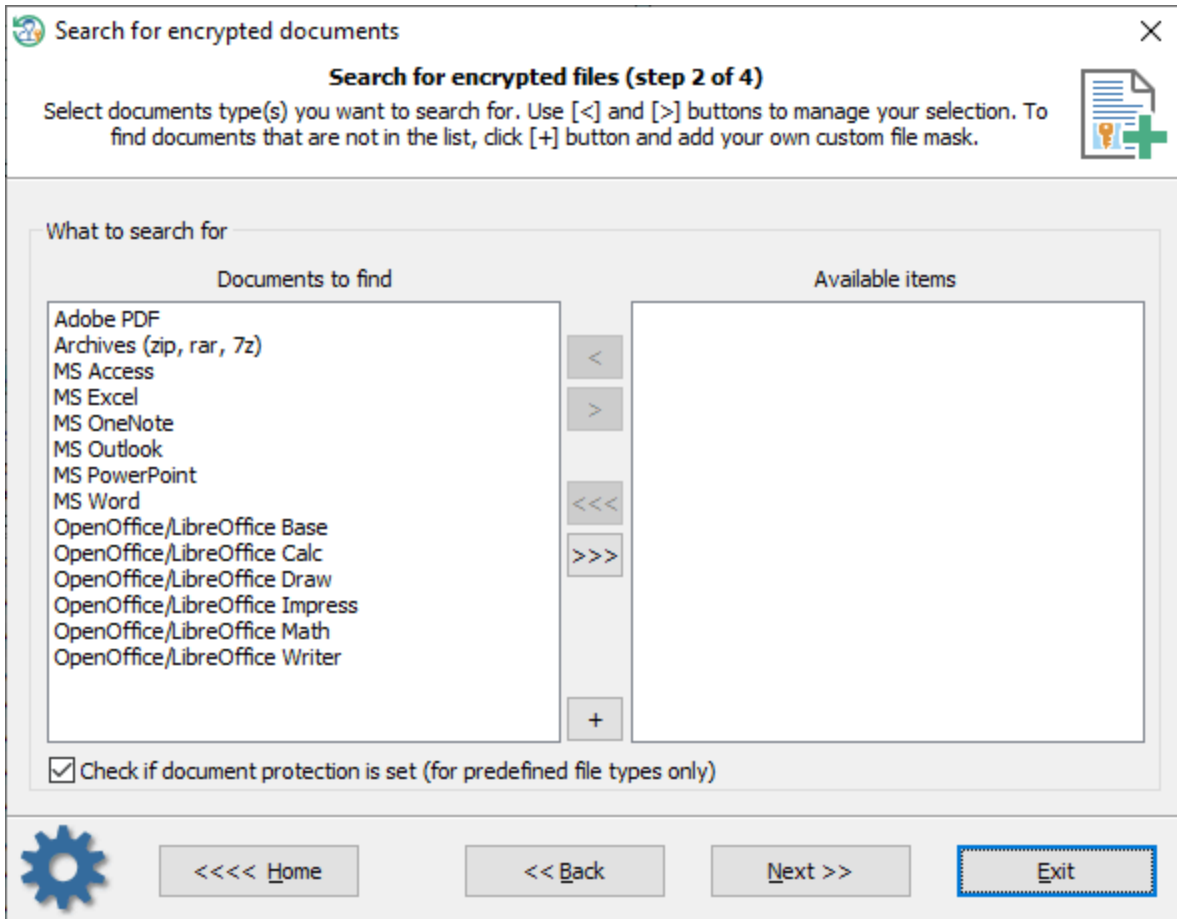
HTML

ZIP

3.9

3.9.1

1



- (zip, rar, 7z)
- Adobe PDF
- MS Word
- MS Excel
- MS Access
- MS PowerPoint
- MS OneNote
- MS Outlook
- OpenOffice/LibreOffice Writer
- OpenOffice/LibreOffice Calc
- OpenOffice/LibreOffice Base
- OpenOffice/LibreOffice Impress
- OpenOffice/LibreOffice Draw
- OpenOffice/LibreOffice Math

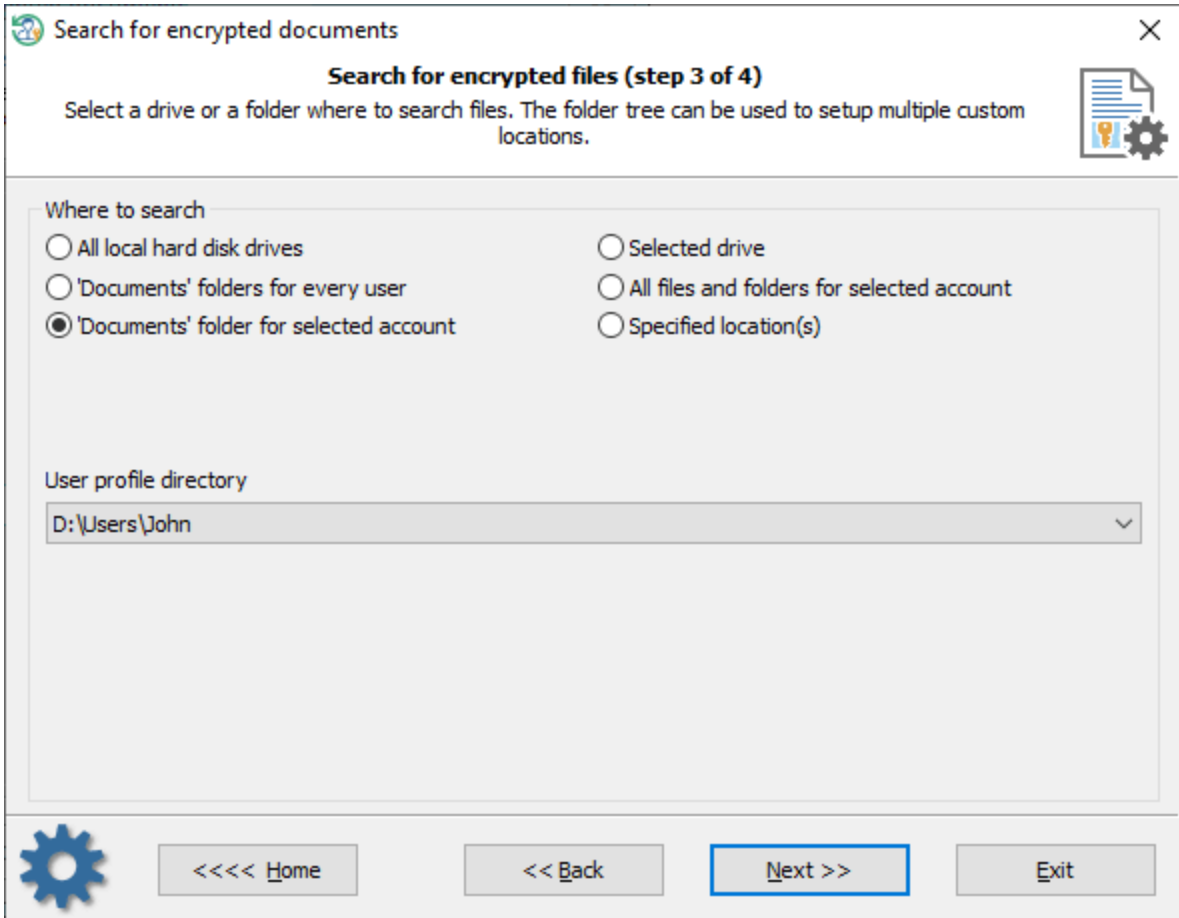
[>] [<]

([+])

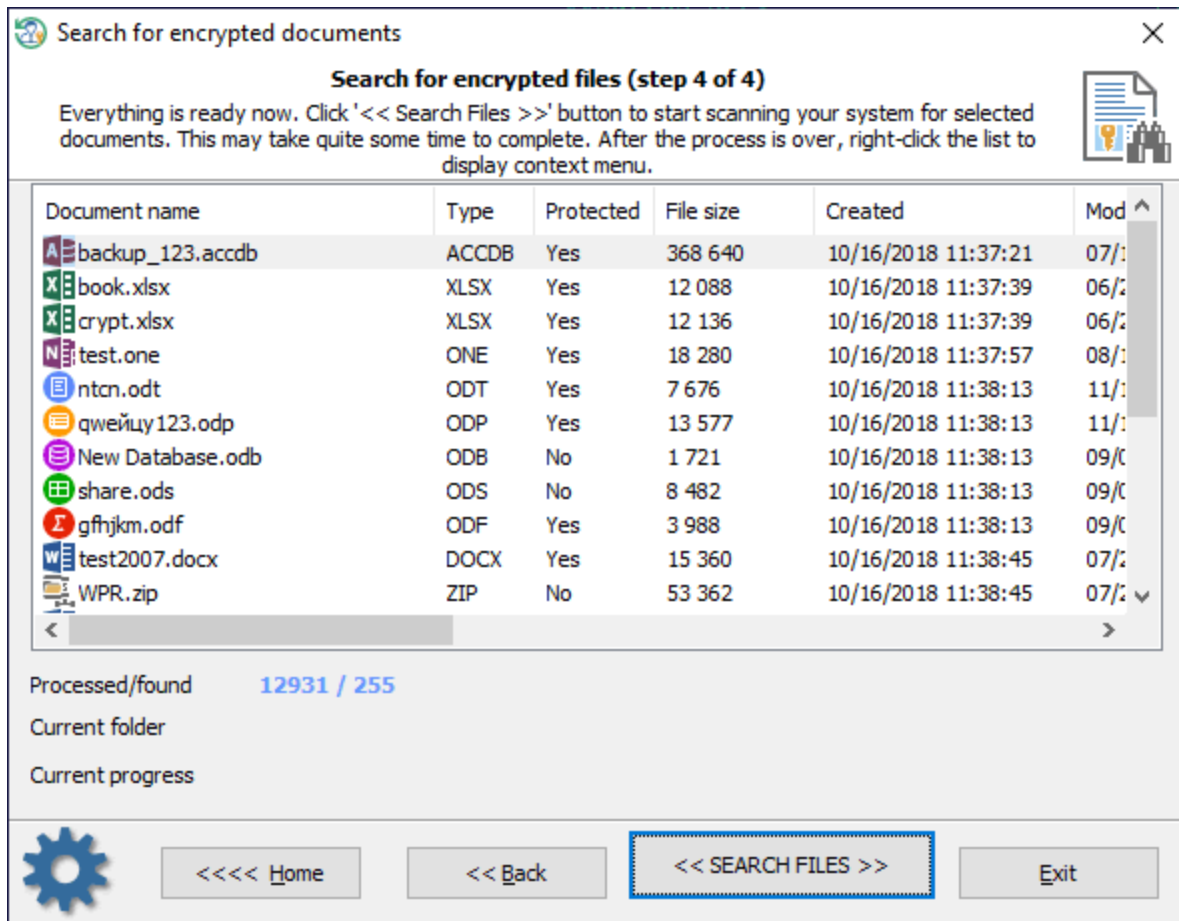
KeePass:

***.kdbx, *.kdb, *.pwd**

2



3



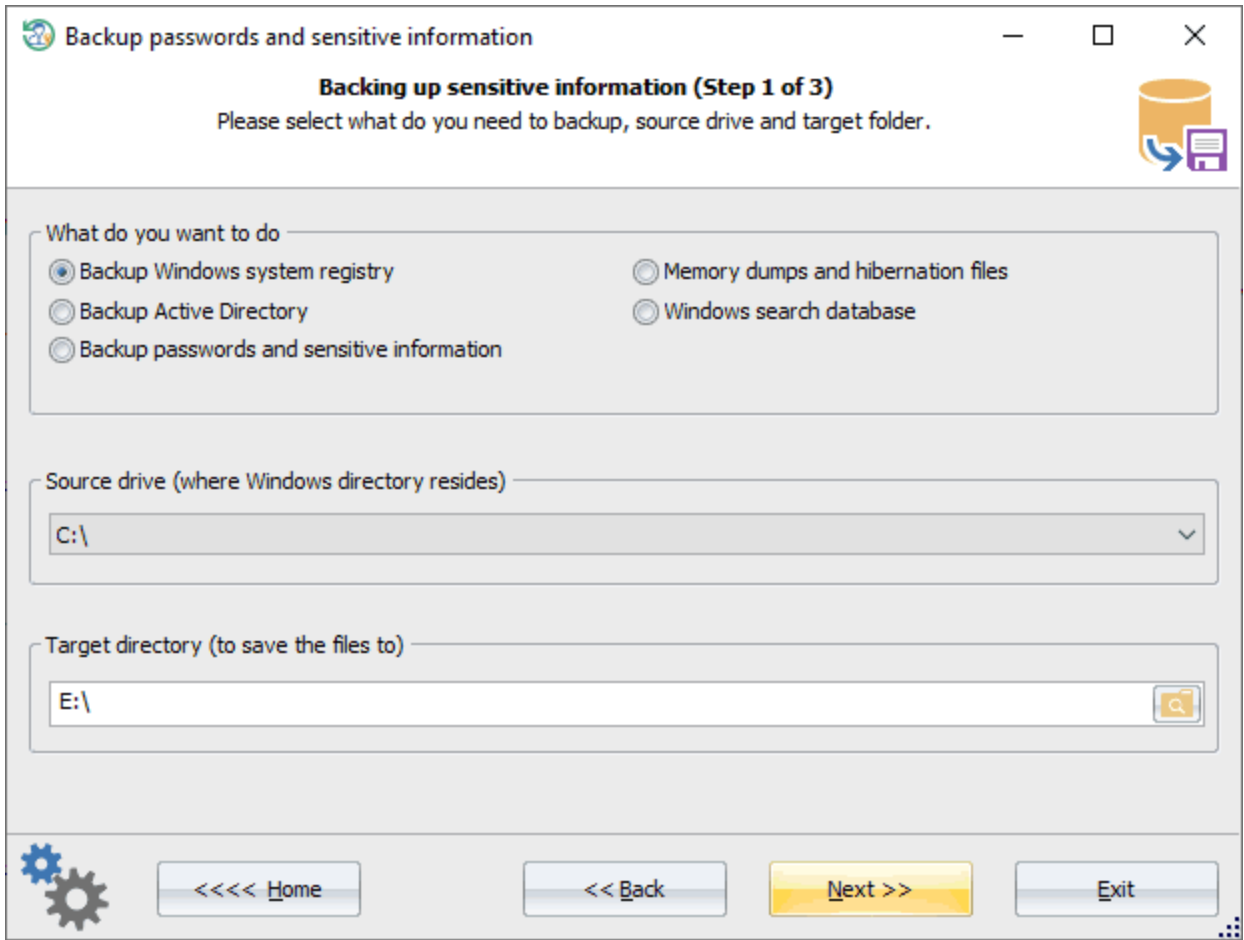
/HTML

3.9.2

Password

Windows

Active Directory. Reset Windows



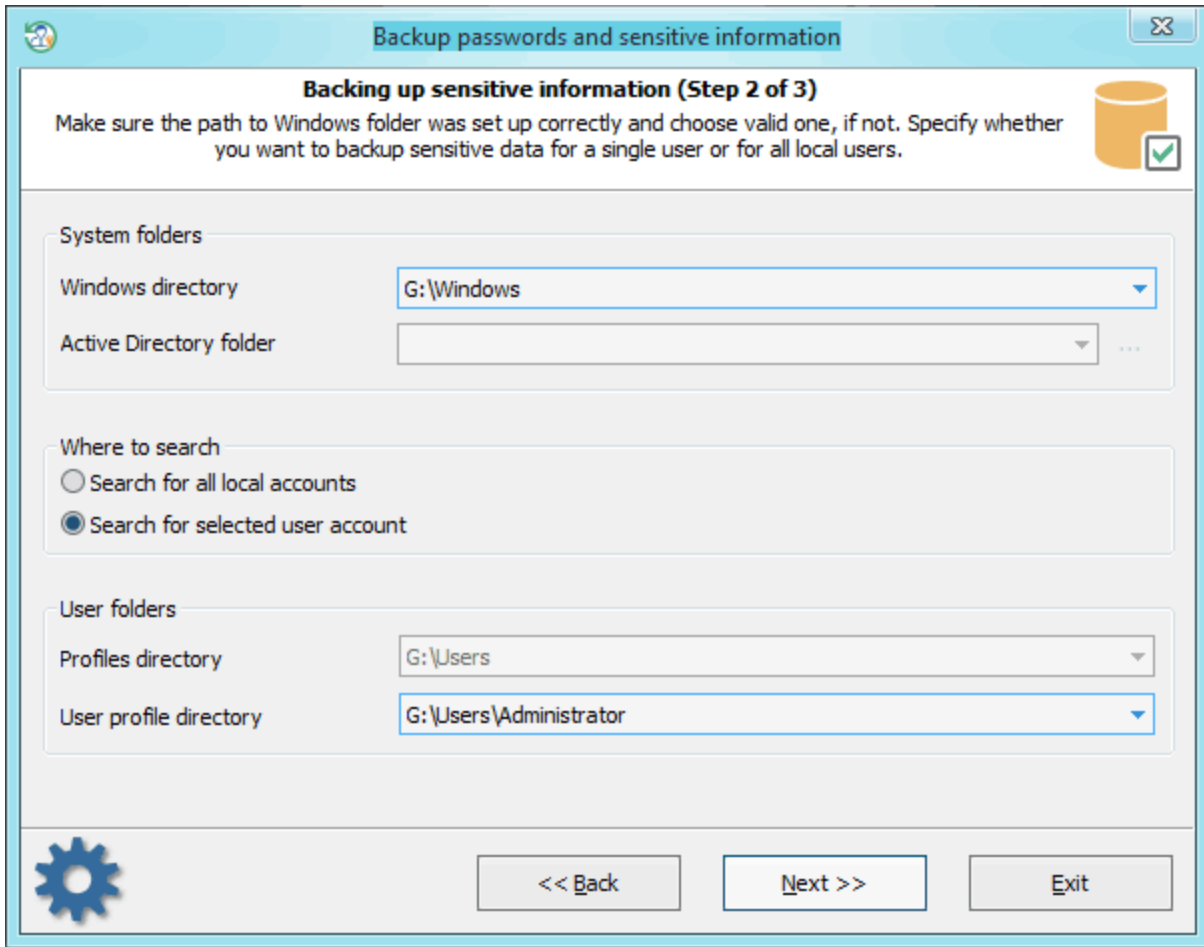
- Windows
- Active Directory
-

- Windows
-

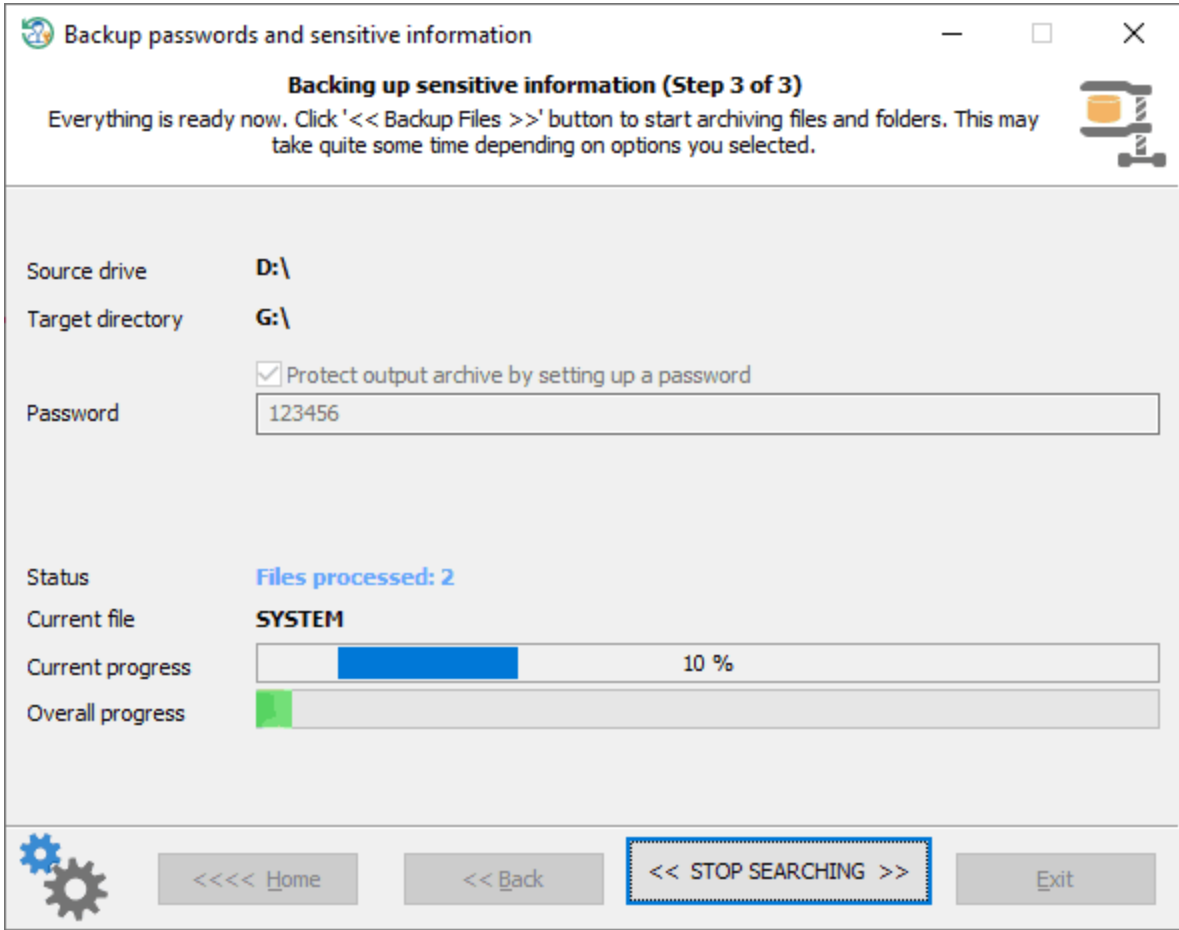
Windows,

(, USB)

Windows



Active Directory,
Windows/NTDS.

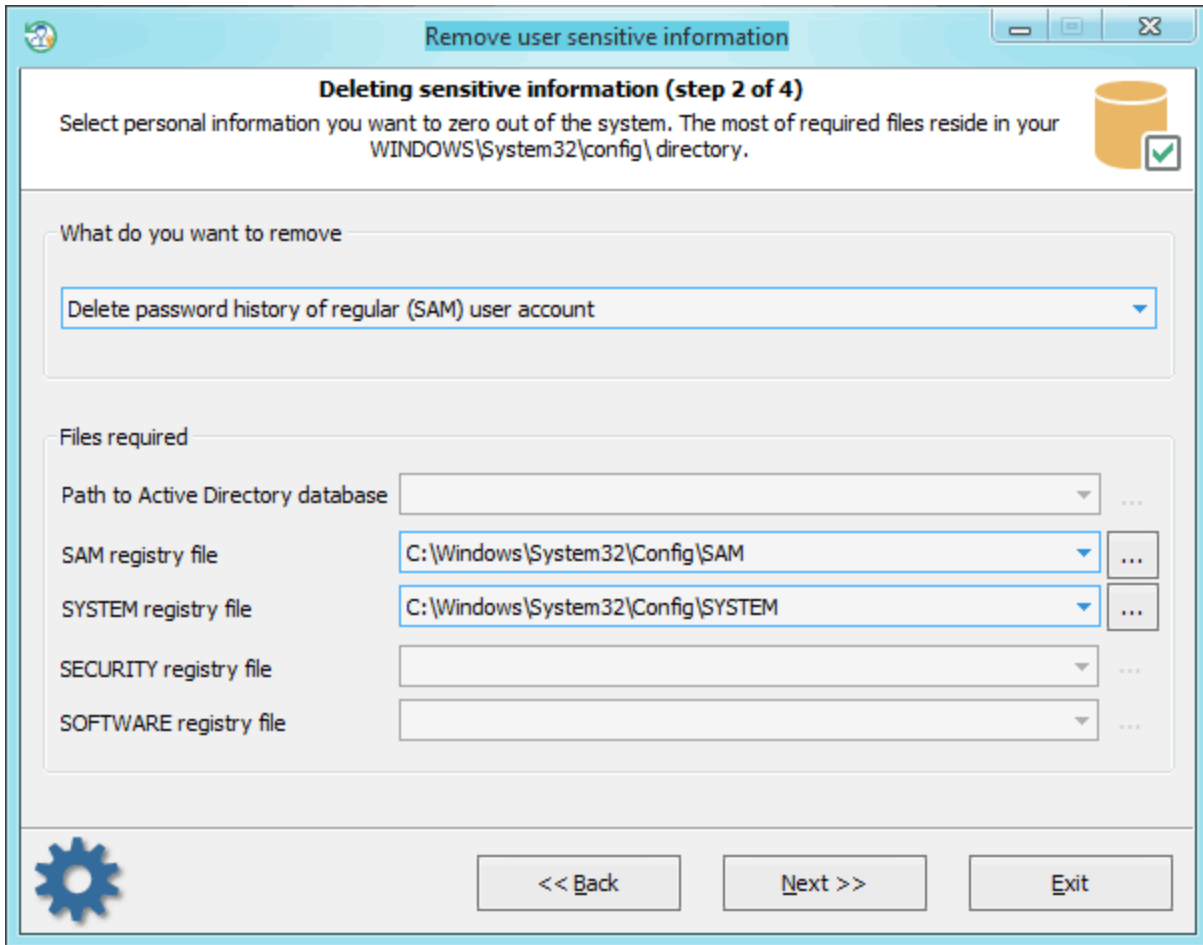


>>
*.ZIP
ZIP

<<

[Windows Password Recovery.](#)

3.9.3

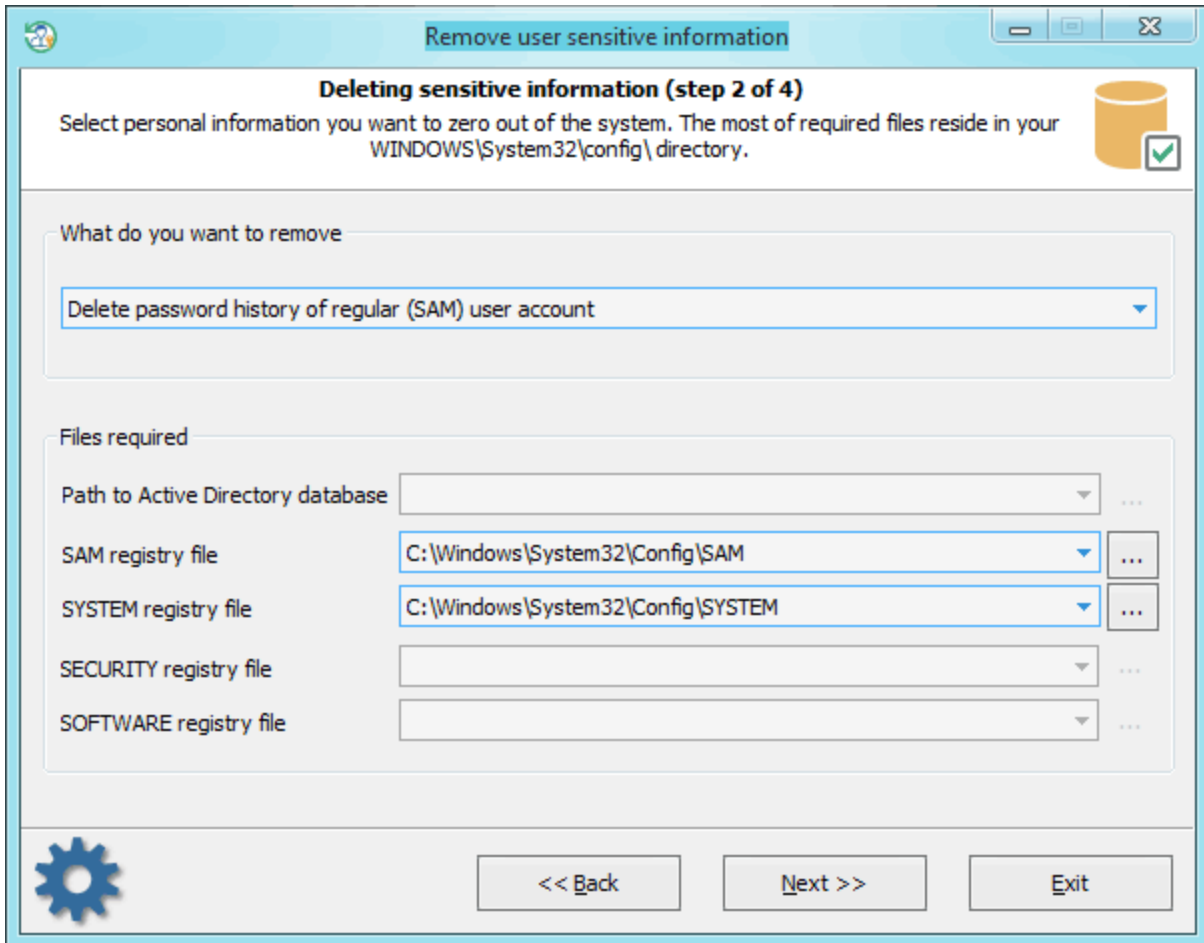


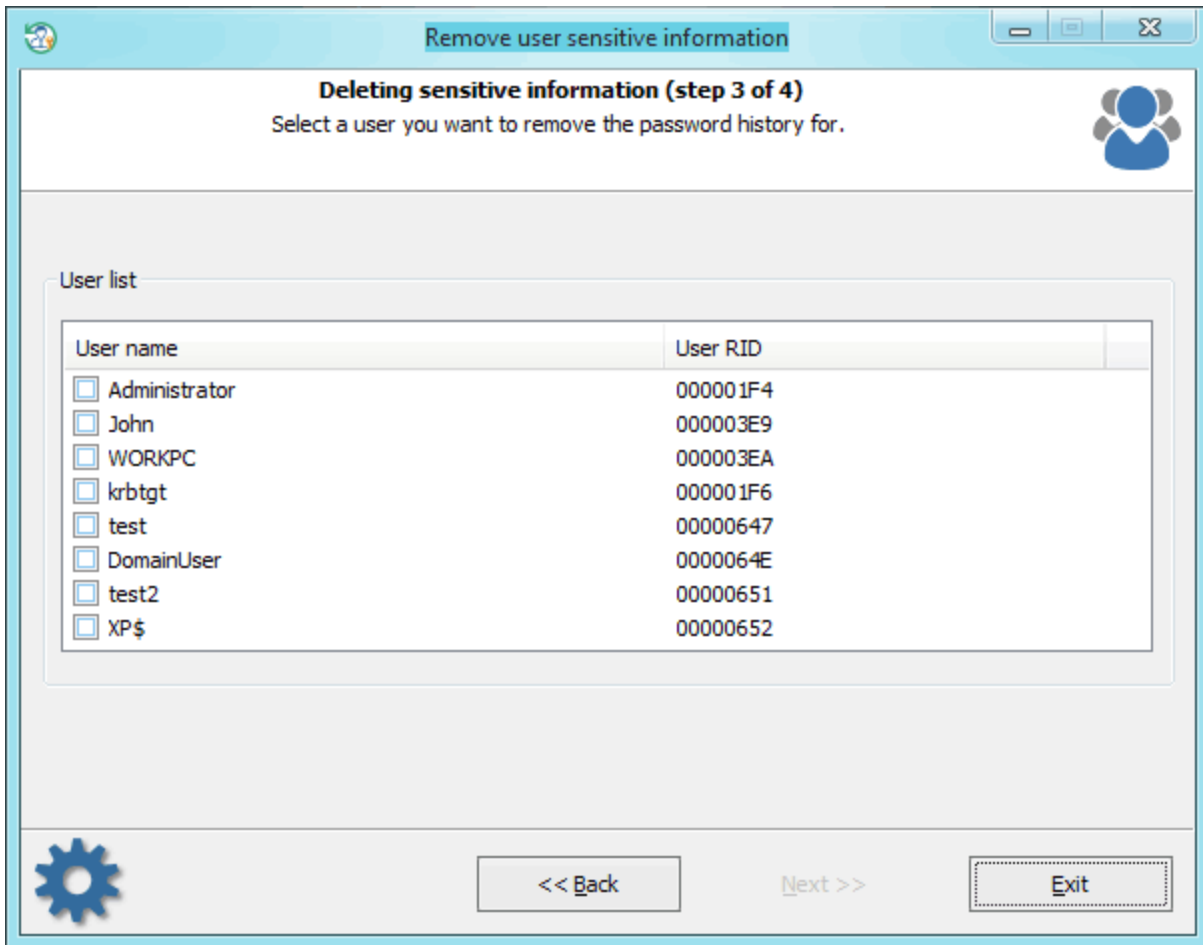
1. Directory. SAM, Active Directory. Start -> Run -> gpedit.msc -> OK. Run () Windows, Win+R. 'Computer Configuration' 'Windows Settings -> Security Settings -> Local Policies -> Security Options'. : Interactive Logon: Number of previous logons to cache.
 2. _____
 3. Windows.
 4. _____
 5. _____
 6. SYSKEY. _____
- _____ Active Directory - (SYSTEM) Active Directory (ntlds.dit);

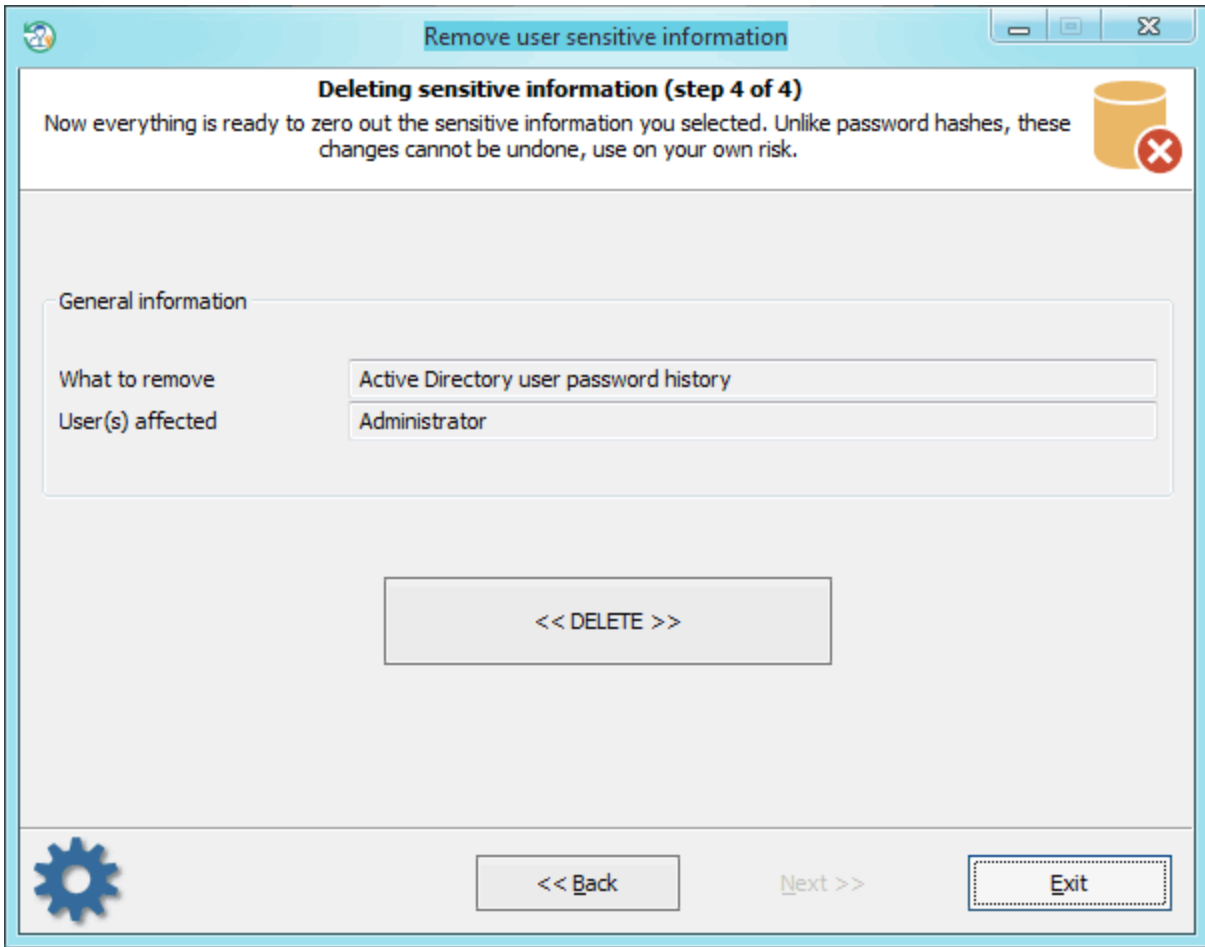
- SAM - SAM SYSTEM
- - SECURITY SYSTEM
- - SECURITY, SOFTWARE SYSTEM
- - SAM, SECURITY SYSTEM
- - SAM, SOFTWARE SYSTEM
- SYSKEY - SAM, SECURITY SYSTEM

Active Directory %WINDIR% Windows, C:\Windows. %WINDIR%\NTDS.
 \system32\config. %WINDIR% - Active Directory , %WINDIR%\NTDS.

3.9.3.1

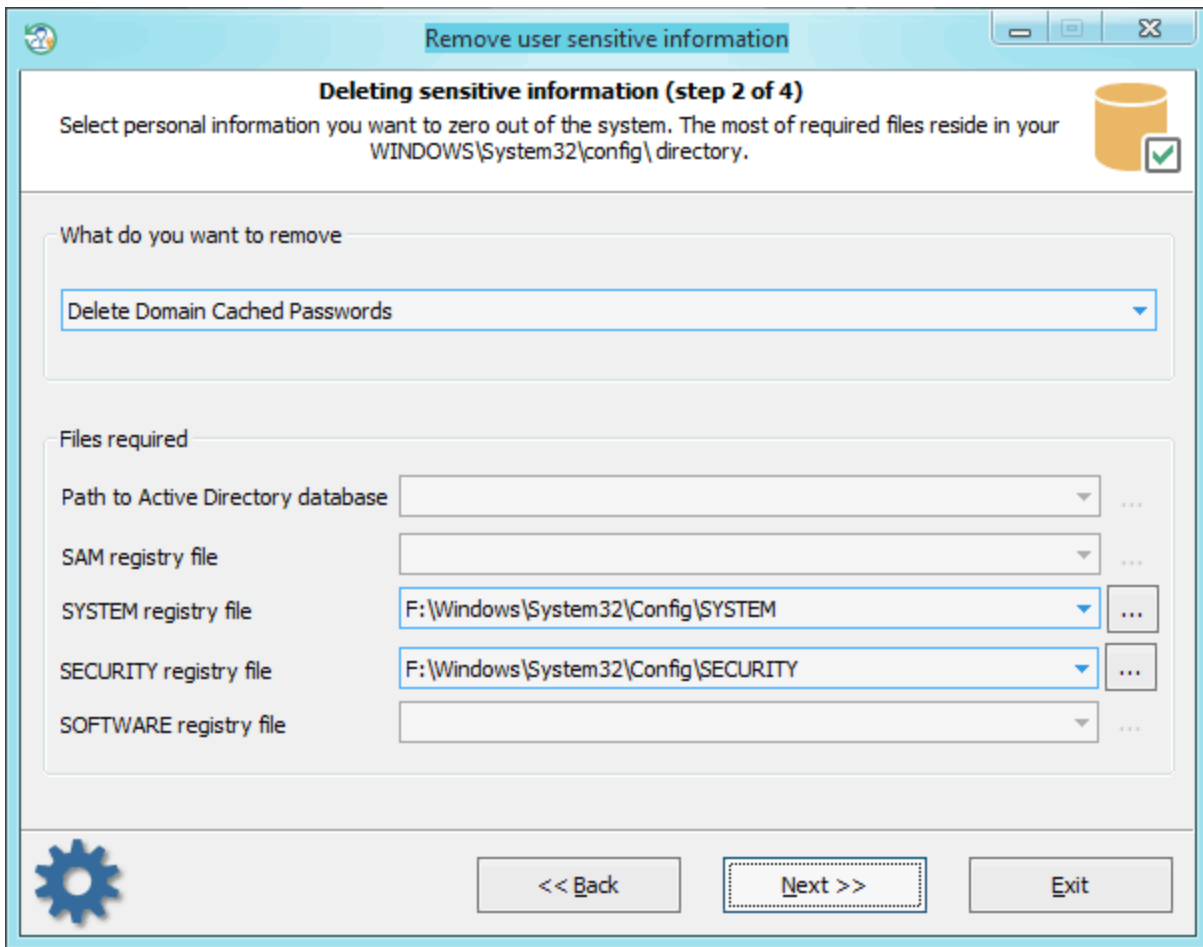


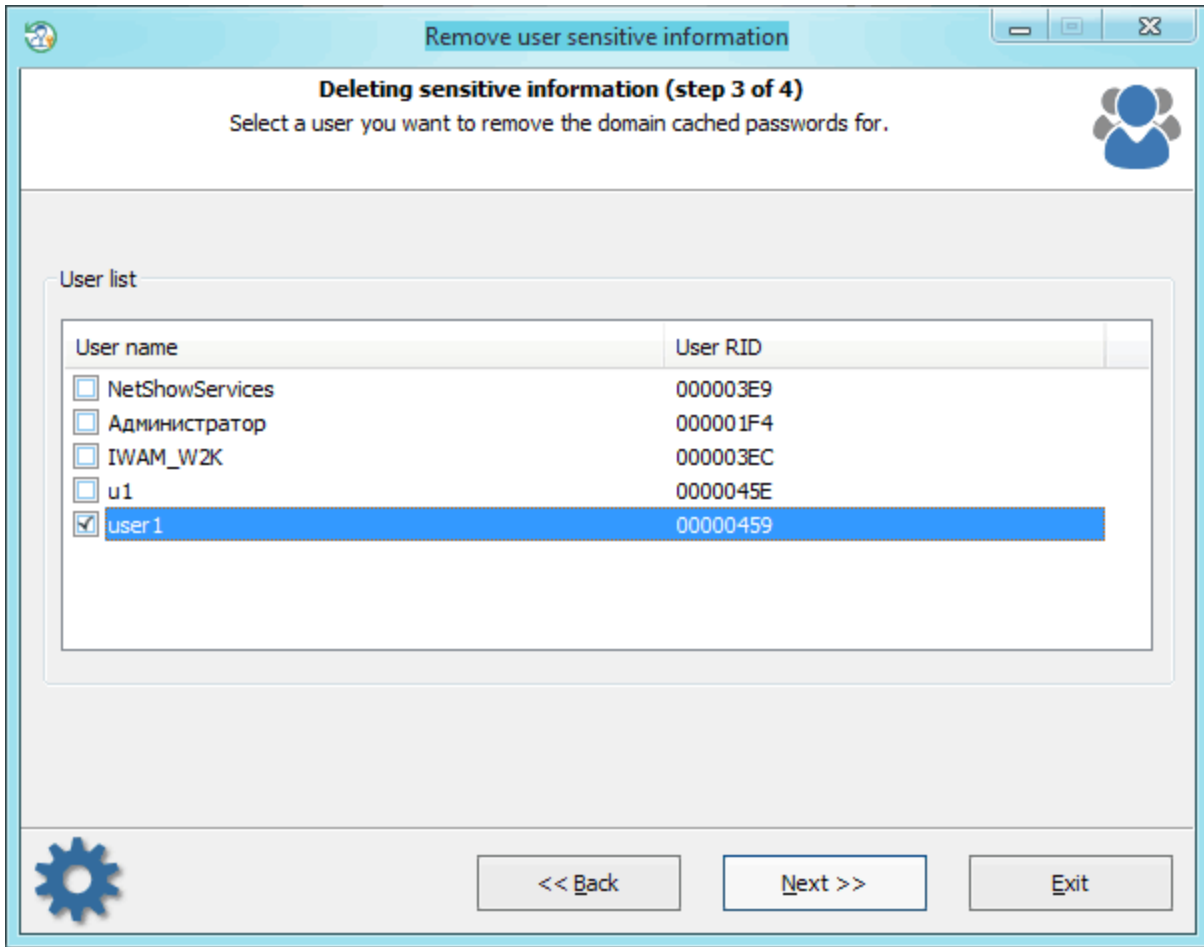


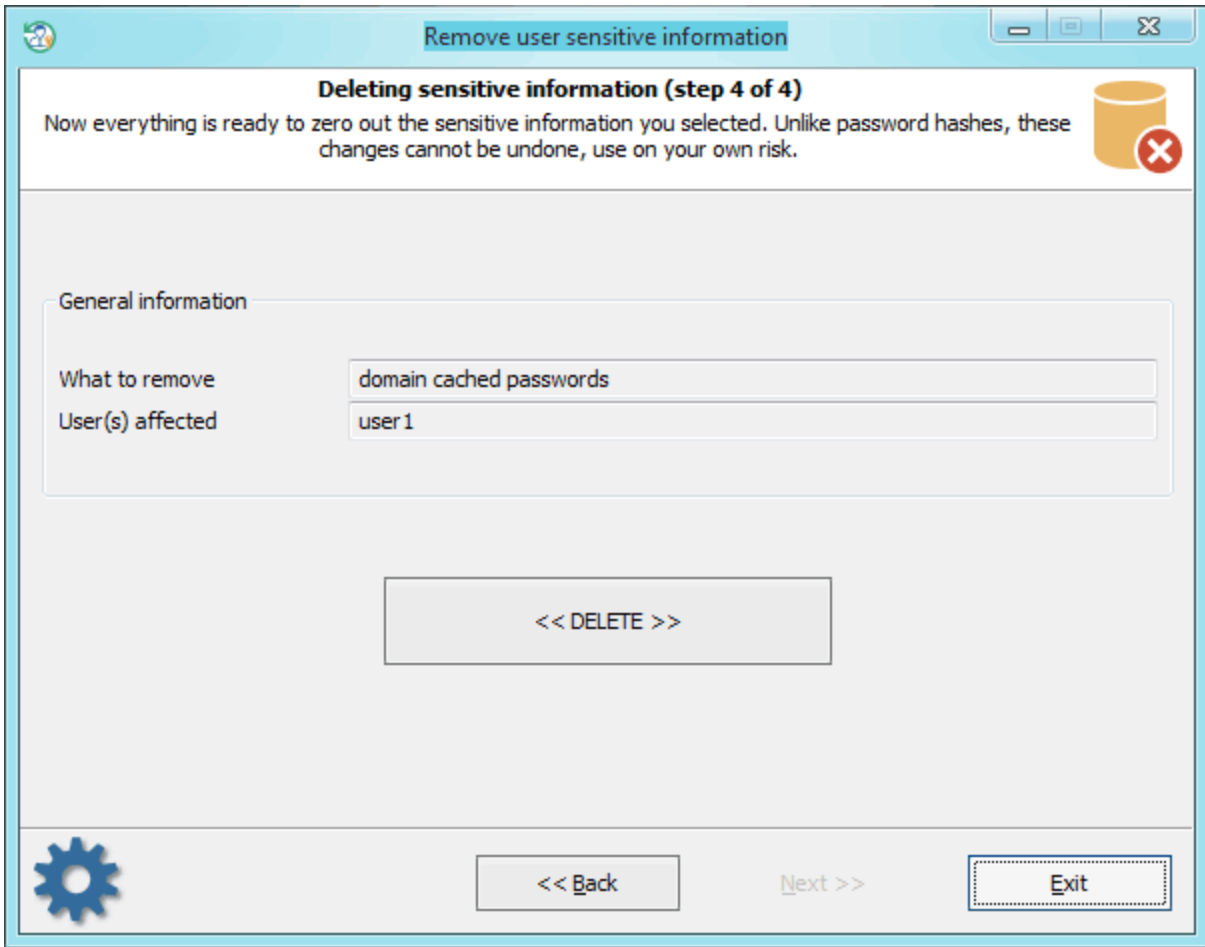


<<Delete>>

3.9.3.2

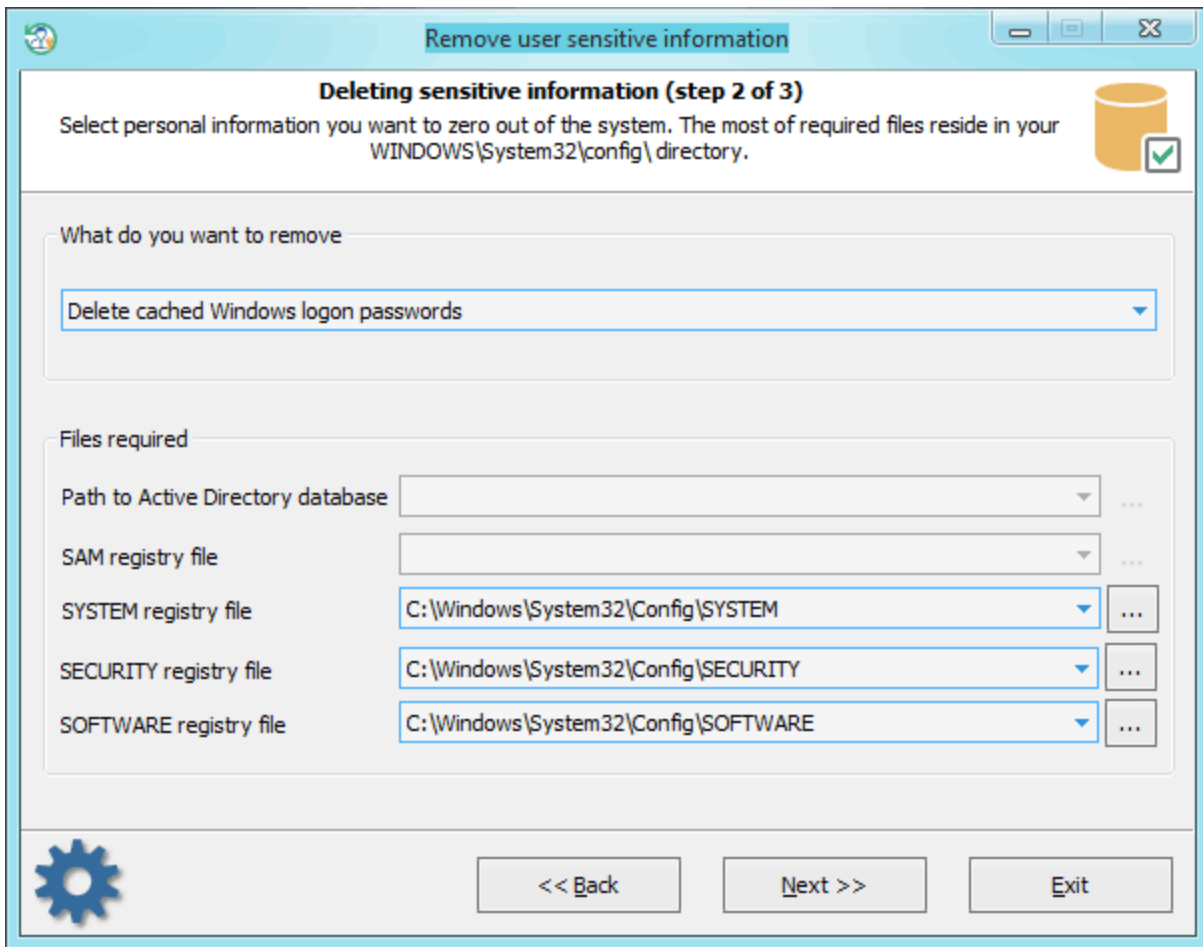




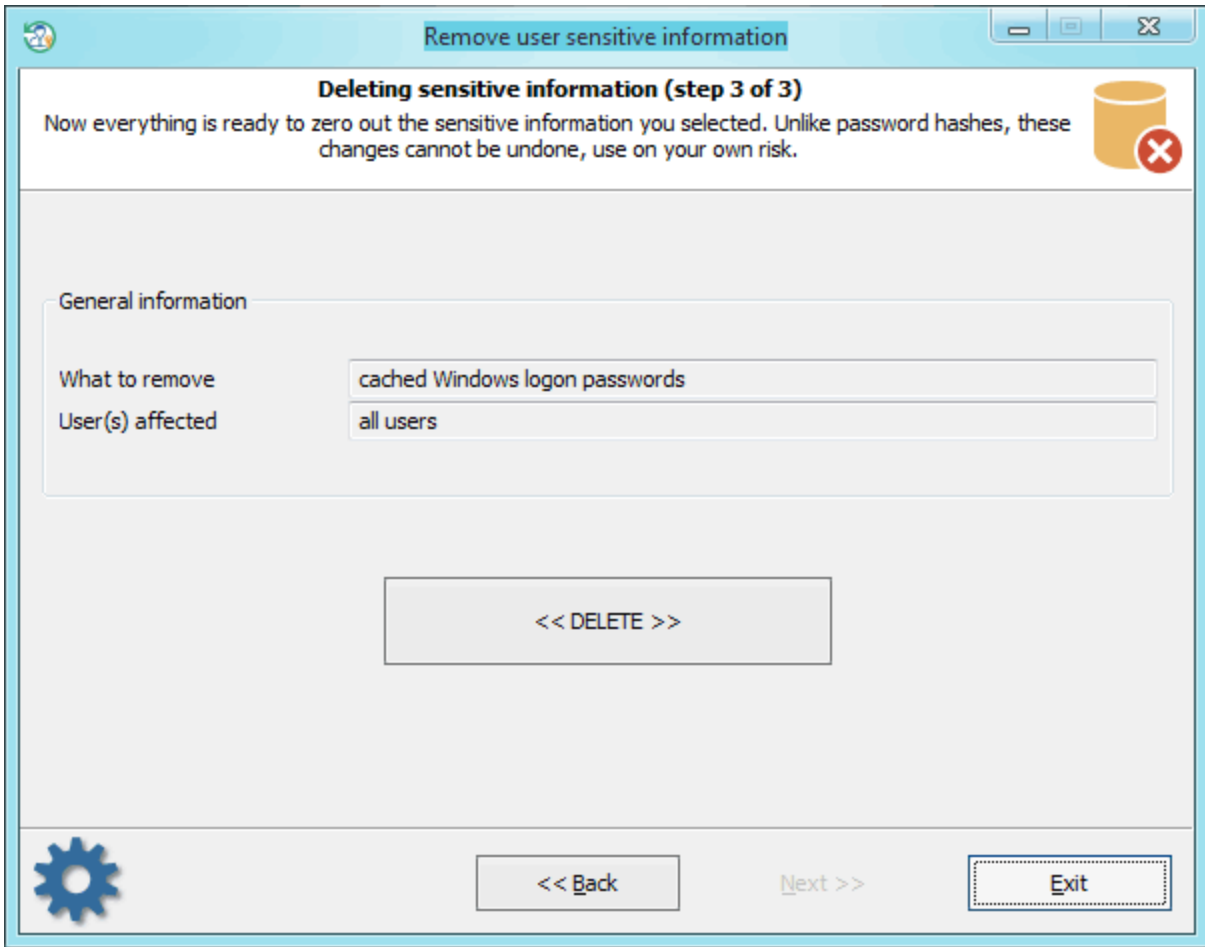


user1.

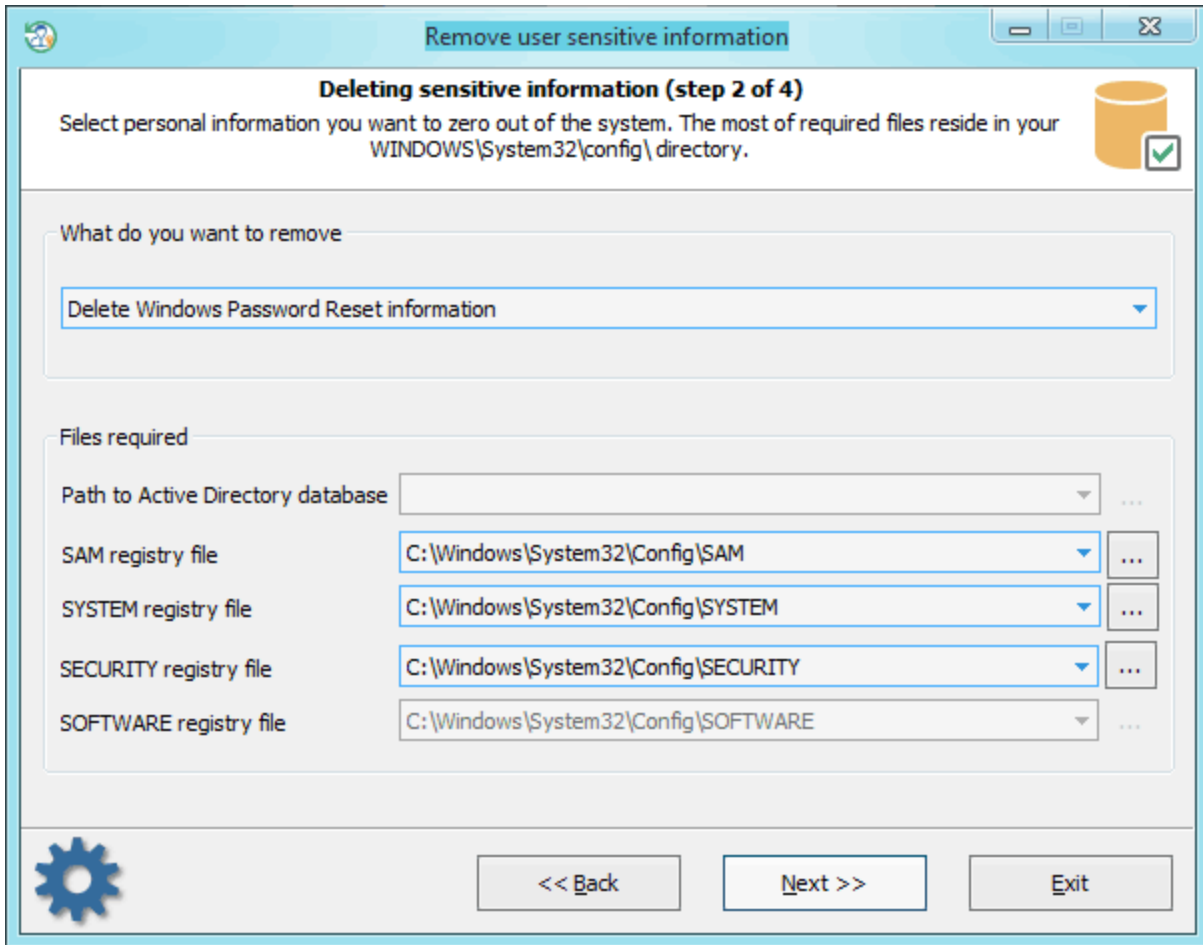
3.9.3.3

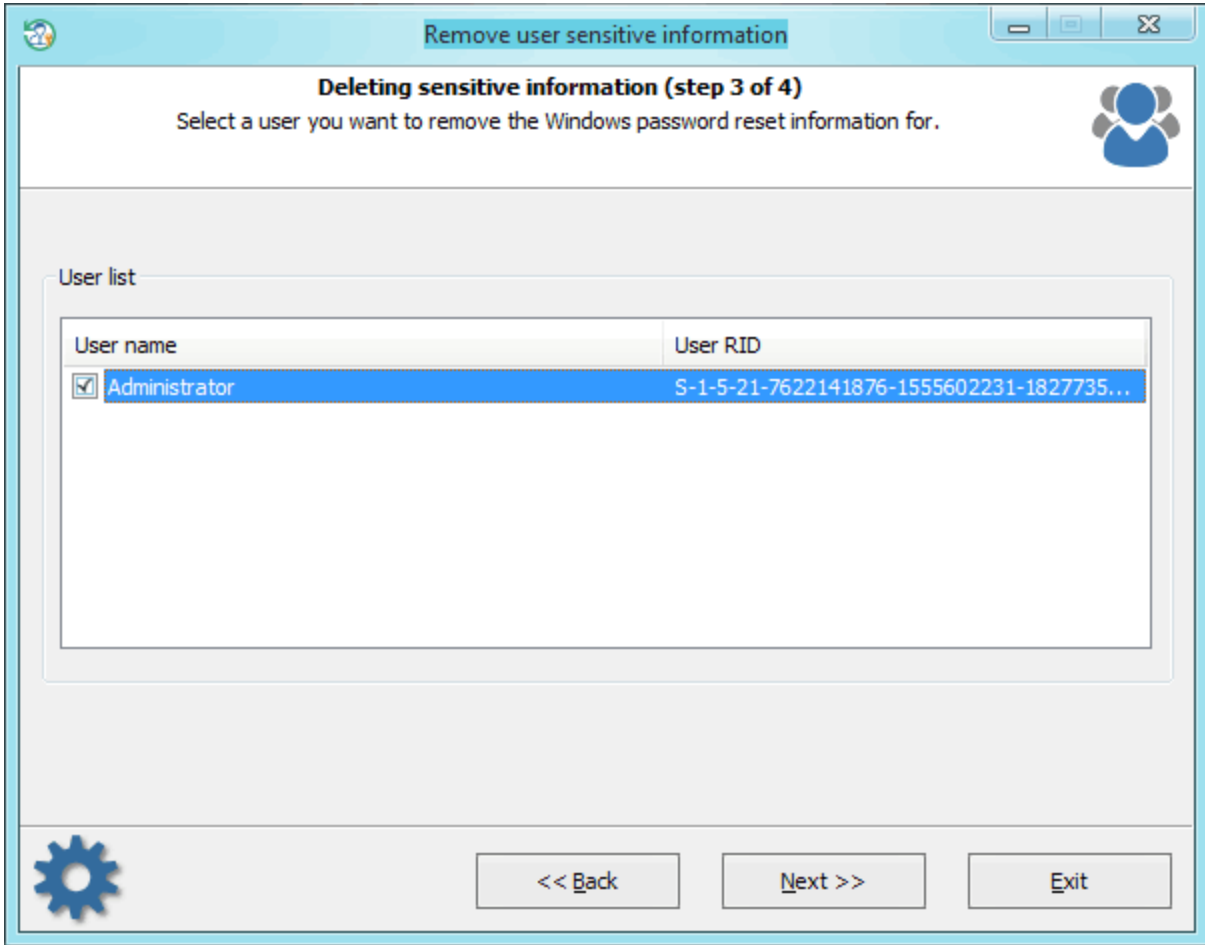


Windows

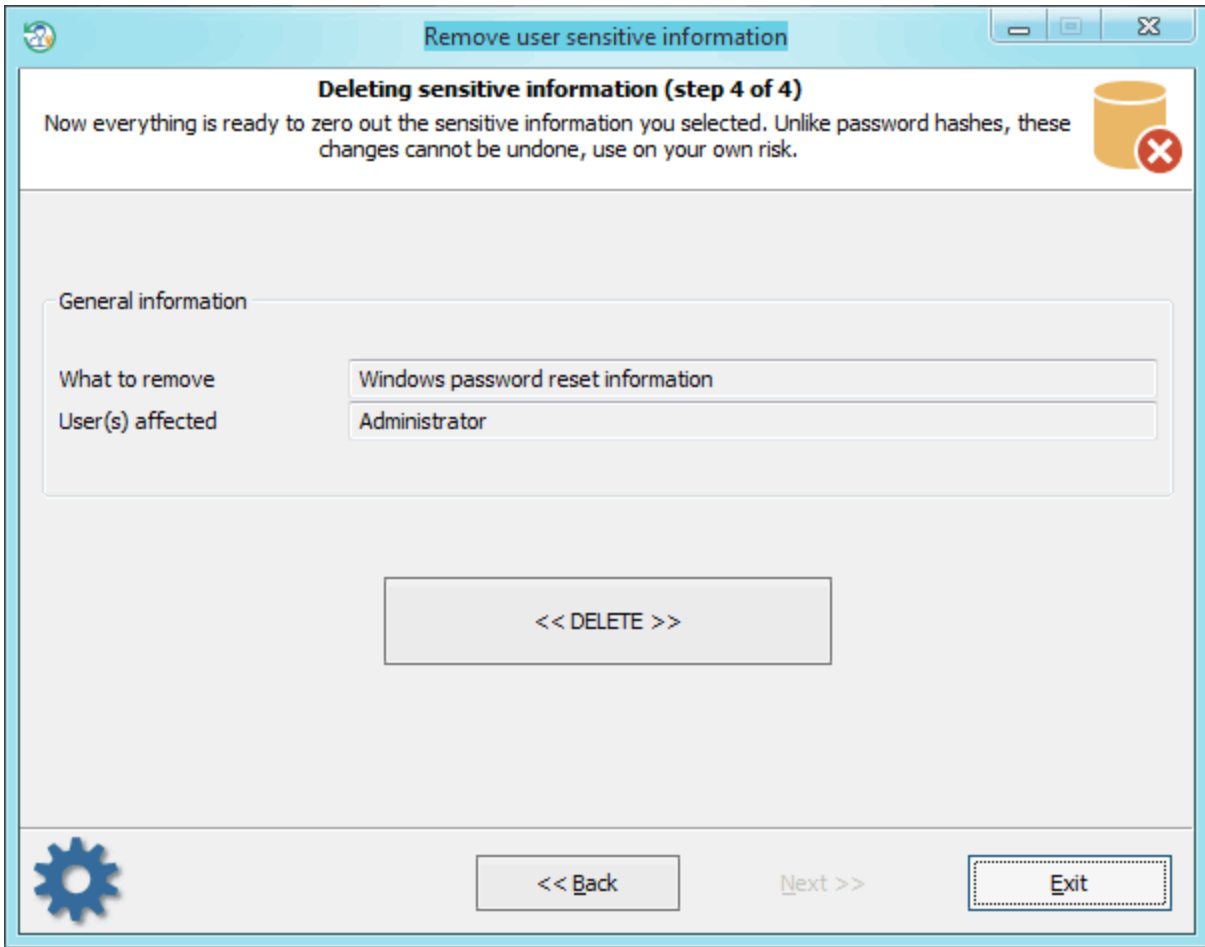


3.9.3.4

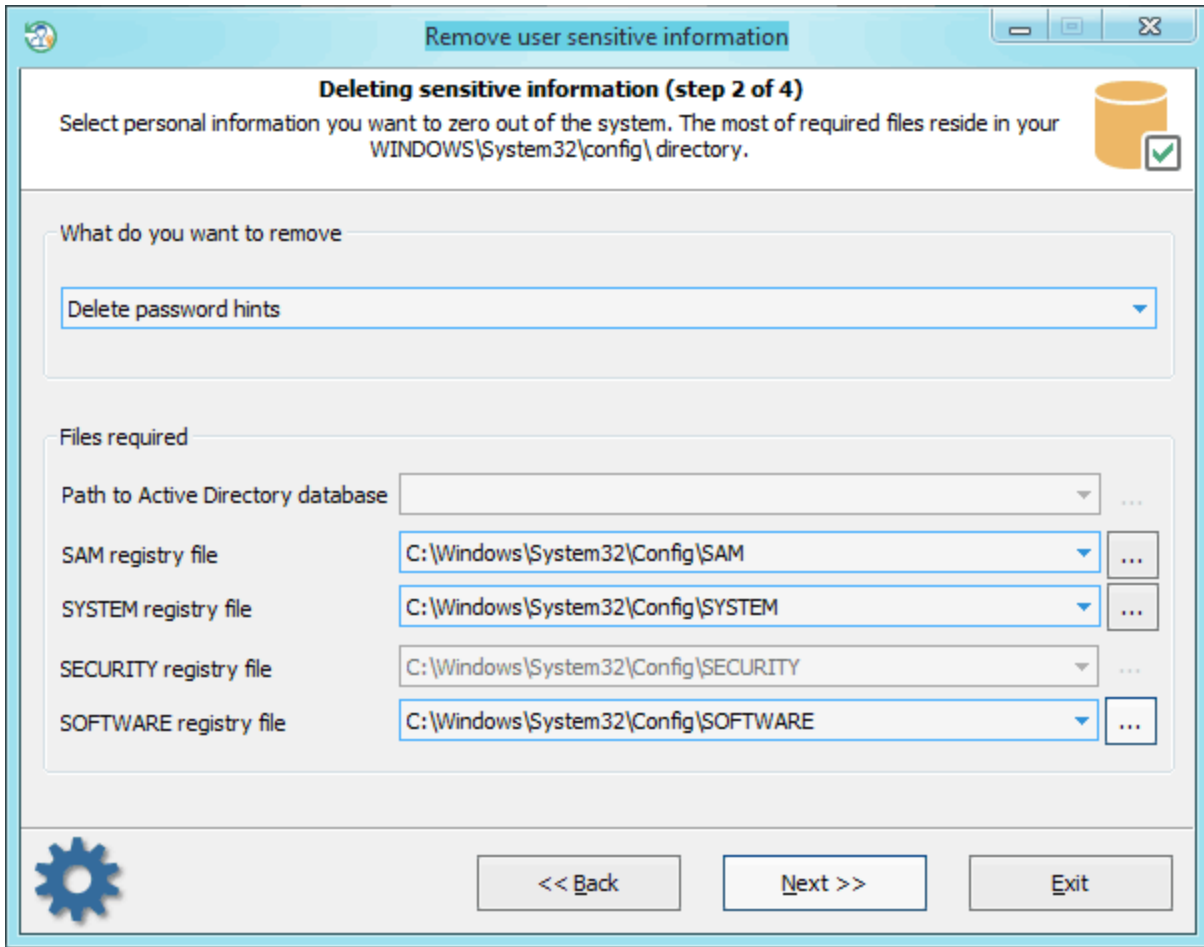




Windows.



3.9.3.5



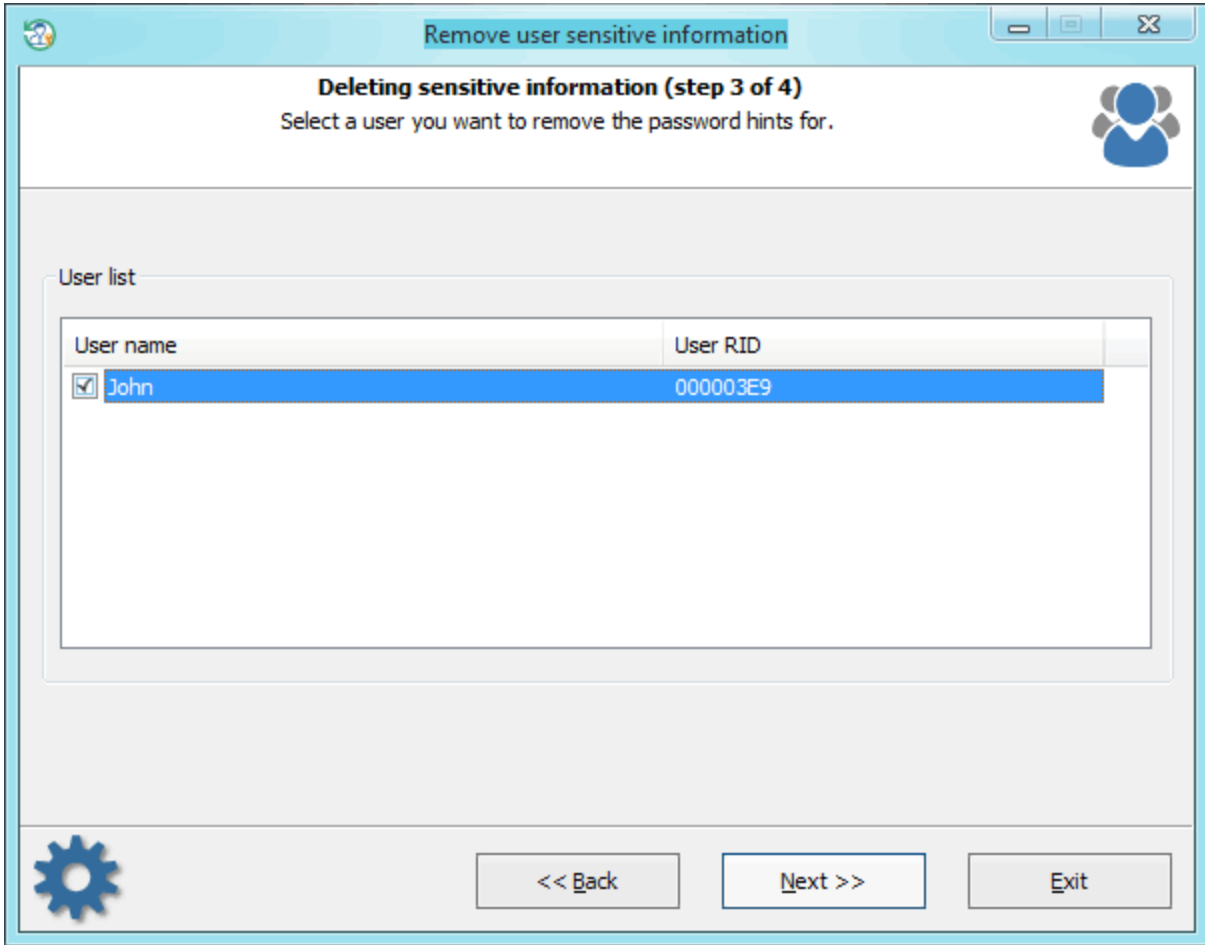
Windows 2003),
SYSTEM.

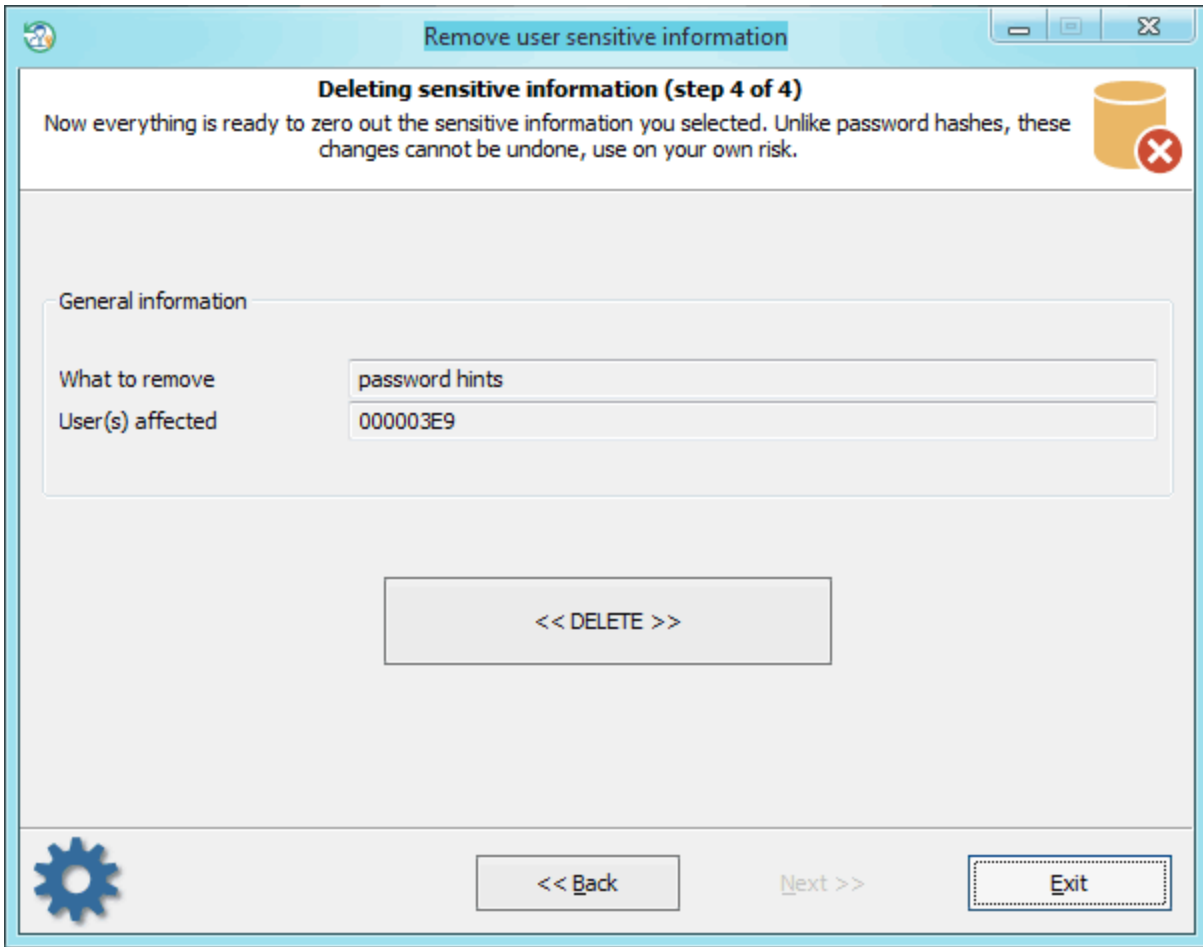
SAM

(Windows Vista

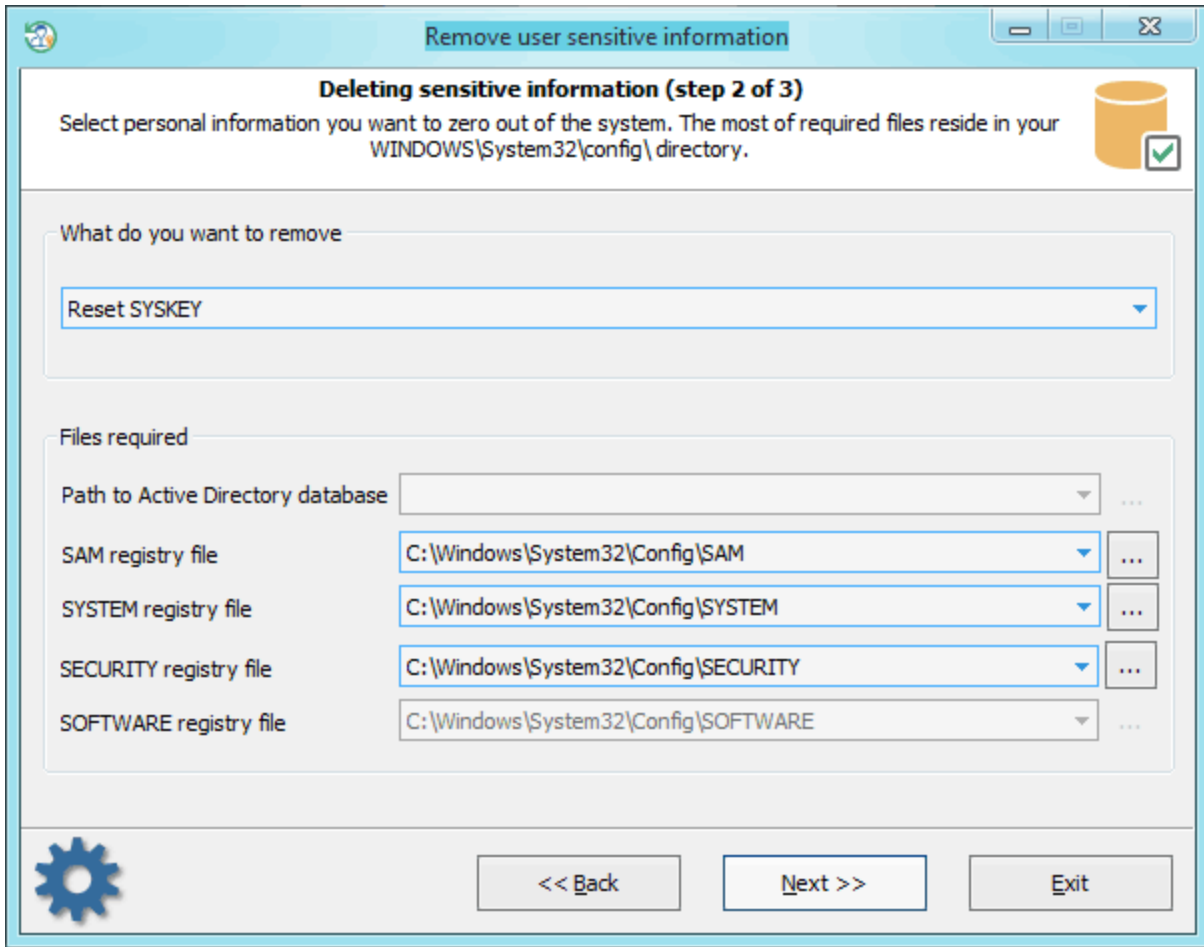
SOFTWARE (
).

Windows XP,



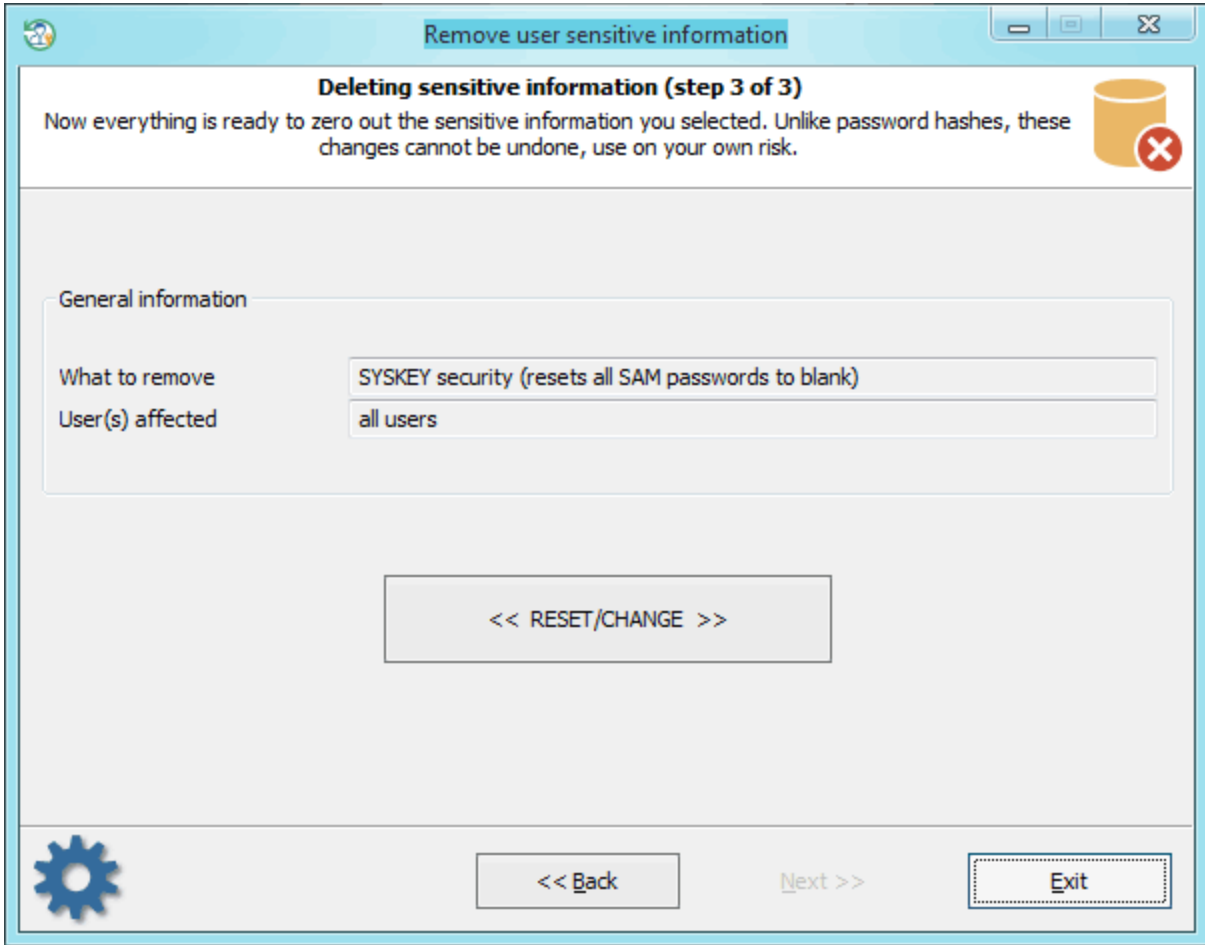


3.9.3.6 SYSKEY



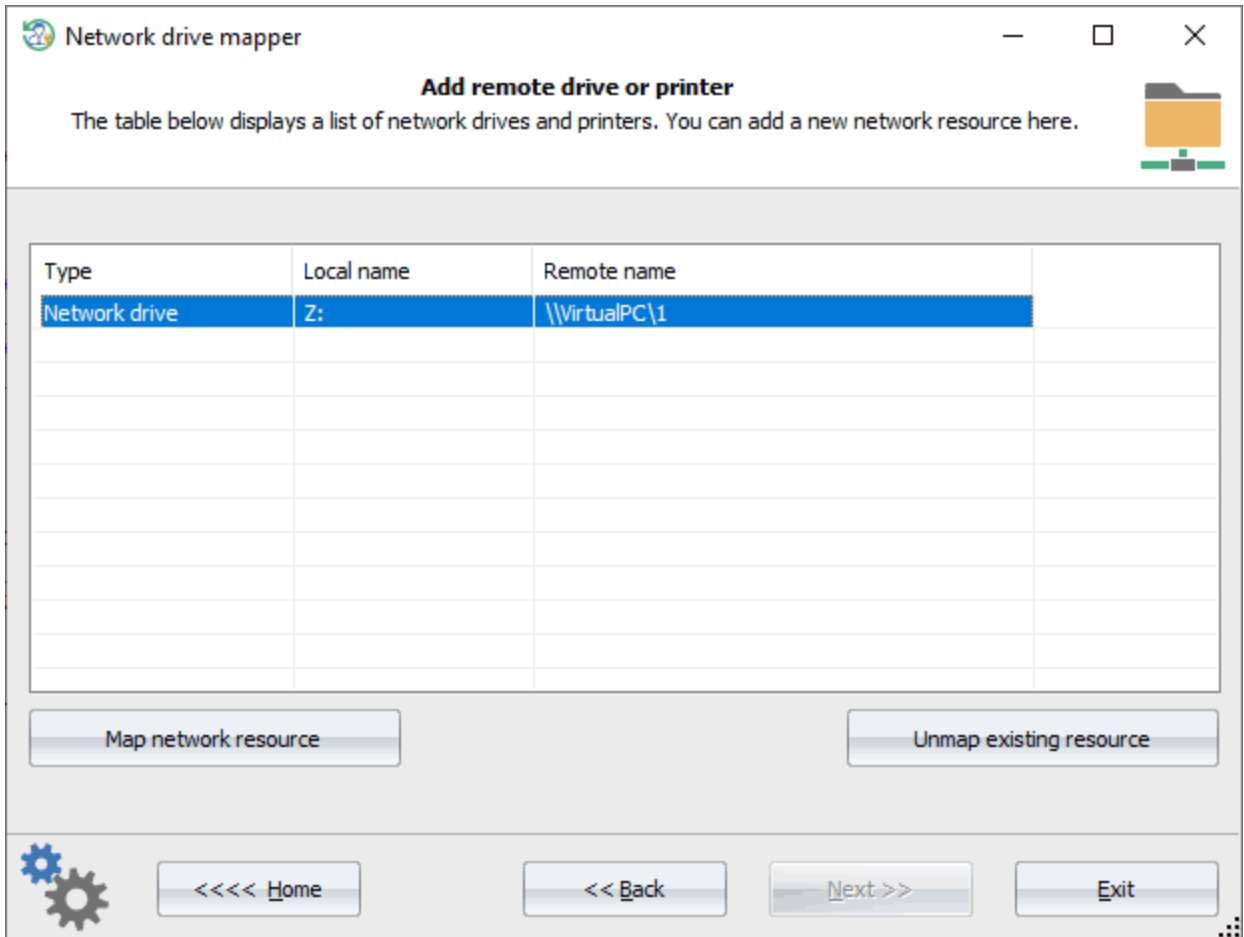
SYSKEY , SYSTEM, SECURITY.
 , , HKLM\CurrentControlSet\Control\Lsa.
 , , - SYSKEY
 , , SYSKEY
 (!)
 Windows.

SYSKEY




! SYSKEY
SYSKEY,
EFS, DPAPI,
SYSKEY,
SYSKEY,
SAM,
LSA . Reset Windows Password 2
SYSKEY.
SYSKEY
! SYSKEY Windows 8,
()
LiveID.

3.9.4



'Map Network resource'.
 \\SERVER\SHARE,
 IP
 SERVER -
 SHARE -
 \\WIN-C2KSHD76D\forall
 \\VPC1
 \\COMP2\C\$

Add remote drive or printer ✕


Fill in all required fields and click OK to add the remote resource 

Network resource type:

Local name, eg. Z: or LPT1:

Remote name, eg. \\Server\share:

Remote user name:

User password: 

3.9.5

ESE (Extensible Storage Engine)

Extensible Storage Engine (

Jet Blue

Microsoft) -

Microsoft
Active Directory,

SQL.
Microsoft Exchange, Windows Search,

Windows,

Windows.

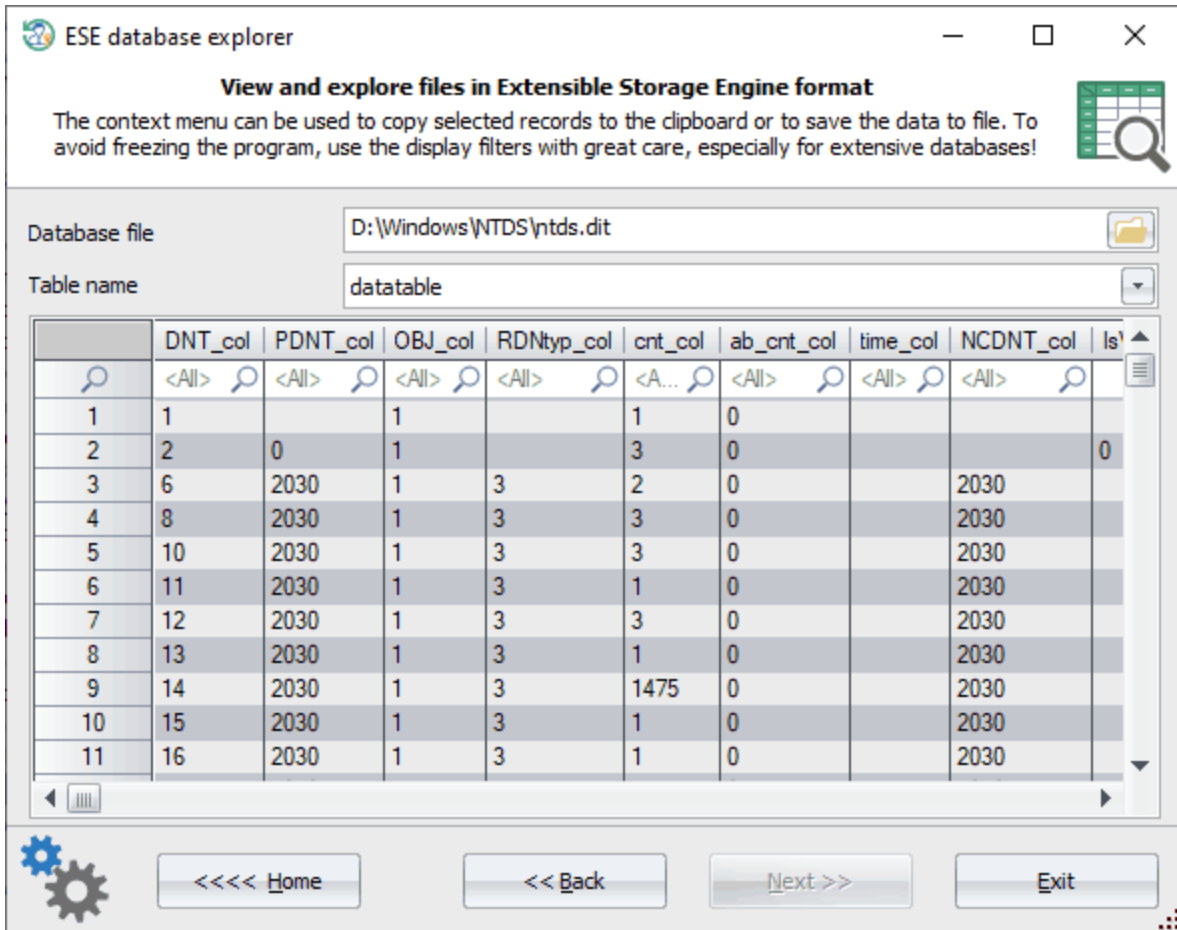
ESE

ESE
Microsoft

(, ESEDatabaseView

NirSoft), RWP
Microsoft ()
ESE

ESE
:
API).



CSV-

ESE
Windows Search
ESE
%SYSTEMDRIVE%\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

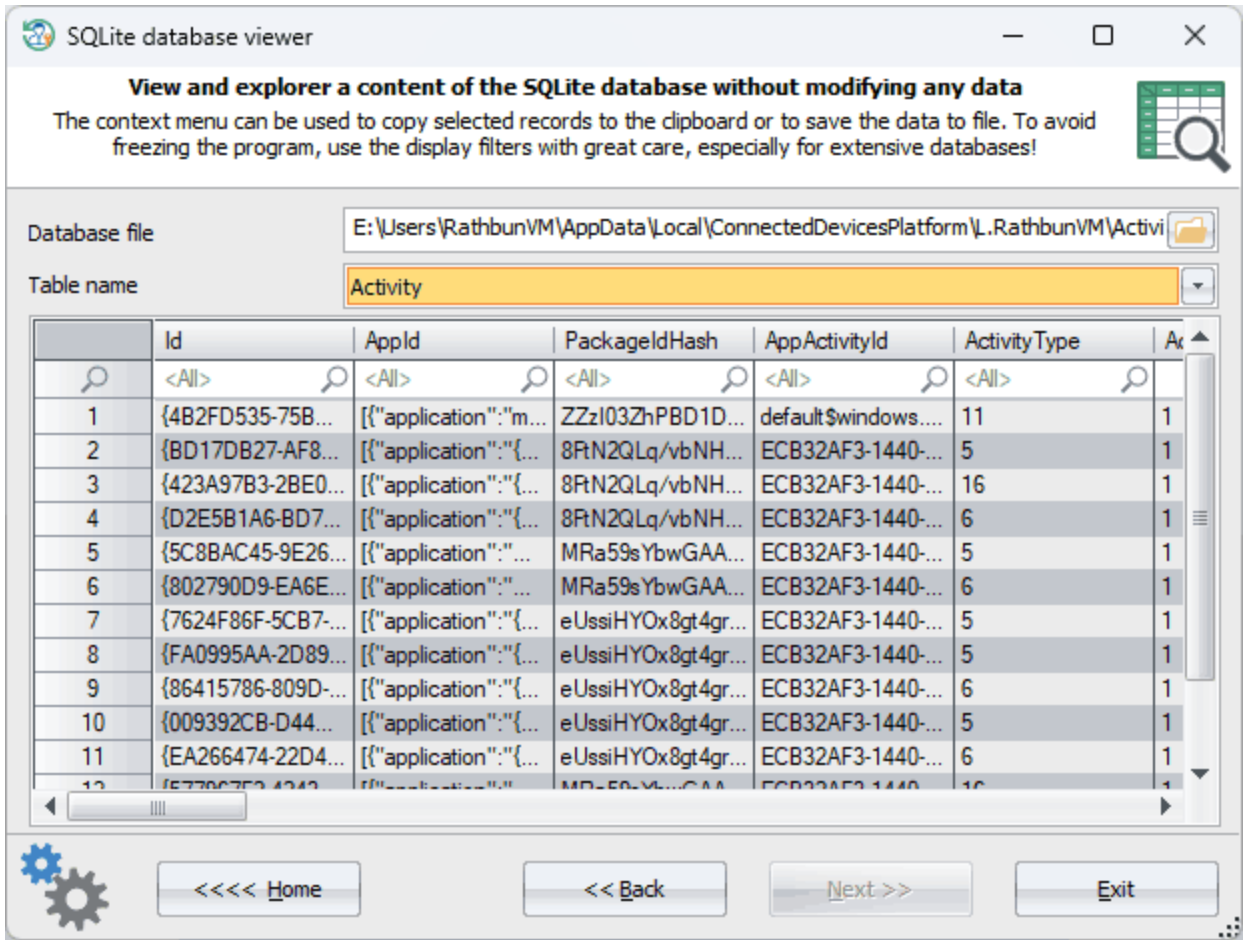
ESE,
[Windows Search explorer.](#)

3.9.6

SQLite

SQLite -

SQLite.



SQLite,

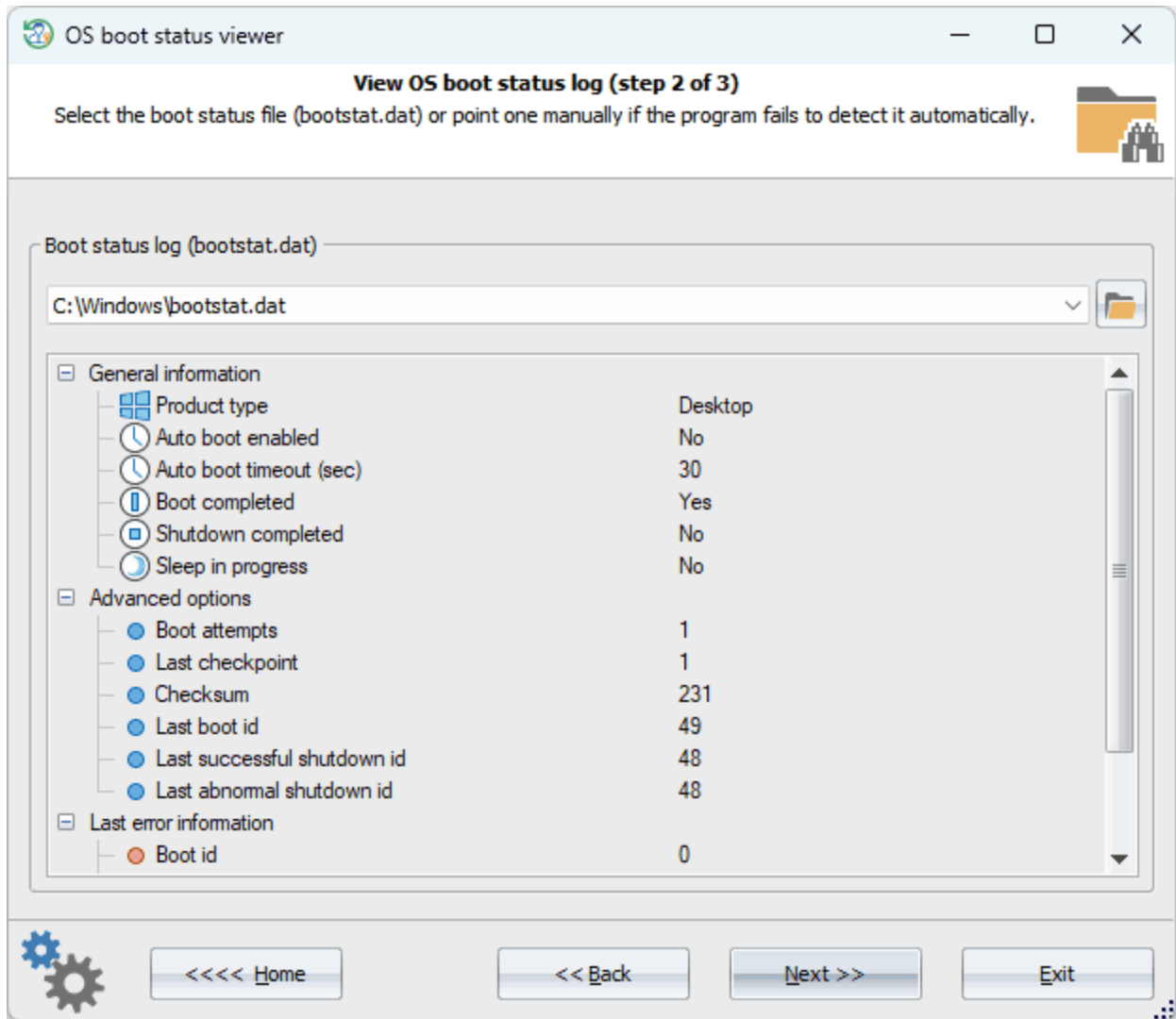
CSV-

3.9.7

bootstat.dat

Windows,

Windows

bootstat.dat

bootstat.dat
Windows.

Windows,
bootstat.dat.

,
EFI,

Windows

OS boot status viewer

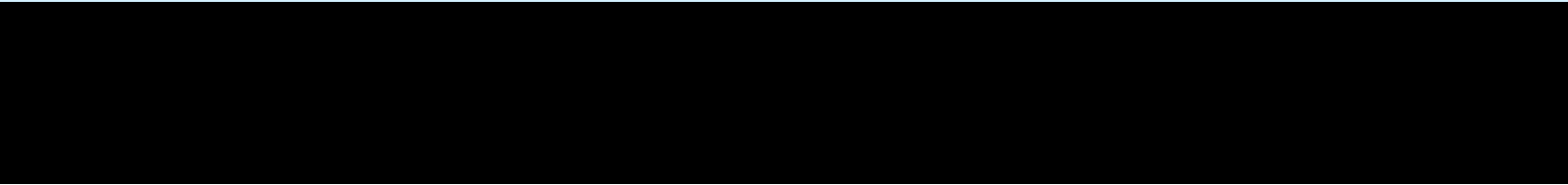
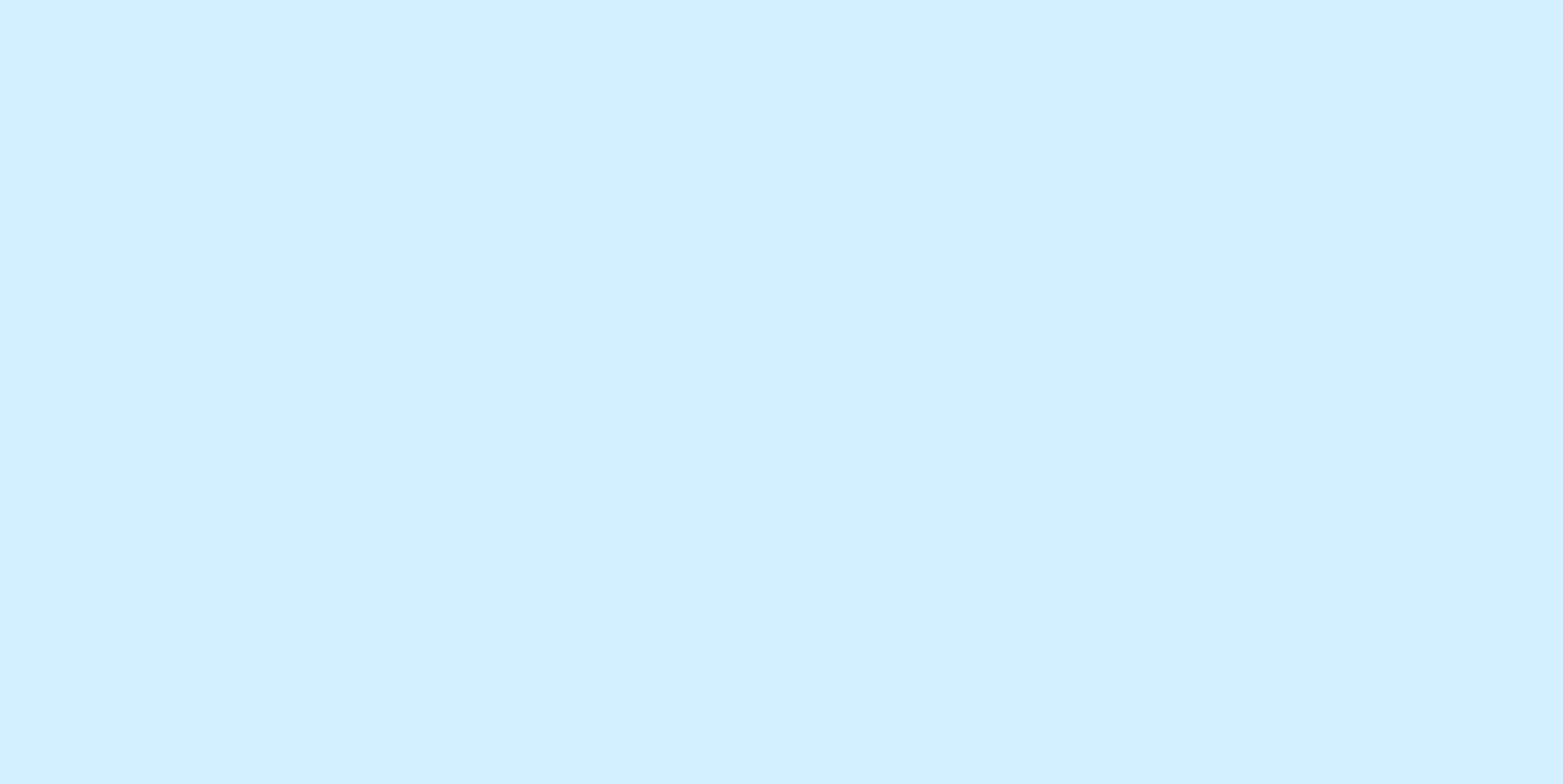
View OS boot status log (step 3 of 3)

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
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	{961BE9FD-A78F-11ED-91C6-C80033...	Information	Event 89	\EFI\Microsoft\Boot\Ci

Navigation: <<<< Home << Back Next >> Exit

- **Time stamp** - Windows BIOS () Windows 10
- **Application** -
- **Type** -
- **Event** -
- **Extended info** -



4

4.1

=====

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.

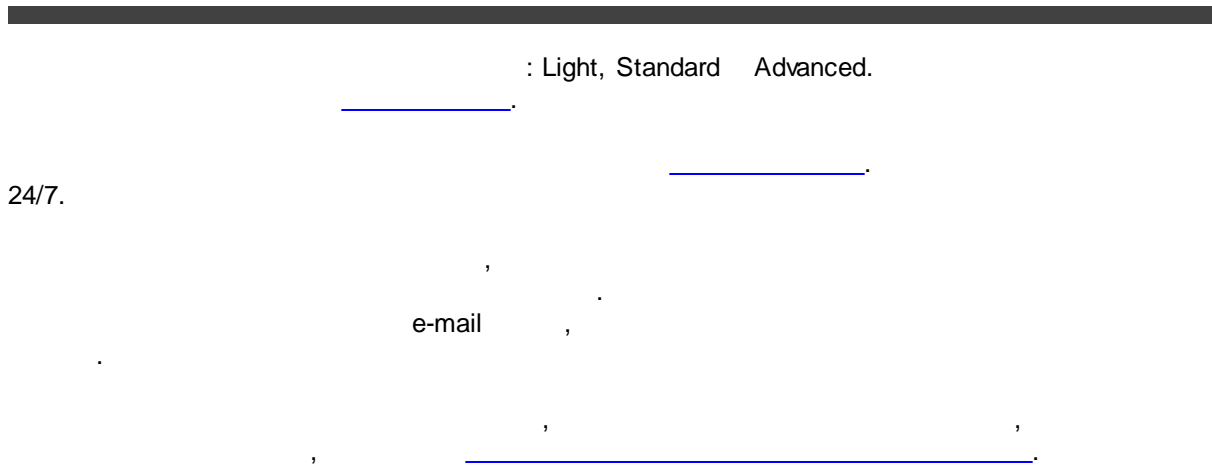
Passcape Software does not warrant that the software is fit for any particular purpose. Passcape Software disclaims all other warranties with respect to the SOFTWARE, either express or implied. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty 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.

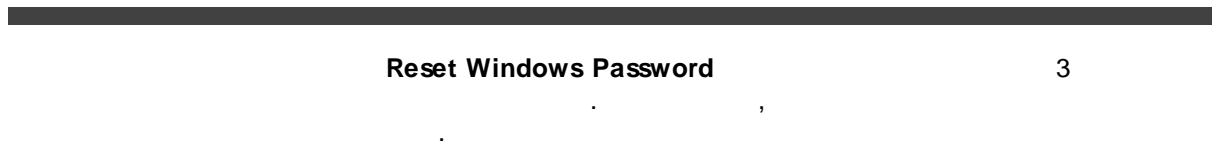
You further attest that the recovered data, passwords and/or files will not be used for any illegal purpose. Be aware password recovery and the subsequencial data decryption of unauthorized or otherwise illegally obtained files may constitute theft or another wrongful action and may result in your civil and (or) criminal prosecution.

All rights not expressly granted here are reserved by Passcape Software.

4.2



4.3



4.4

: Light, Standard Advanced.

	Light	Standard	Advanced
Windows NT/2000/XP/Vista/7/8/10/11	+	+	+

	Light	Standard	Advanced
Windows NT/2000/2003/2008/2012/2016/2019/2022	+	+	+
Windows 32/64-bit	+	+	+
Windows	+	+	+
	+	+	+
IDE/SATA/SCSI/RAID	+	+	+
	+	+	+
Extended download warranty	+	+	+
14-	+	+	+
,	-	-	+
Microsoft account . . . Windows, Live ID,	+	+	+
CD/DVD	+	+	+
USB	+	+	+
HDD	+	+	+
UEFI	+	+	+
,	+	+	+
	+	+	+
	+	+	+
	+	+	+
' (1) '	+	+	+
	-	-	+
	-	-	+
' (1) '	-	-	+
SAM	+	+	+
Active Directory	-	-	+
(SAM)	+	+	+
(SAM)	+	+	+
' SAM (1) '	+	+	+
Windows 10	+	+	+
Active Directory	-	-	+
Active Directory	-	-	+
' Active Directory (1) '	-	-	+
/ DSRM (2)	-	-	+

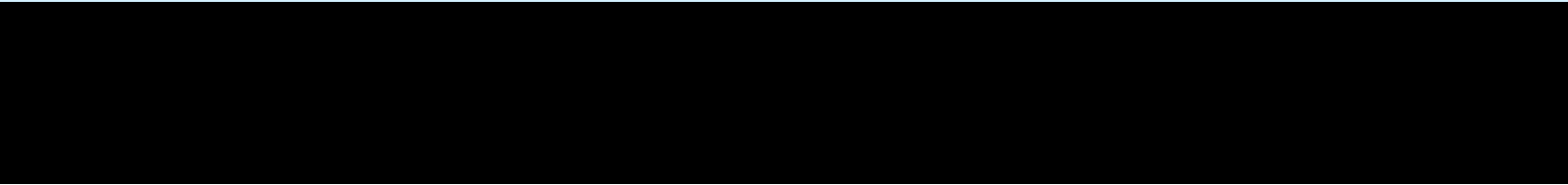
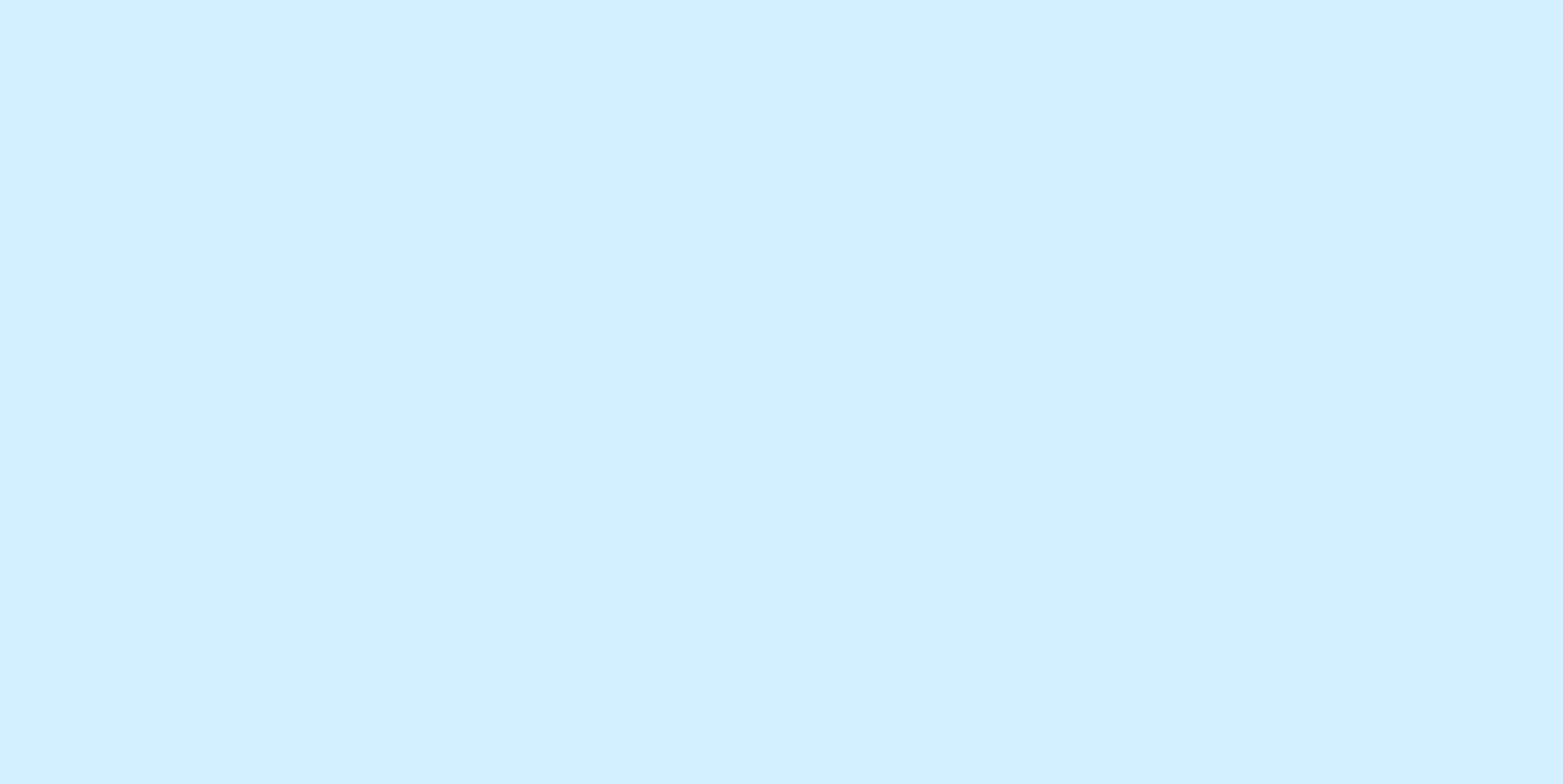
	Light	Standard	Advanced
(DCC)	-	+	+
(DCC)	-	+	+
IDE/SATA/SCSI/RAID/NVME	+	+	+
()	+	+	+
SYSKEY	+	+	+
SYSKEY-	+	+	+
SYSKEY-	+	+	+
	+	+	+
LM/NTLM (SAM)	+	+	+
	-	+	+
	-	+	+
LM/NTLM Active Directory	-	-	+
Windows PIN	+	+	+
Directory (3) Active	-	-	+
SAM	-	+	+
	-	-	+
	-	+	+
	-	+	+
(4)	-	-	+
	-	+	+
	-	+	+
	-	+	+
Skype	-	+	+
LibreOffice, MyOffice, PDF Microsoft Office, OpenOffice,	-	+	+
pan Aadhaar and e-	-	+	+
, hiberfil.sys	-	+	+
	-	+	+
(SAM)	-	+	+
Active Directory	-	+	+
	-	+	+
Windows	-	+	+
	-	+	+

	Light	Standard	Advanced
	-	+	+
SYSKEY ()	-	+	+
SYSKEY	-	+	+
	-	+	+
(5)	-	+	+
PIN	-	+	+
PIN (8)	-	+	+
	-	+	+
-	-	+	+
	+	+	+
	+	+	+
ESE (6)	-	-	+
	+	+	+
	-	+	+
	-	+	+
Microsoft Live ID	+	+	+
, Windows Active Directory	+	+	+
-	-	+	+
	-	+	+
	-	+	+
	-	+	+
SAM	-	+	+
Bitlocker	+	+	+
Bitlocker, Active Directory	-	-	+
	-	+	+
	-	+	+
	-	-	+
	-	+	+
	-	+	+
	+	+	+
	-	+	+
Windows Hello (8)	-	+	+
(6)	+	+	+
(7)	+	+	+
(7)	+	+	+
(7)	+	+	+

	Light	Standard	Advanced
(6)	+	+	+
(7)	+	+	+
(7)	+	+	+
Windows (6)	+	+	+
Telegram (6)	+	+	+
Telegram	-	-	+
Telegram	-	-	+
(6)	-	-	+
(6)	+	+	+
IP (6)	+	+	+
	-	+	+
	-	+	+
Windows (6)	+	+	+
(6)	+	+	+
Windows (6)	+	+	+
(6)	+	+	+
USB (6)	+	+	+
(6)	+	+	+
(6)	+	+	+
Windows media:	-	-	+
Windows media:	-	-	+
Windows media:	-	-	+
Windows Photos:	-	-	+
Windows Photos:	-	-	+
Media Player:	-	-	+
Media Player:	-	-	+
(6)	-	-	+
Windows Search (6)	-	-	+
SQLite (6)	-	-	+
(6)	-	-	+
(7)	-	+	+
(7)	-	+	+
(6)	-	-	+
(6)	-	-	+
	-	+	+
(7)	+	+	+
	+	+	+
*.RAW *.ZIP	+	+	+

	Light	Standard	Advanced
*.E01	-	+	+

- (1) :
- (2) Directory Services Restore Mode ,
- (3) .
- (4) : , , , ,
- (5) , , , .
- (6) Advanced
- (7) Standard Advanced
- (8) TPM



5

5.1



support@passcape.com.

-
-
-
-
-

Windows,

RWPCrash.log,

5.2



info@passcape.com.

5.3



FAQ.

support@passcape.com.

: sales@passcape.com

!

© 2024 Passcape Software. All rights reserved.