Reset Windows Password

Руководство пользователя

Passcape Software

Введение

1 Введение

1.1 О программе

Reset Windows Password изначально была разработана для сброса, изменения и восстановления паролей учетных записей Windows. Например, когда забыт или утерян пароль единственной учетной записи Администратора ПК. На сегодняшний день Reset Windows Password является одним из самых оптимальных и наиболее функциональных решений в своем классе. Программа поддерживает все версии Windows (на базе Windows NT), работает с Active Directory и кэшированными паролями домена, использует навыки искусственно интеллекта для быстрого восстановления некоторых паролей, имеет ряд других, уникальных возможностей. Она также включает в себя широчайший спектр инструментов для анализа данных, судебной экспертизы и поиска артефактов Windows.

Интерфейс приложения выполнен в виде традиционного пошагового мастера. Таким образом, процесс работы подходит даже для неподготовленного пользователя. Например, удаление пароля Администратора состоит всего из трех шагов, причем часть рутинной работы берет на себя сама программа:

1. Выбор SAM и SYSTEM файлов (программа автоматически производит поиск установленных операционных систем и предлагает найденные файлы реестра).
2. Выбор учетной записи пользователя.
3. Удаление или изменение пароля.

При помощи встроенной утилиты, которая поставляется вместе с программой, можно за пару минут создать загрузочный CD, DVD или USB диск (поддерживаются также такие устройства как Compact Flash, SmartMedia, SONY Memory Stick, Secure Digital, ZIP drives, USB Hard Disk drives и др.). Reset Windows Password поддерживает жесткие диски IDE, SATA, SCSI, RAID, совместим с файловыми системами FAT, FAT32, NTFS, NTFS5, поставляется с большим набором дополнительных драйверов жестких дисков: Highpoint, Intel, Jmicron, Marvell, Nvidia, Silicion Image, Sis, Uli, Via, Vmware и др.

1.2 Особенности и преимущества

Преимущества программы:

- Поддержка всех версий Windows на базе Windows NT. Включая серверные ОС.
- Поддержка 32/64-битных Windows.
- Большая коллекция драйверов жестких дисков. Установка дополнительных драйверов без перезагрузки программы.
- Сброс и изменение паролей локальных и доменных пользователей, локального администратора, администратора домена, других учетных записей Active Directory.
- Активация и разблокировка учетных записей пользователей, локальных и доменных администраторов.
- Редактор учетных записей, политики паролей, ограничений интерфейса и системы.
- Включение/отключение опции окончания срока действия пароля.
- Автоматический поиск нескольких операционных систем.
- Поддержка неанглийских версий Windows и паролей в национальных кодировках.
- Дамп хэшей паролей пользователей из SAM для их дальнейшего анализа.
- Дамп хэшей паролей из Active Directory.
- Дамп кэшированных паролей домена.
- Несколько продвинутых модулей для извлечения и расшифровки текстовых паролей, хранящихся в Active Directory.
- Отмена изменений, внесенных в систему.
- Удаление паролей и других конфиденциальных данных с компьютера.

- Продвинутые алгоритмы поиска и восстановления паролей.
- Сброс SYSKEY.
- Поиск начального пароля SYSKEY.
- Поиск серийных ключей различных программ.
- Поиск и расшифровка сетевых паролей.
- Резервное копирование реестра и Active Directory, а также другой конфиденциальной информации.
- Поддержка дисков, зашифрованных Bitlocker.
- Поиск паролей для виртуальных машин.
- Дисковые утилиты.
- Поиск и восстановление паролей для документов PDF, OPENOFFICE, MS WORD, EXCEL и т.д.
- Инструменты для криминалистического анализа: статистика входа в систему, история железа, программ, сети, посещений Интернет, буфера обмена, usb, активность пользователя, системные события, последний доступ к оборудованию, временная шкала активности, поиск лиц на фото и видео, монитор использования системных ресурсов, обозреватель базы данных Windows Search и т.п.

Приложение доступно в трех редакциях: **Light**, **Standard** и **Advanced**. Детальный список всех возможностей для каждой редакции можно посмотреть тут.

1.3 Системные требования

Требования
x64 микропроцессор, минимум 1 ГБ ОЗУ, CD-ROM или USB диск. Размер загрузочного USB диска должен не менее 512 МБ (рекомендуется 2-32 ГБ USB диск для обеспечения наилучшей совместимости). BIOS компьютера должен поддерживать загрузку с CD, DVD или USB устройств.

Совместимость
Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7-11, Windows Server 2000-2022. Файловые системы: FAT, FAT32, NTFS, NTFS5, ReFS. Программа совместима с большинством CD/DVD рекордеров и USB устройств, включая Memory Stick, Compact Flash, SmartMedia, Secure Digital, USB flash drives, USB ZIP drives, USB Hard Disk drives и др.

Ограничения
Если целевая система использует нестандартное запоминающее устройство, для его работы, возможно, потребуется установить драйвер этого устройства, совместимый с Windows 11. Обратитесь к руководству по материнской плате за деталями.

Известные проблемы
- Если в целевой системе присутствуют 2 или более логических диска, буквы для этих дисков могут быть назначены в произвольном порядке.
- Если вы сбрасываете пароль встроенной учетной записи Администратора, имейте в виду, что в некоторых версиях Windows для ее активации и входа в систему, потребуется выполнить загрузку ОС в безопасном режиме.
- Программа поддерживает все типы шифрования SYSKEY. В некоторых случаях может потребоваться начальный пароль SYSKEY или загрузочная дискета. Однако программа также позволяет сбросить вручную или производить поиск SYSKEY пароля.
- После сброса пароля локальной учетной записи, вы временно потеряете доступ к паролям веб-страниц, паролям LAN и беспроводной сети, зашифрованным EFS файлам, сообщениям электронной почты, которые зашифрованы закрытыми ключами. Обратитесь к базе знаний Майкрософт за более подробной информацией.

- Сброс паролей определенных учетных записей Active Directory может не возыметь должного эффекта. Например на RODC.
- Сброс паролей, а также другие функции, подразумевающие запись на диск, на виртуальной ОС не имеют никакого эффекта.
- При сбросе пароля для учетной записи Microsoft, необходимо указать непустой пароль. В противном случае, вы не сможете войти в систему.

Создание загрузочного диска

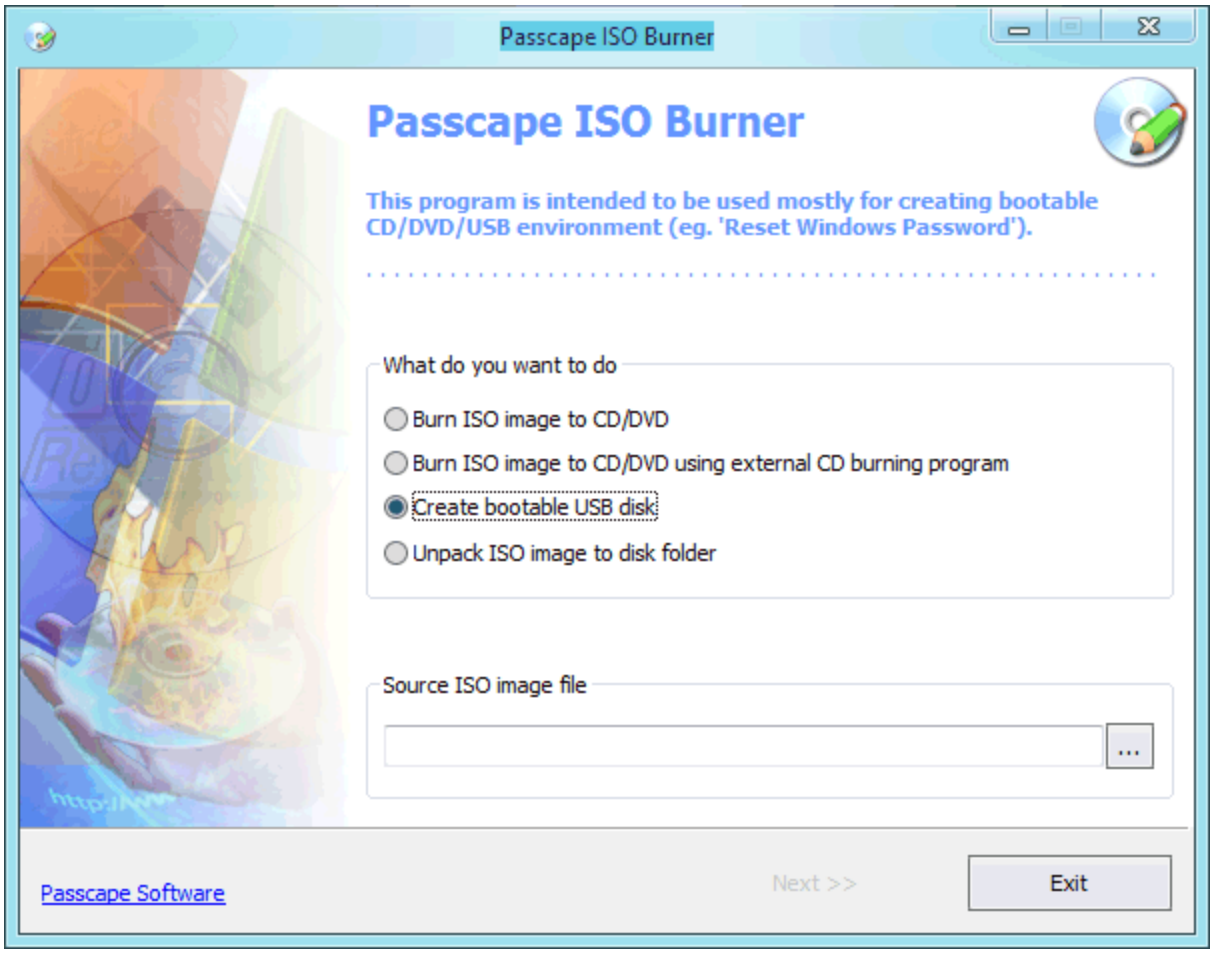
2 Создание загрузочного диска

2.1 3 простых шага для запуска программы с загрузочного диска

1. Скачайте архив с программой Reset Windows Password по адресу https://www.passcape.com/download/rwp.zip (или используйте ссылку, которая была выслана в вашем регистрационном письме).
2. Создайте загрузочный диск RWP: распакуйте файл RWP.ZIP, запустите утилиту IsoBurner.exe, выберите опцию для создания CD/DVD/USB, укажите путь к распакованному ISO образу с программой и создайте загрузочный диск из этого образа.
3. Включите проблемный компьютер и измените его BIOS/UEFI настройки таким образом, чтобы ваш диск (CD-ROM, DVD-ROM или USB) был первым в списке загрузочных устройств. Сохраните параметры и перезагрузитесь еще раз для того, чтобы запустить программу с вашего CD, DVD или USB диска. Если BIOS/UEFI поддерживает функцию быстрого выбора загрузочного диска (обычно клавиша F8), можно воспользоваться этой опцией.

2.2 Создание загрузочного диска RWP

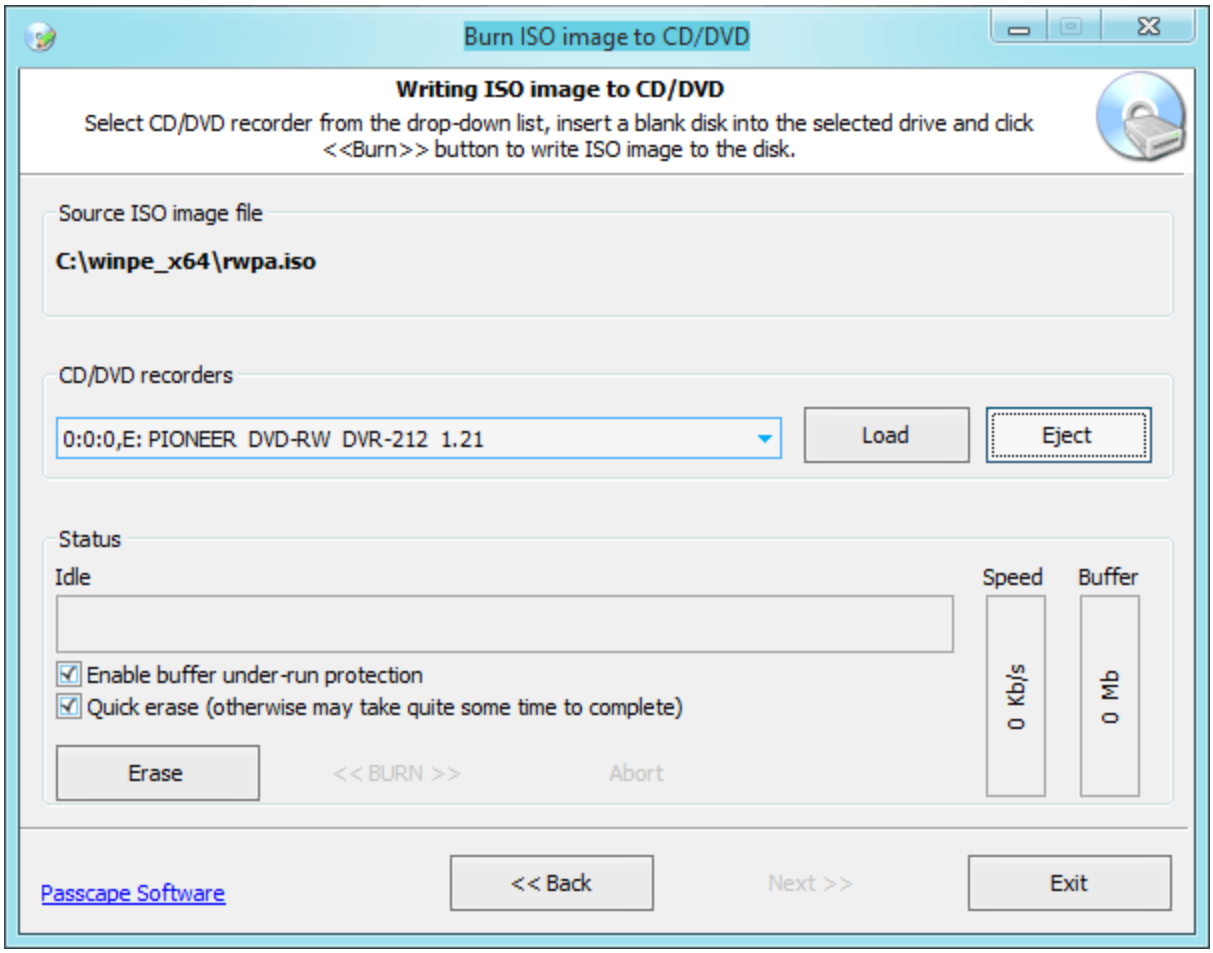
Passcape ISO Burner



Passcape ISO Burner это программа для создания загрузочных CD, DVD или USB дисков из ISO-9660 образов. Программа бесплатна и доступна для скачивания и использования с нашего сайта: https://www.passcape.com/download/pib.zip

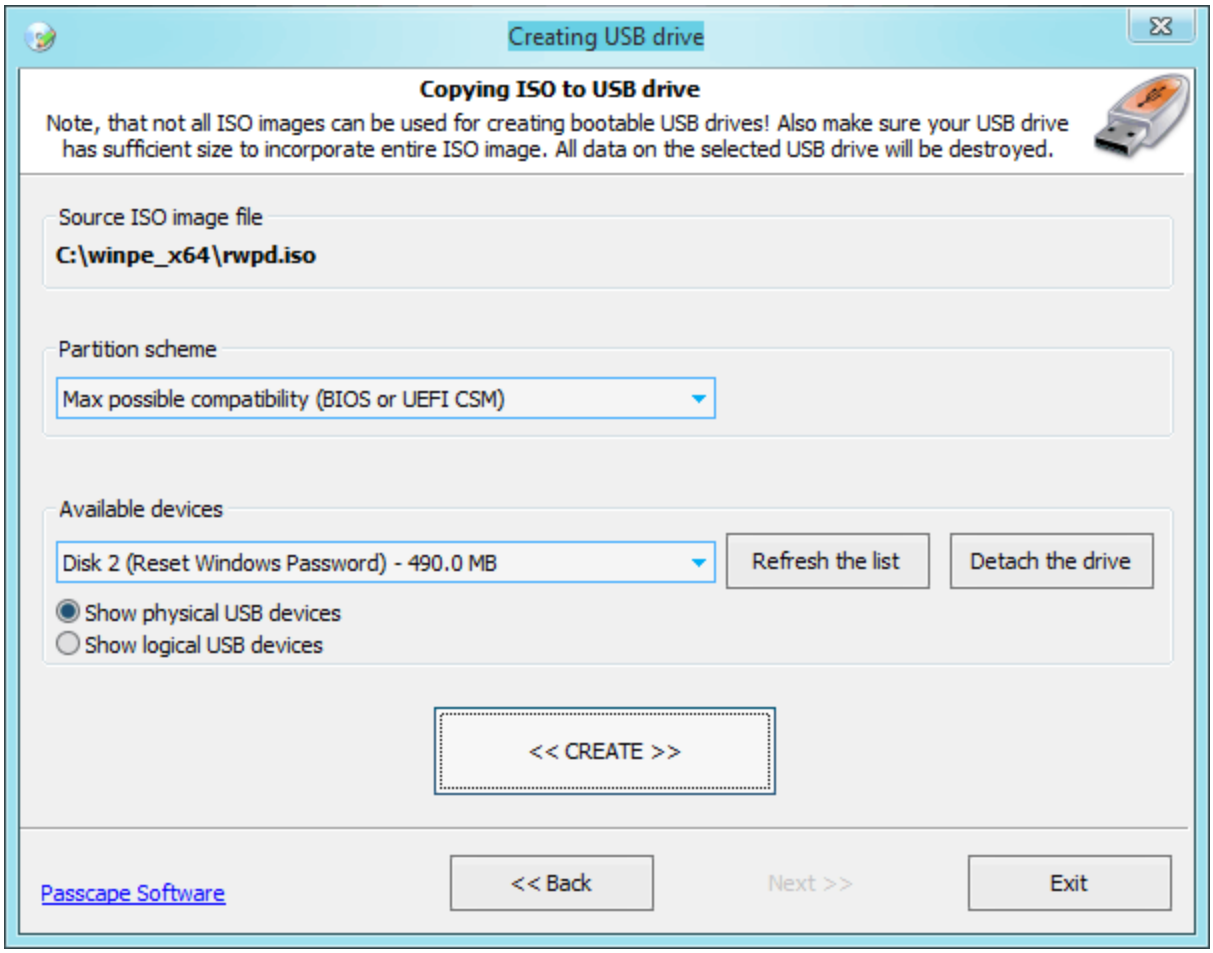
Интерфейс приложения предельно простой. При запуске, программа попросит вас выбрать, что вы хотели бы сделать:
- Записать ISO образ на CD/DVD с помощью этого приложения.
- Записать ISO образ на CD/DVD, используя внешнюю программу, установленную на вашем компьютере. Например, Nero или ее бесплатный аналог ImgBurn.
- Использовать ISO-образ для создания загрузочного USB диска.
- Распаковать ISO образ на диск (учтите, это действие может привести к потере загрузочных данных).

Создание загрузочного CD с Reset Windows Password



Выберите первый пункт меню: '*Burn ISO image to CD/DVD*'. В нижней части экрана, указываем путь к файлу с ISO образом. После этого активируется кнопка 'Next', и можно переходить непосредственно к созданию диска. Все, что нам нужно, это выбрать рекордер, вставить пустую CD/DVD болванку и нажать на кнопку <<Burn>> для прожига выбранного ISO образа на диск.

Создание загрузочного USB с Reset Windows Password



Выберите загрузочный ISO образ с программой и установите опцию создания загрузочного USB. После появления следующего диалога, подключите USB-устройство к компьютеру, оно должно автоматически появиться в списке найденных устройств. Нажмите на кнопку << CREATE >> для форматирования и создания загрузочного USB. В некоторых случаях (например, если USB-устройство определяется как жесткий диск, и есть расширенные записи раздела на этом диске) программе может понадобиться перезагрузка для переназначения букв дисков.

Программа предлагает несколько схем работы (режимов форматирования) для обеспечения лучшей совместимости при загрузке с USB-устройств. Если Вы не уверены, какую схему лучше выбрать, можно использовать следующий простой алгоритм:

- Если целевой компьютер собран на базе UEFI, выберите режим 'Max compatibility with new PCs (FAT32 MBR for UEFI)'. При этом будет создан USB-носитель для запуска на компьютерах с UEFI с включенным режимом безопасной или быстрой загрузки.
- Если в целевом ПК стоит BIOS, выберите режим 'Max compatibility with old PCs (FAT32 MBR for BIOS)'. Будет создан загрузочный USB, полностью совместимый с БИОС прошивками.
- Если о целевом ПК ничего не известно, переключитесь на схему максимально возможной совместимости ('Max possible compatibility'). Этот режим создает загрузочные USB диски, которые могут работать как с BIOS и UEFI (если включен режим совместимости или **Compatibility Support Mode**). На некоторых ПК или ноутбуках режиме совместимости также известен как **Legacy Boot Mode**.

UEFI (Unified Extensible Firmware Interface) — замена устаревшему BIOS. Она отличается от BIOS как самой процедурой загрузки, так и способами взаимодействия с ОС. Если вы купили компьютер в 2010 году и позже, то, вероятнее всего, у вас UEFI.

Будьте осторожны! Все данные на целевом диске будут стерты. Если программе не удается обнаружить загрузочные данные в исходном ISO-образе, будет выдано соответствующее предупреждение.

Кроме того, имейте в виду, что некоторые антивирусы могут блокировать создание загрузочных дисков или записи некоторых загрузочных файлов даже без выдачи соответствующих предупреждений!

2.3 Изменение настроек BIOS/UEFI

Общая информация

Для запуска Reset Windows Password с загрузочного диска, вам, скорее всего, потребуется изменить настройки вашего компьютера (BIOS/UEFI) так, чтобы разрешить запуск программы с загрузочного CD, DVD или USB носителя. Вот примерный алгоритм работы:

1. Во время загрузки компьютера, сразу после включения, несколько раз нажимайте клавишу **Del**, пока не окажетесь в меню с настройками BIOS. Некоторые версии BIOS используют другие горячие клавиши; например, **F2**, **F10**, **F11**, **ESC** и т.д. Обычно внизу экрана отображается соответствующая подсказка.
2. Войдите в настройки BIOS/UEFI, найдите меню, которое отвечает за загрузочные устройства. Отредактируйте его таким образом, чтобы загрузочный CD или USB с Reset Windows Password был первым в списке устройств.
3. Сохраните изменения и перезагрузите компьютер.

Если BIOS/UEFI поддерживает функцию быстрого выбора загрузочного диска (обычно клавиша F8), можно воспользоваться этой опцией. В этом случае, модификация BIOS/UEFI не потребуется.

Для более детальной информации, обратитесь к справочному руководству материнской платы вашего ПК.

Меняем настройки BIOS, вопросы и ответы

Q: БИОС моего компьютера имеет несколько пунктов загрузки: USB FDD, USB ZIP, USB HDD, USB CDROM. Какой из них следует выбрать?
A: Разные производители BIOS задают настройку загрузочных устройств по-разному. В большинстве случаев, чтобы загрузиться с обычной флешки на некоторых материнских платах вы должны выбрать опцию USB-ZIP, на других USB-HDD. Чаще - последнее.

Q: Приложению требуется очень много времени (иногда до 10 минут) для загрузки с USB-носителя.
A: Скорее всего, носитель работает на медленном протоколе USB 1.1. Во-первых, устройство должно поддерживать спецификацию 2.0 или выше. Во-вторых, USB порт на материнской плате, куда вы подключили запоминающее устройство, должно поддерживать спецификацию 2.0+. И в-третьих, необходимо включить поддержку USB 2.0 (или выше) в BIOS, если имеется соответствующая опция.

Q: Компьютер вообще не загружается с USB устройства. При попытке загрузки – черный экран или сообщение 'no operating system'.
A: Попробуйте найти опцию 'Legacy USB storage detect' и включить ее. В настройках загрузки желательно иметь только один USB-носитель. Если у вас два и более USB-устройства, подключенных к компьютеру (например, ИБП, принтер, сканер, модем и т. д.), оставьте только один загрузочный USB-диск. Если это не помогло, отключите USB устройство от компьютера, выключите компьютер, подключите USB-устройство к другому USB-порту, включите компьютер и попробуйте загрузиться еще раз. Если и это не помогает – попробуйте обновить БИОС. Возможно, материнская плата не поддерживает загрузку с USB, либо не поддерживает файловую систему, в которой отформатирован USB накопитель.

Q: При загрузке с CD или USB возникают разные виды ошибок: висит голубой или черный экран, ошибки загрузки реестра, драйверов и т.д.
A: Возможно, недостаточно оперативной памяти. Минимальный требуемый размер памяти для загрузки программы - 1 ГБ. Для комфортной работы, необходимо 2 ГБ и больше.

Q: Не могу попасть в BIOS, требуется пароль.
A: Неприятный сюрприз может поджидать вас, когда вы попытаетесь изменить настройки загрузочного устройства в BIOS. Дело в том, что некоторые производители оборудования, продавцы или предыдущие владельцы ПК могут устанавливать свой пароль для доступа к BIOS. Другими словами, для того, чтобы изменить настройки BIOS, вам потребуется ввести пароль, который, как правило, не представляется возможным выяснить.
Некоторые версии BIOS позволяют сбросить настройки, нажав определенную клавишу на клавиатуре; как правило, это клавиша **Ins**. Для некоторых типов AMI BIOS это сочетание клавиш **Ctrl+Alt+Del+Ins**. На BIOS компании Award, эта комбинация должна быть нажата и удерживаться во время включения компьютера. Однако, используйте эти комбинации с большой осторожностью, т.к. они сбрасывают и все остальные настройки.
Кроме того, существуют универсальные секретные пароли. Они приводятся ниже и подходят для многих популярных старых версий BIOS. Версия и тип BIOS обычно отображается в течение нескольких секунд во время начальной загрузки компьютера в нижней части экрана.
Если ни один из универсальных паролей работает, можно воспользоваться методом, описанным во многих руководствах пользователя материнской платы: просто сбросить параметры BIOS путем замыкания соответствующей перемычки. Она, как правило, расположена рядом с большой CMOS батарейкой. Если на материнской плате нет CMOS батареи, найти микрочип с маркировкой Dallas или Odin; перемычка должна быть где-то рядом. Просто удаление CMOS батареи не всегда помогает, так как микросхема BIOS может спокойно прожить и работать несколько часов без питания. Для сброса настроек BIOS крайне не рекомендуется коротить CMOS батарею на саму себя, так как это может существенно сократить время ее автономной работы.
В сети можно найти целый ряд программ для восстановления паролей и сброс БИОС. Например, cmospwd и killcmos. Настоятельно не рекомендуется сбрасывать настройки BIOS в ноутбуках. Это может привести к полному краху системы.

Q: При начальной загрузке всплывает окно с ошибкой в котором говорится, что процессор не поддерживает 64-битный режим или запуск 64-битных приложений.
A: Reset Windows Password больше не поддерживает 32-битные процессоры. Свяжитесь с техподдержкой, чтобы получить ссылку на последнюю 32-разрядную версию. Это ограничение не действует на 32-разрядные операционные системы.

Q: Можно ли загрузить BIOS-совместимый загрузочный CD/USB диск в UEFI?
A: Да. Войдите в настройки UEFI. Для этого нажмите ESC, F2 или DEL во время загрузки ПК. Откройте меню 'Boot' и включите опцию 'Launch CSM'. Теперь найдите вкладку 'Security' и отключите 'Secure Boot Control'. Сохраните изменения и перезапустите компьютер. Войдите еще раз в настройки UEFI и убедитесь, что ваше DVD/USB устройство стало доступно в разделе загрузка. Некоторые UEFI имеют меню выбора устройств (активируемое, как правило, клавишей F8), в котором можно быстро выбрать загрузочное устройство и режим его работы.

Q: Можно ли создать USB диск, который будет загружаться и в BIOS, и в UEFI?
A: Да. Запустите утилиту IsoBurner и выберите режим максимальной совместимости ('Max possible compatibility') при создании загрузочного USB. Этот режим создает загрузочные диски, которые могут работать как с BIOS, так и с UEFI (если включен режим совместимости). На некоторых компьютерах или ноутбуках режим совместимости также известен как 'Legacy Boot Mode'.

Q: USB флешка отсутствует в вариантах загрузки UEFI. Как включить загрузку с этого диска?

A: Похоже, USB был отформатирован в режиме BIOS или в UEFI CSM, но ваш UEFI позволяет загрузку только в режиме безопасной загрузки UEFI. Придется разрешить загрузку в режиме совместимости. В настройках UEFI отключите опцию 'Boot - Fast Boot' и 'Security - Secure Boot', затем активируйте режим совместимости ('Compatibility Support Mode' или похожее название). Альтернативным решением будет просто создание загрузочного диска с помощью схемы 'Max compatibility with new PCs (FAT32 MBR for UEFI)'. Эта схема полностью совместима с режимом UEFI Secure Boot.

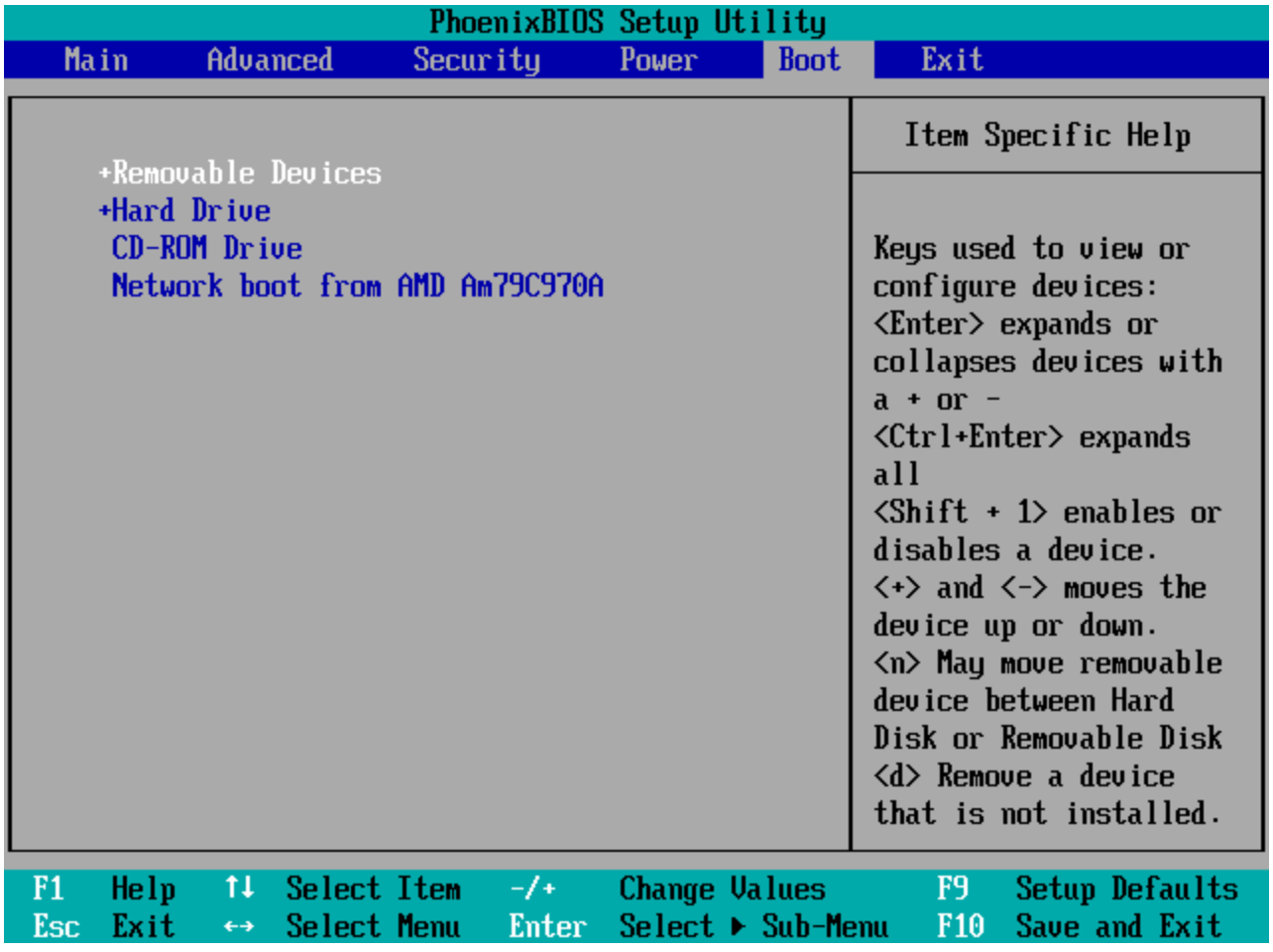
Секретные универсальные пароли BIOS

Производитель BIOS	Универсальный пароль
AWARD BIOS 2.50	AWARD_SW, 01322222, j262, TTPTHA, KDD, ZBAAACA, aPAf, lkwpeter, t0ch88, t0ch20x, h6BB
AWARD BIOS 2.51	AWARD_WG, HLT, BIOSTAR, SWITCHES_SW, 256256, j256, ZAAADA, Syxz, ?award, alfarome, Sxyz, SZXY
AWARD BIOS 2.51G	HEWITTRAND, HLT, biostar, HELGA-S, bios*, g6PG, j322, ZJAAADC, Wodj, h6BB, t0ch88, zjaaadc
AWARD BIOS 2.51U	condo, biostar, CONDO, CONCAT, 1EAAh, djonet, efmukl, g6PG, j09F, j64, zbaaaca
AWARD BIOS 4.5	AWARD_SW, AWARD_PW, PASSWORD, SKYFOX, award.sw, AWARD?SW, award_?, award_pc, ZAAADA, 589589
AWARD BIOS 6.0	AWARD_SW, HLT, KDD, ?award, lkwpeter, Wodj, aPAf, j262, Syxz, ZJAADC, j322, TTPTHA, six spaces, nine spaces, 01355555, ZAAADA
AMI BIOS	AMI, SER, A.M.I., AMI!SW, AMIPSWD, BIOSPASS, aammii, AMI.KEY, amipswd, CMOSPWD, ami.kez, AMI?SW, helgaЯs, HEWITT RAND, ami', AMISETUP, bios310, KILLCMOS, amiami, AMI~, amidecod
AMPTON BIOS	Polrty
AST BIOS	SnuFG5
BIOSTAR BIOS	Biostar, Q54arwms
COMPAQ BIOS	Compaq
CONCORD BIOS	last
CTX International BIOS	CTX_123
CyberMax BIOS	Congress
Daewoo BIOS	Daewuu, Daewoo
Daytec BIOS	Daytec
DELL BIOS	Dell

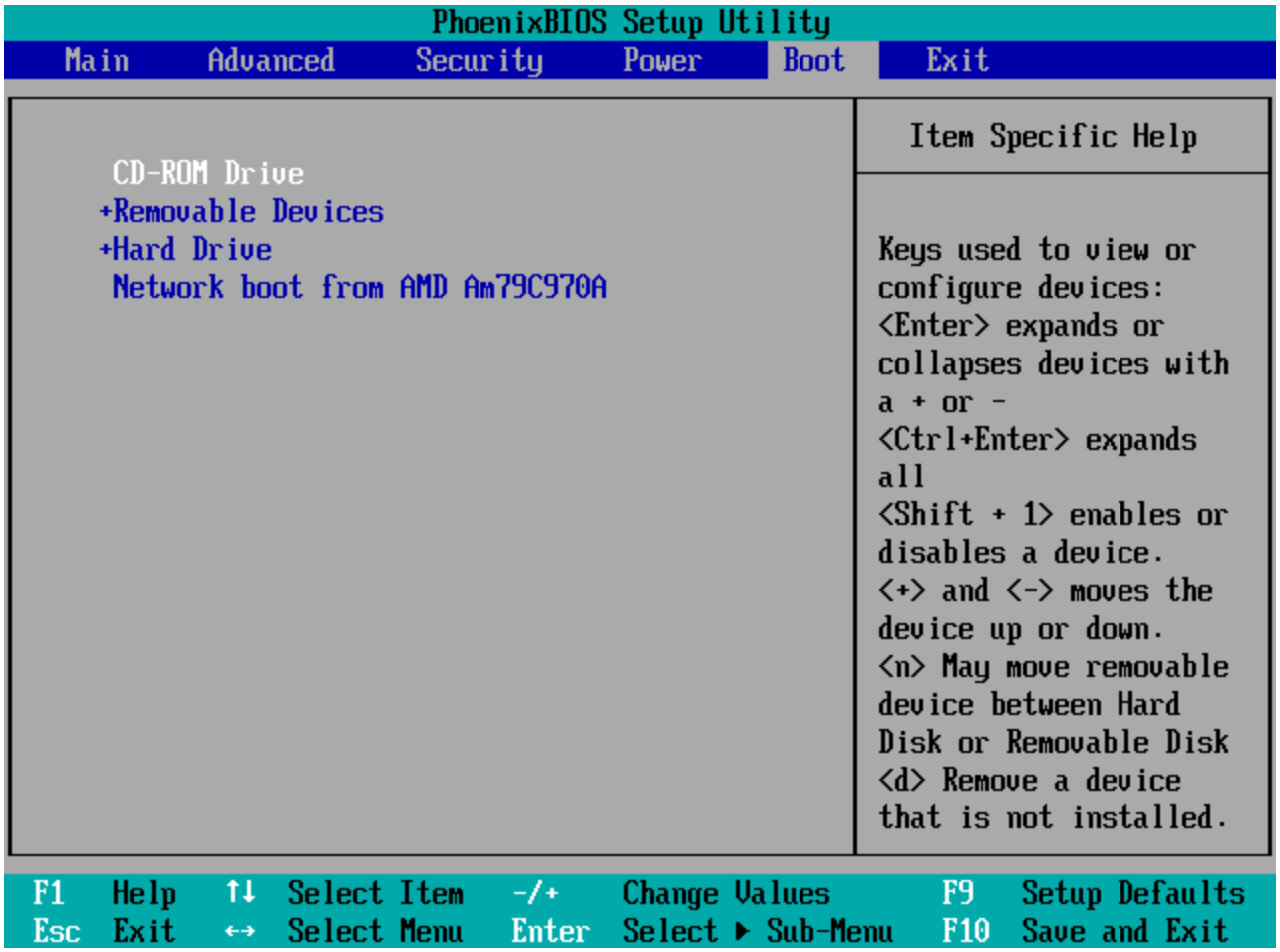
Digital Equipment BIOS	komprie
Enox BIOS	xo11nE
Epox BIOS	Central
Freetech BIOS	Posterie
HP Vectra BIOS	hewlpack
IMB BIOS	IBM, MBIUO, sertafu
Iwill BIOS	iwill
JetWay BIOS	spooml
Joss Technology BIOS	57gbz6, technology
M Technology BIOS	mMmM
MachSpeed BIOS	sp99dd
Magic-Pro BIOS	prost
Megastar BIOS	star, sldkj754, xyzall
Micronics BIOS	dn_04rjc
Nimble BIOS	xdfk9874t3
Packard Bell BIOS	bell9
QDI BIOS	QDI
Quantex BIOS	teX1, xljlbj
Research BIOS	Col2ogro2
Shuttle BIOS	Col2ogro2
Siemens Nixdorf BIOS	SKY_FOX
SpeedEasy BIOS	lesarot1
SuperMicro BIOS	ksdjfg934t
Tinys BIOS	tiny, tinys
TMC BIOS	BIGO
Toshiba BIOS	Toshiba, 24Banc81, toshy99
Vextrec Technology BIOS	Vextrex

Vobis BIOS	merlin
WIMBIOS v.2.10 BIOS	Compleri
Zenith BIOS	3098z, Zenith
ZEOS BIOS	zeosx

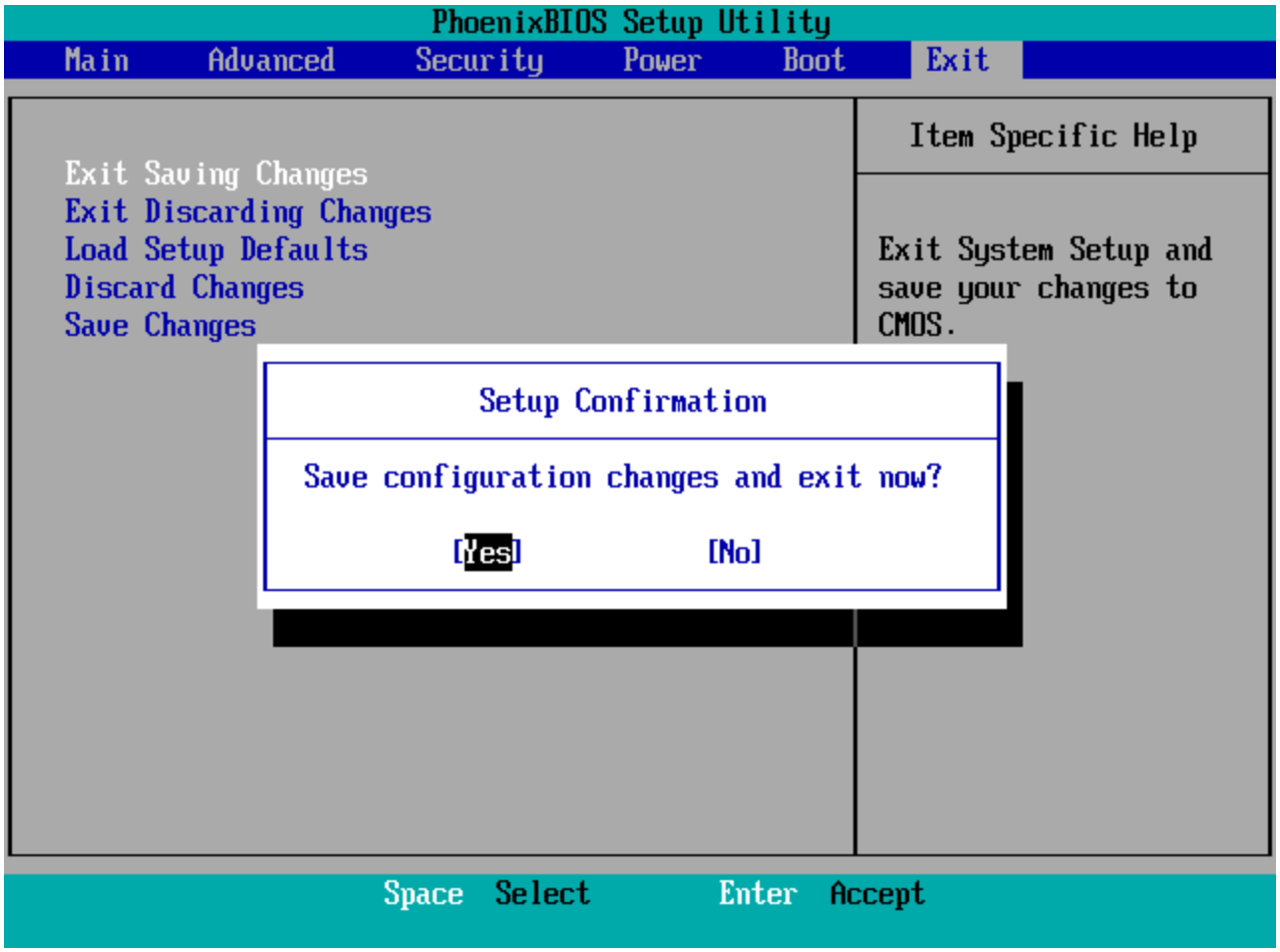
2.4 Запуск программы с загрузочного CD/DVD/USB диска на BIOS-совместимых ПК



Включите компьютер. Нажимайте клавишу **Del** до тех пор, пока не войдете в меню BIOS. Некоторые версии BIOS используют другие горячие клавиши: F2, F10, F11, ESC и т.д. Обычно, внизу экрана на несколько секунд отображается подсказка.

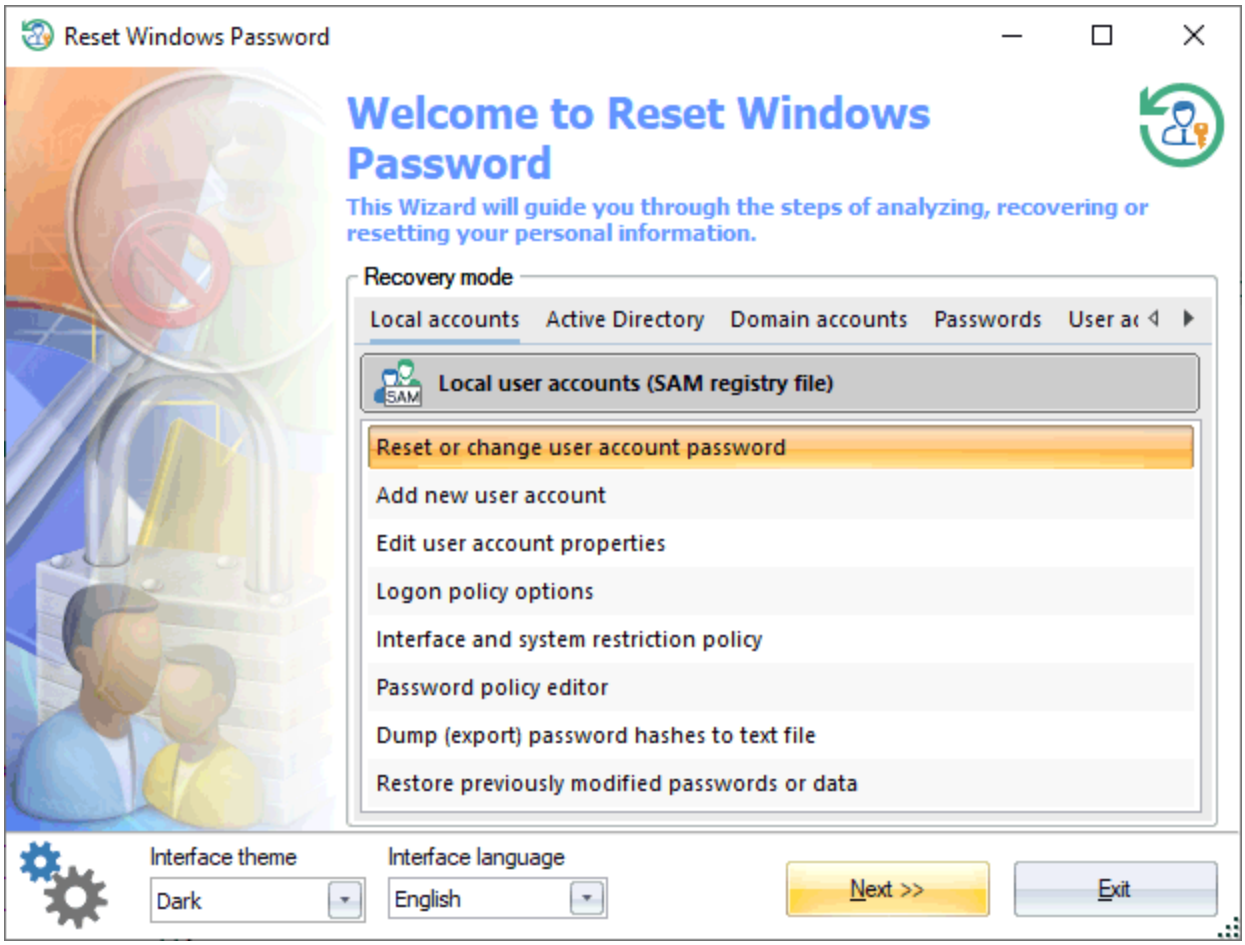


Отредактируйте загрузочное меню BIOS таким образом, чтобы CD или USB диск с Reset Windows Password был первым в списке загрузочных устройств.



Сохраните сделанные изменения и перезагрузите компьютер.

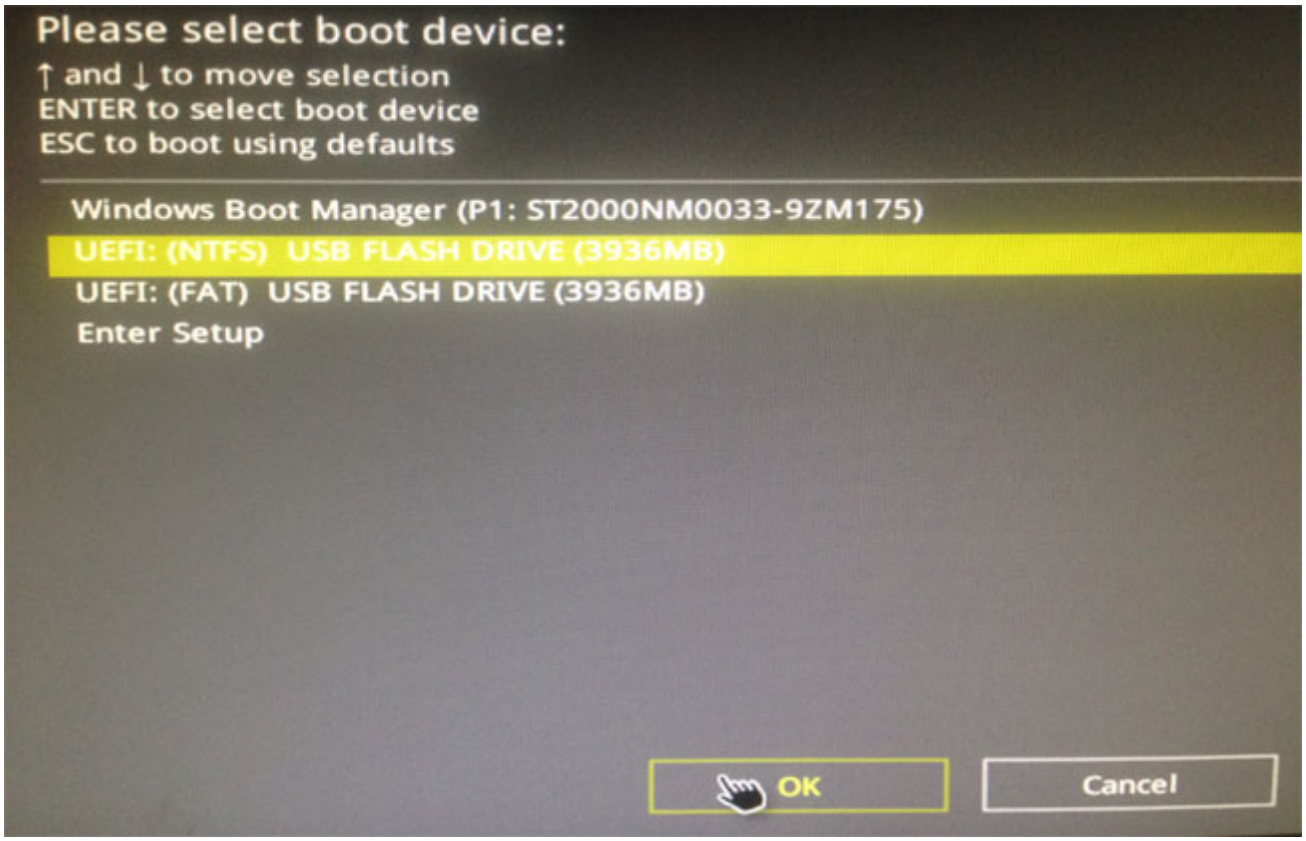
Если все прошло нормально, вы можете увидеть такое текстовое сообщение. Нажмите любую клавишу для загрузки Reset Windows Password. В противном случае, будет запущена установленная операционная система.



RWP был успешно загружен и готов к работе.

2.5 Запуск программы при наличии опции быстрого выбора загрузочного устройства

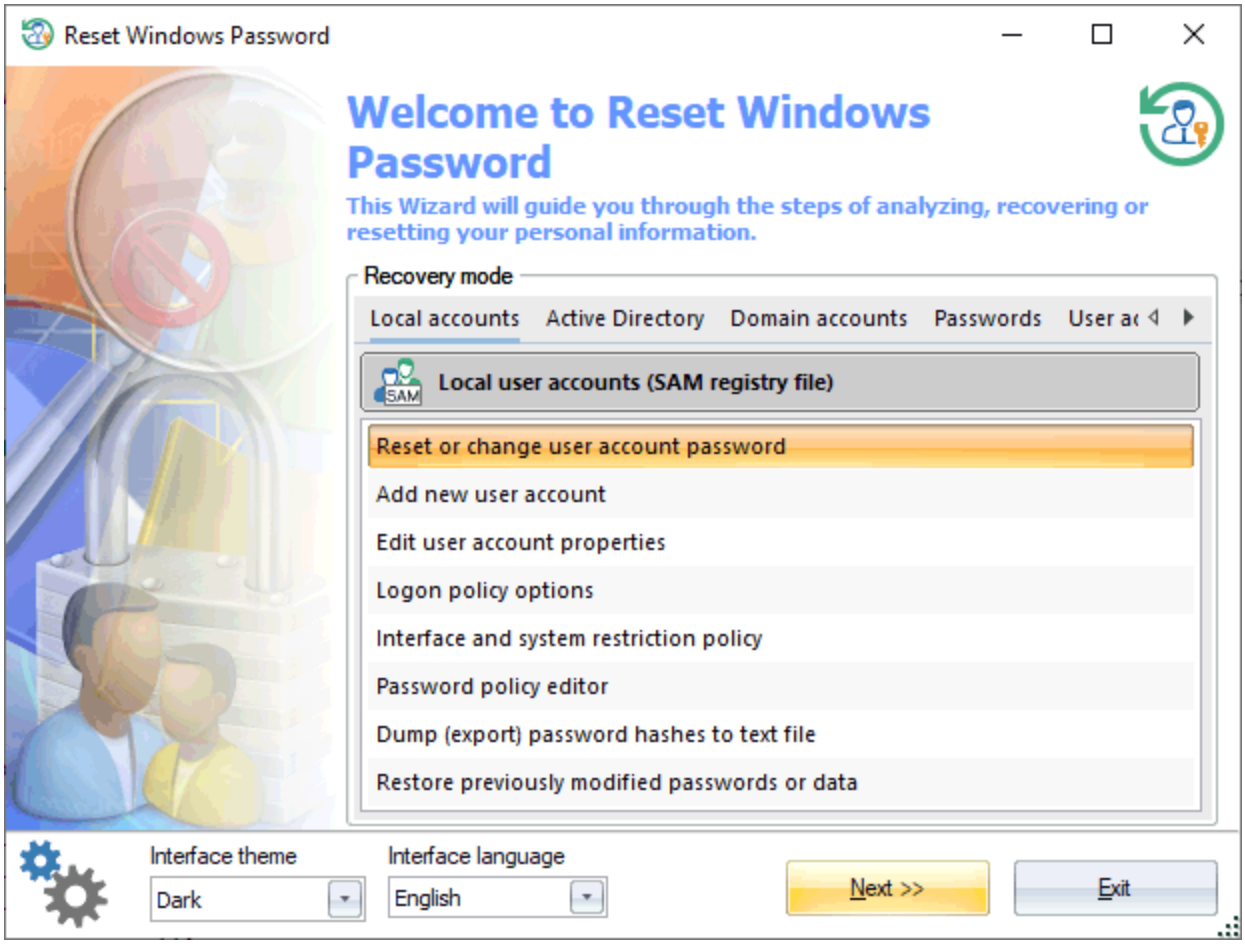
Если BIOS/UEFI поддерживает функцию выбора носителя при загрузке компьютера, можно воспользоваться ей для запуска программы. В зависимости от производителя UEFI, используются разные горячие клавиши для вызова этой функции, обычно это F8. В большинстве версий UEFI выбор загрузчика также доступен из главного меню UEFI.



Работа с программой

3 Работа с программой

3.1 Главное окно



В начале Мастер программы предлагает выбрать один из шести режимов работы: **Local accounts** – операции с обычными учетными записями, которые хранятся в файле реестра SAM, **Active Directory** – операции с доменными учетными записями, хранящимися в базе данных NTDS.DIT, **Domain accounts** - операции с кэшированными записями домена (записи хранятся в реестре SECURITY), **Passwords** - поиск и восстановление текстовых паролей, **User activity** - последняя активность пользователя**, Forensic tools** - инструменты криминалистического анализа, **Files and drives** - файловые и дисковые утилиты, **Utilities** - дополнительные утилиты. После выбора режима работы, программа предлагает выбрать одну из доступных операций (см. ниже).

Локальные учетные записи (SAM)

- Сброс или изменение пароля пользователя
- Создание новой учетной записи
- Редактор свойств учетной записи
- Изменение параметров входа в систему

- Политика ограничений интерфейса и системы
- Редактор политики паролей
- Дамп (экспорт) парольных хэшей
- Дамп Windows PIN
- Откат сделанных ранее изменений

Учетные записи Active Directory (AD)
- Сброс или изменение пароля пользователя
- Сброс/изменение пароля DSRM (Directory Services Restore Mode)
- Редактор свойств учетной записи
- Редактор политики паролей
- Поиск ключей шифрования BitLocker
- Дамп (экспорт) парольных хэшей
- Откат сделанных ранее изменений

Кэшированные записи доменна (DCC)
- Сброс или изменение пароля пользователя
- Дамп (экспорт) парольных хэшей
- Откат сделанных ранее изменений

Пароли
- Поиск паролей локальных учетных пользователей
- Поиск паролей доменных учетных записей
- Поиск паролей кэшированных записей домена
- Расшифровка биометрических паролей Windows Hello
- Восстановление PIN-кодов
- Поиск пароля SYSKEY
- Поиск паролей виртуальных машин
- Поиск и восстановление паролей к зашифрованным документам
- Поиск сетевых, почтовых и интернет паролей
- Поиск серийных номеров и регистрационных ключей

Активность пользователя
- Последняя активность пользователя
- Журнал и статистика учетных записей
- История оборудования
- История установки программ
- История сетевых соединений
- Поиск последних открываемых документов
- История Интернет активности пользователя
- История IP адресов пользователей

Криминалистический анализ
- История запуска программ
- Временная шкала активности Windows
- Анализ Windows Media
- Записки Windows
- Отслеживание доступа к камере и микрофону
- История буфера обмена
- История корзины
- История USB
- Монитор использования системных ресурсов
- Обозреватель баз данных Windows Search
- Удаленный рабочий стол
- Системные события Windows
- Расшифровщик Telegram

Файлы и диски
- Создание образа диска
- Загрузка дополнительных драйверов IDE/SATA/SCSI/RAID
- Расшифровка дисков, зашифрованных Bitlocker
- Монтирование виртуального диска
- Скрытые тома и разделы
- Последние измененные файлы
- Последние измененные папки
- Калькулятор контрольной суммы или хэша
- Поиск дубликатов файлов
- Удаление ненужных файлов и очистка реестра
- Анализ диского пространства
- Анализ файлов и папок
- Быстрый поиск на диске

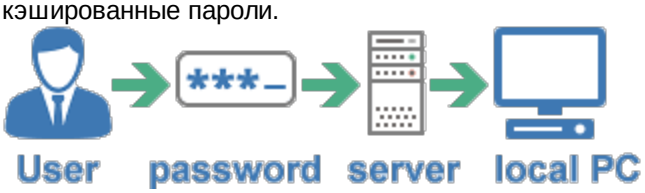
Утилиты
- Поиск зашифрованных документов
- Резервное копирование паролей и конфиденциальной информации
- Удаление приватной информации пользователя
- Подключение сетевых дисков
- Обозреватель баз данных ESE (Extensible Storage Engine)
- Просмотр баз данных SQLite
- Журнал состояния загрузки ОС

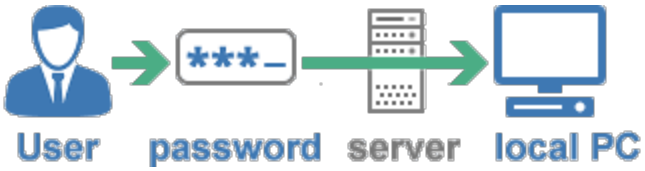
Схематичное описание типов учетных записей

SAM
Учетные записи обычного домашнего пользователя ПК. Пароли хранятся в файле реестра SAM на этом же компьютере.

ACTIVE DIRECTORY
Учетные записи пользователей домена. Пароли хранятся в базе данных NTDS.DIT на доменном ПК.

DCC
Учетные записи пользователей домена. Кэшированные пароли могут храниться на локальном ПК. Вход в учетную запись производится либо через домен, либо, если домен недоступен, используются кэшированные пароли.

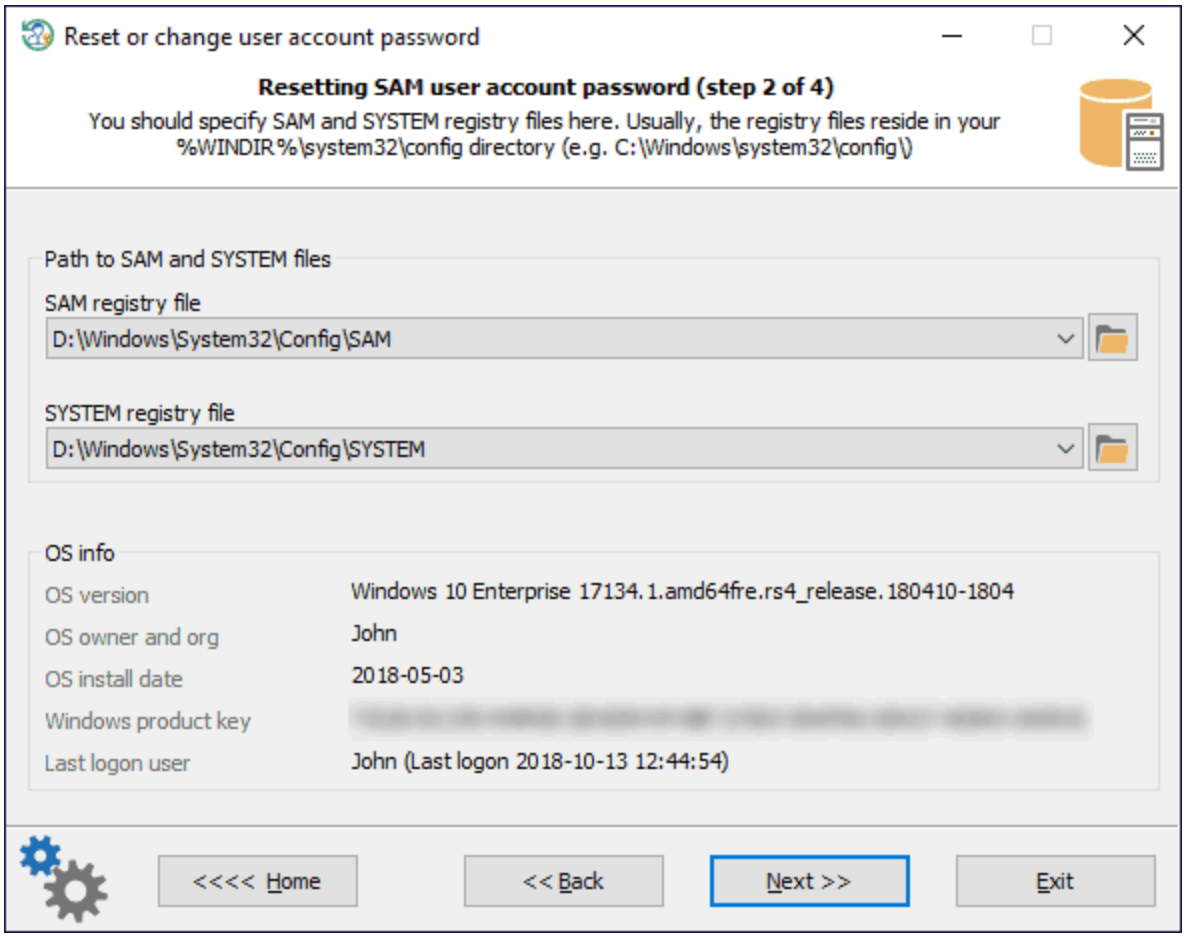




3.2 Локальные учетные записи

3.2.1 Сброс или изменение пароля пользователя

Выбор источника данных

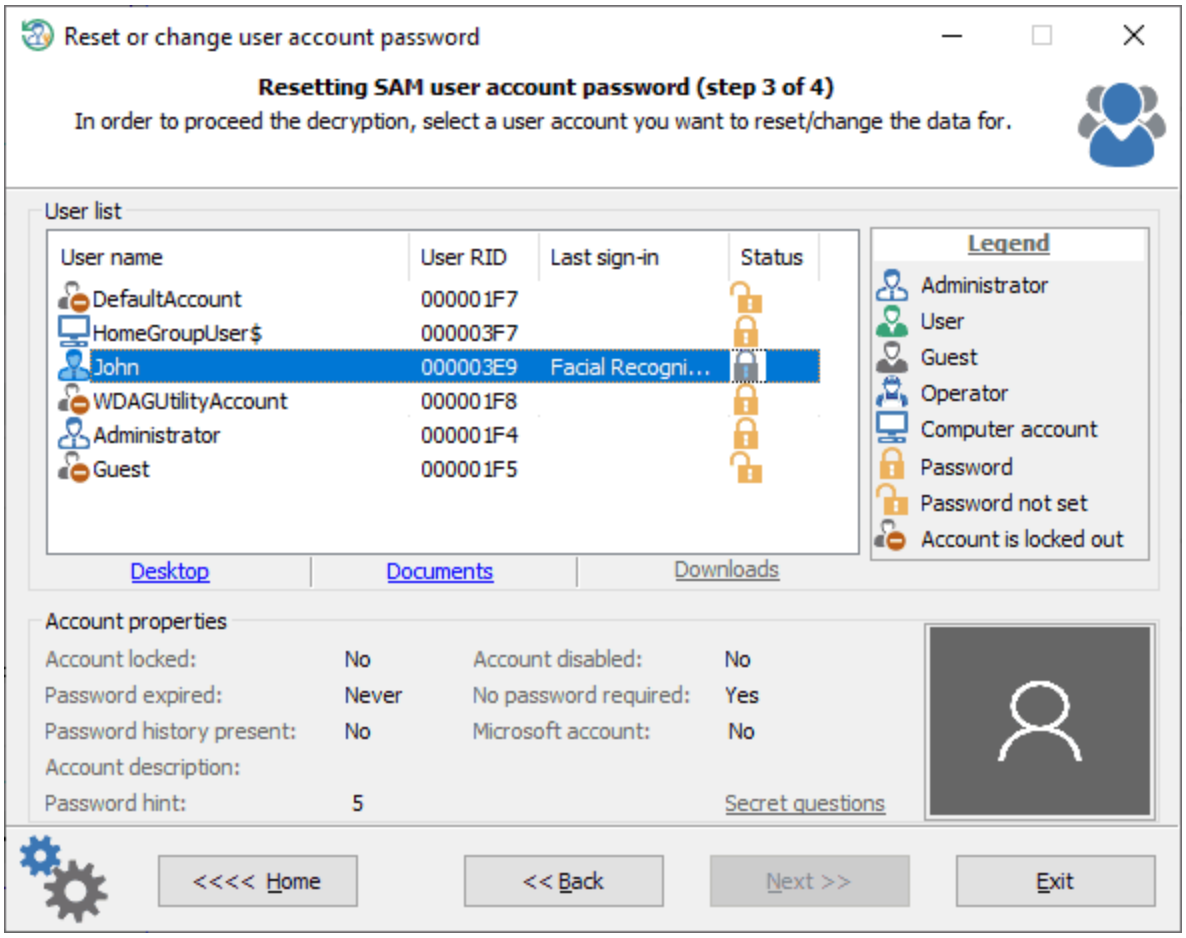


Чтобы сбросить пароль обычный учетной записи, вы должны указать два файла реестра: **SAM** и **SYSTEM**. Приложение автоматически производит поиск и предлагает на выбор подходящие файлы. Файлы реестра находятся в каталоге **%WINDIR%\system32\config**. Где %WINDIR% - каталог Windows.

Если во время предыдущего шага был выбран режим Active Directory, то вместо файла SAM необходимо установить местоположение базы данных Active Directory. По умолчанию это папка **%WINDIR%\NTDS**. Таким образом, полный путь к базе данных Active Directory может выглядеть так: C:\Windows\NTDS\ntds.dit

Группа *OS Info* показывает версию найденной Операционной Системы и дату установки, владельца системы, последнего входившего пользователя и найденный ключ продукта Windows.

Выбор учетной записи

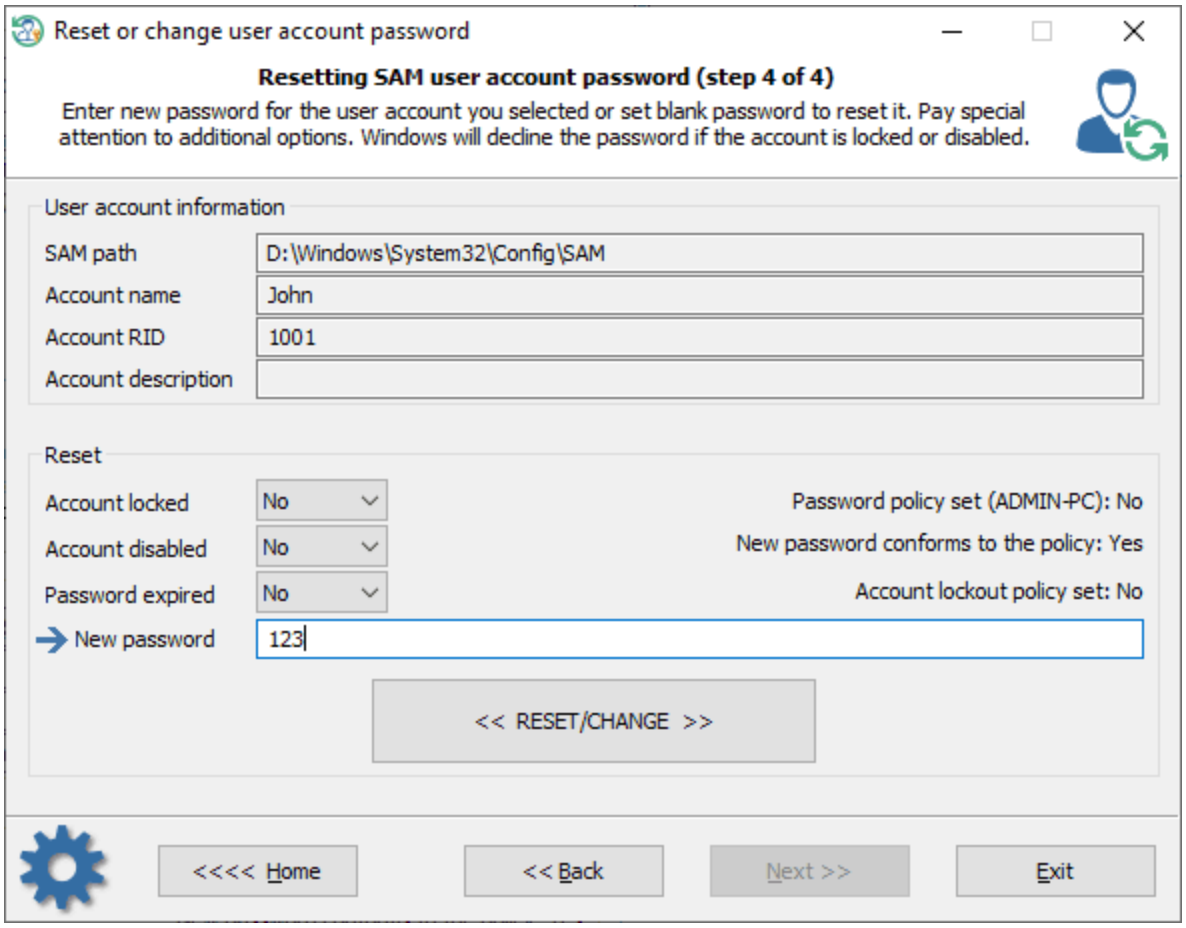


Верхняя часть диалога отображает список найденных пользователей, их статус и тип последнего входа в систему. Выделив один из них, можно просмотреть свойства этой учетной записи. А именно: является ли учетная запись заблокированной или отключенной, требуется ли пароль на вход, хранится ли история ранее введенных паролей, имеется ли подсказки о пароле и т.д.

Можно также открыть рабочий стол, папку с документами или закачками выбранного пользователя.

В Windows 10 v17063 появились так называемые секретные вопросы, которые служат для дополнительной защиты локальных учетных записей от несанкционированной смены пароля. Reset Windows Password может успешно вытаскивать и отображать секретные вопросы

Сброс пароля



Для сброса, оставьте поле ввода 'Новый пароль' пустым и нажмите на кнопку 'Сброс/Смена'. Обратите внимание на дополнительные опции. Учетная запись не должна быть заблокированной, отключенной, срок действия пароля не должен быть истекшим.

Если в системе использовалась локальная или доменная политика паролей, убедитесь, что новый пароль соответствует требованиям длины и сложности и не совпадает ни с одним из введенных ранее паролей (если присутствует история паролей). В противном случае, система может отказать в доступе, даже если пароль был успешно сброшен или изменен.

При сбросе пароля встроенного Администратора, имейте в виду, в некоторых версиях Windows для активации и входа под этой встроенной учетной записью, потребуется выполнить загрузку системы в безопасном режиме. Чтобы сделать это, перед запуском Windows, нажимайте клавишу F8 до тех пор, пока не появится текстовое окно с выбором способа загрузки системы. В этом окне выберите безопасный режим. После этого, встроенная учетная запись Администратора станет активной, и вы сможете использовать ее для входа в систему.

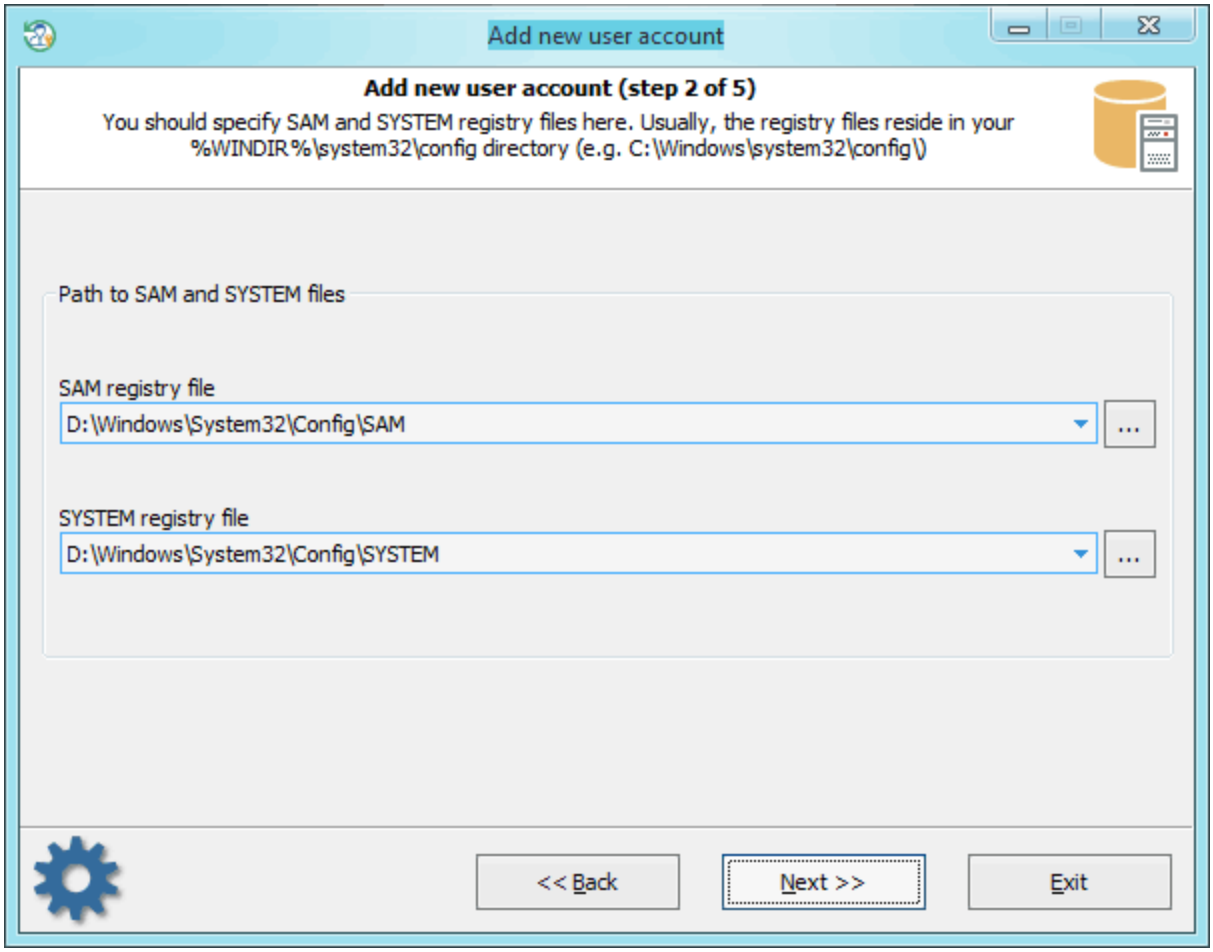
На операционных системах Windows 8 и более новых, для запуска безопасного режима нажмите кнопку выключения компьютера, затем нажмите удерживая клавишу Shift на клавиатуре и выберите пункт 'Перезагрузка'.

Обратите внимание, для входа в учетную запись Microsoft, надо задать непустой пароль.

3.2.2 Создание новой учетной записи

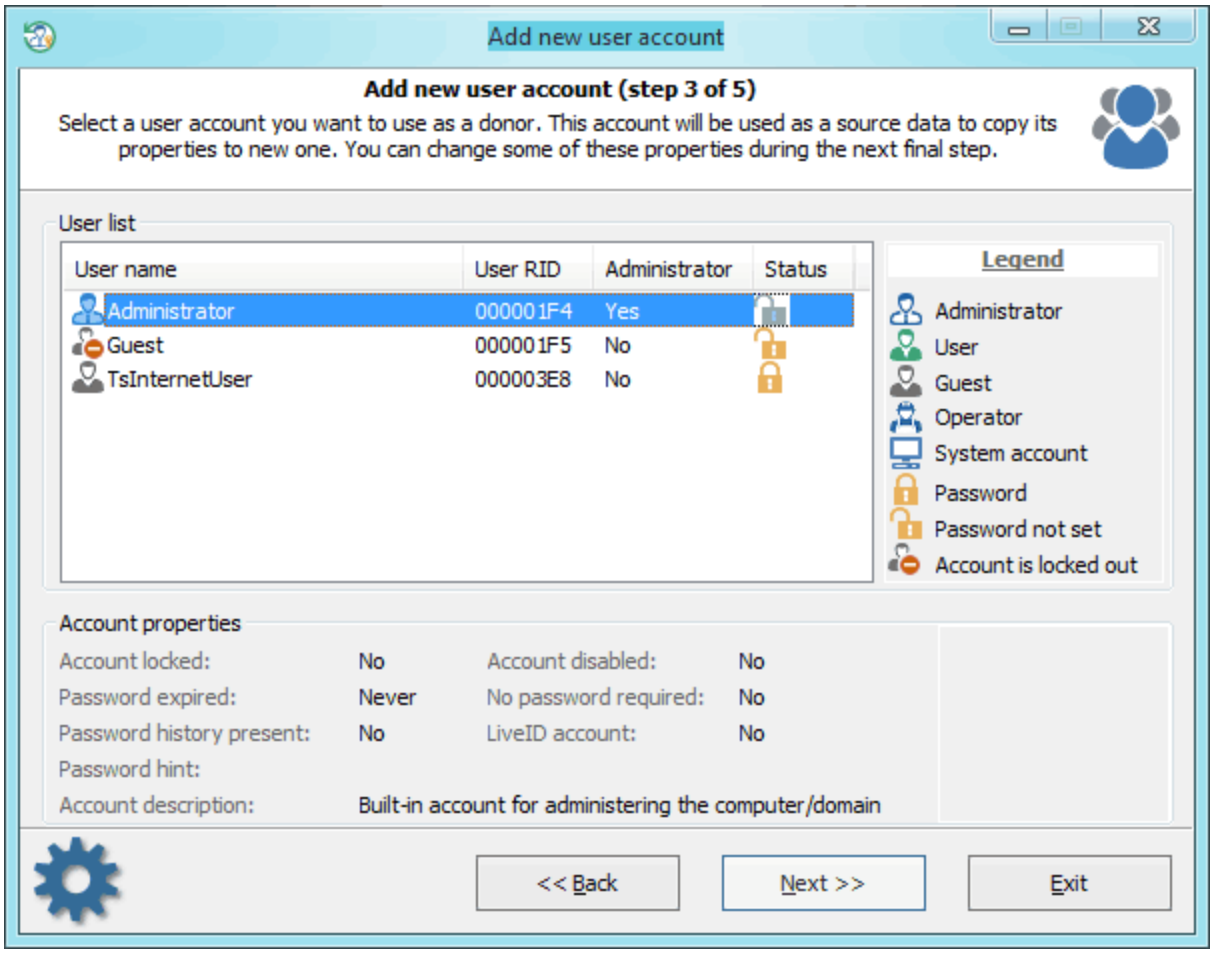
Добавить новую учетную запись очень просто. Мы постарались организовать этот процесс в обычные 3 шага.

1. Выбор источника данных



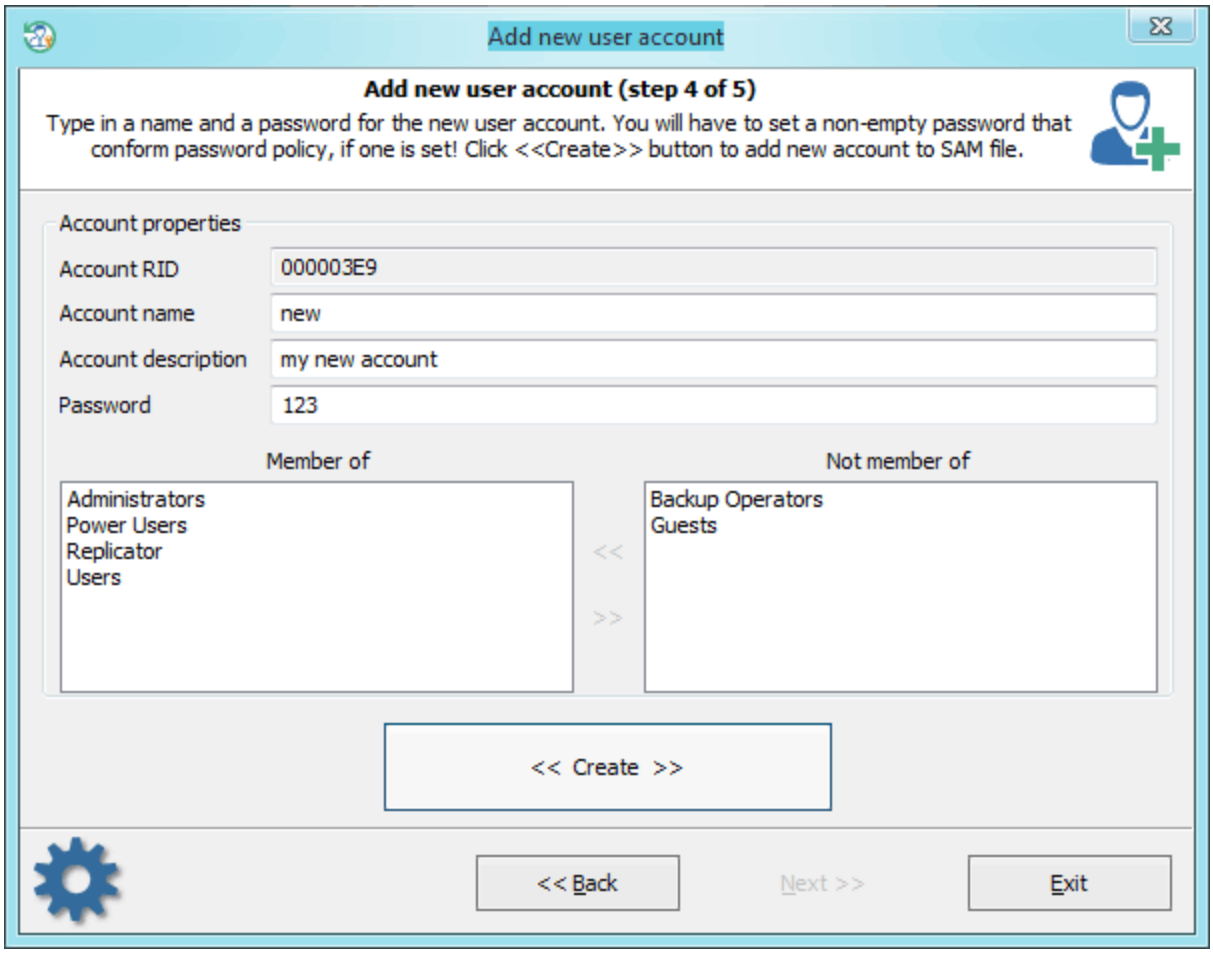
На начальном этапе необходимо выбрать файлы **SAM** и **SYSTEM**. Программа производит поиск и предлагает эти файлы автоматически. В случае, если необходимо выбрать их вручную, знайте, что эти файлы реестра находятся в каталоге **%WINDIR%\system32\config**.

2. Выбор донорской учетной записи



Выберите пользователя, чья учетная запись будет использована в качестве донора. Все свойства исходной, донорской учетной записи будут скопированы в новую. Не проблема, если исходный аккаунт заблокирован или отключен. Программа изменит критические свойства и установит соответствующие флаги. Например, если исходной учетке разрешено входить в систему только в определенные часы, Reset Windows Password, отключит это ограничение для новой учетной записи.

3. Добавление новой учетной записи



Теперь все что вам нужно, это задать какое-либо имя, описание и пароль для новой учетной записи. Можно оставить поле пароля пустым. Однако, учтите, если в системе установлена политика паролей, то необходимо задать пароль, который подходит требованиям этой политики.

Особое внимание уделите заданию правильного членства в группах. Как правило, новая учетная запись должны быть членом группы 'Администраторы' и/или 'Пользователи', если иное не определено политикой безопасности операционной системы. Установка неправильного членства может привести к некоторым сложностям, например, при удалении этой учетной записи.

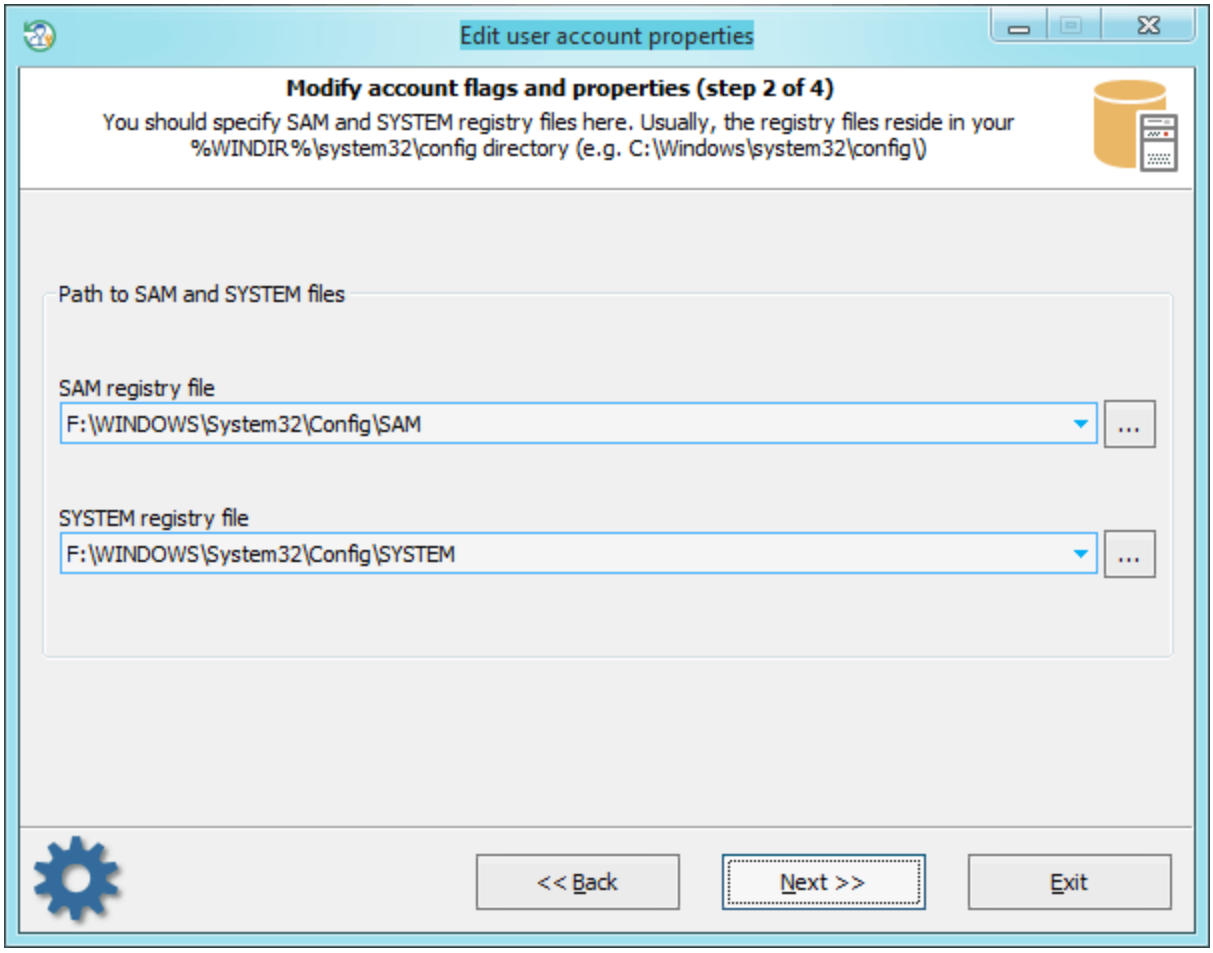
После того, как учетная запись успешно создана, можно вернуться в главный диалог, выбрать режим редактирования свойств учетной записи и установить или сбросить некоторые расширенные флаги, если это требуется.

3.2.3 Редактор свойств учетной записи

Reset Windows Password позволяет манипулировать расширенными свойствами выбранной учетной записи пользователя, а также менять учетную запись Microsoft на локальную и наоборот. Это бывает чрезвычайно полезно, если необходимо быстро разблокировать/включить заблокированную или отключенную учетную

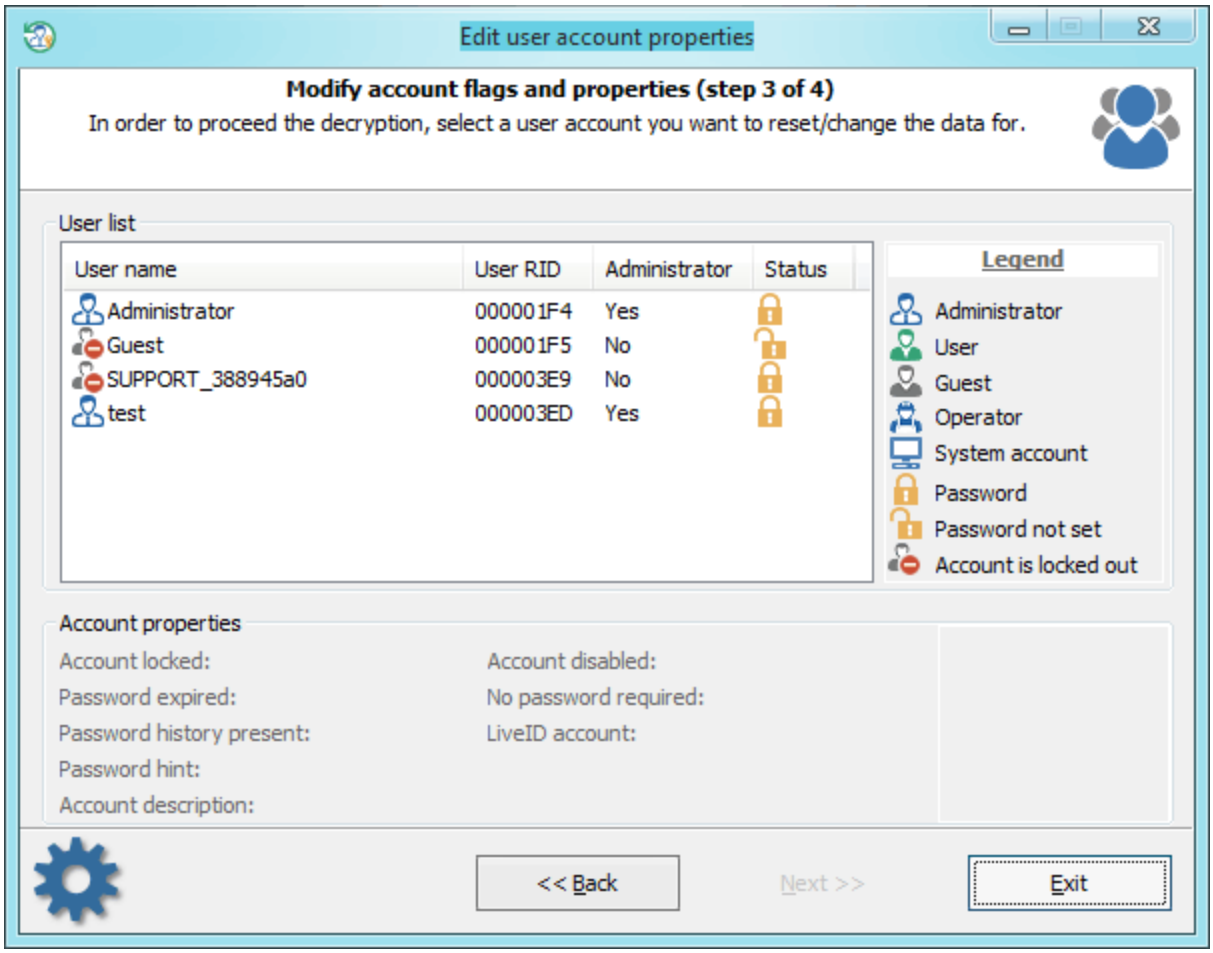
запись, сбросить флаг 'Вышел срок действия пароля', отключить вход при помощи Smart-карты, например, когда она утеряна и т.д. Изменить проблемную учетную запись довольно просто. Сначала необходимо выбрать файлы операционной системы.

Выбор источника данных



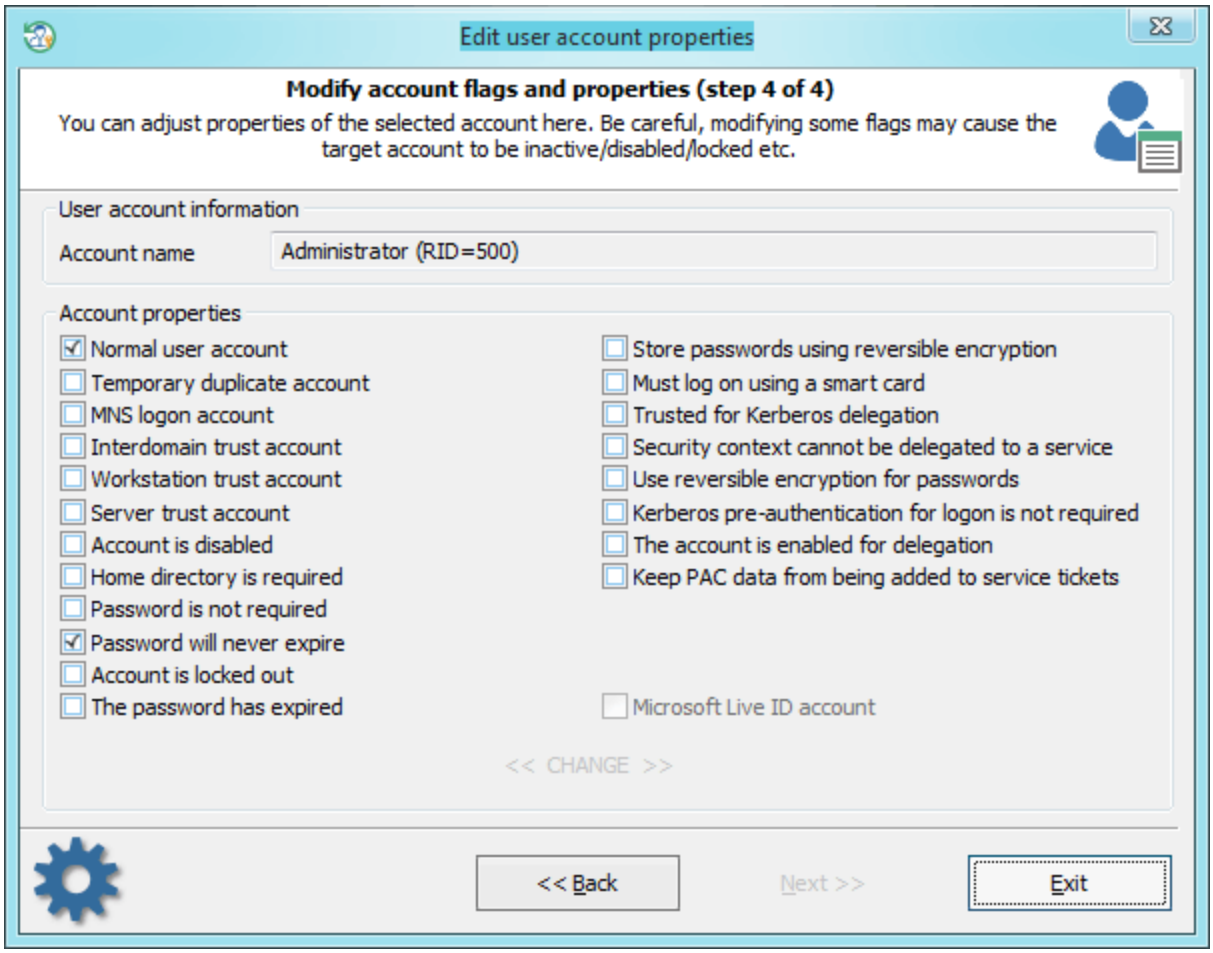
Программе требуется два файла. Это либо **SAM** и **SYSTEM** (в случае с локальными учетными записями) или **NTDS.DIT** и **SYSTEM** (когда необходимо изменить свойства пользователя домена). RWP автоматически производит поиск этих файлов. Но можно также указать путь к ним вручную. Они находятся в каталогах **%WINDIR%\system32\config** и **%WINDIR%\NTDS**. Где %WINDIR% - каталог Windows. Полный путь к базе Active Directory может выглядеть так: C:\Windows\NTDS\ntds.dit

Выбор учетной записи Windows



После того, как исходные файлы выбраны, программа отображает список найденных учетных записей. Выберите интересуемую вас и нажмите кнопку 'Далее', чтобы открыть финальный диалог со ее свойствами.

Изменение свойств учетной записи



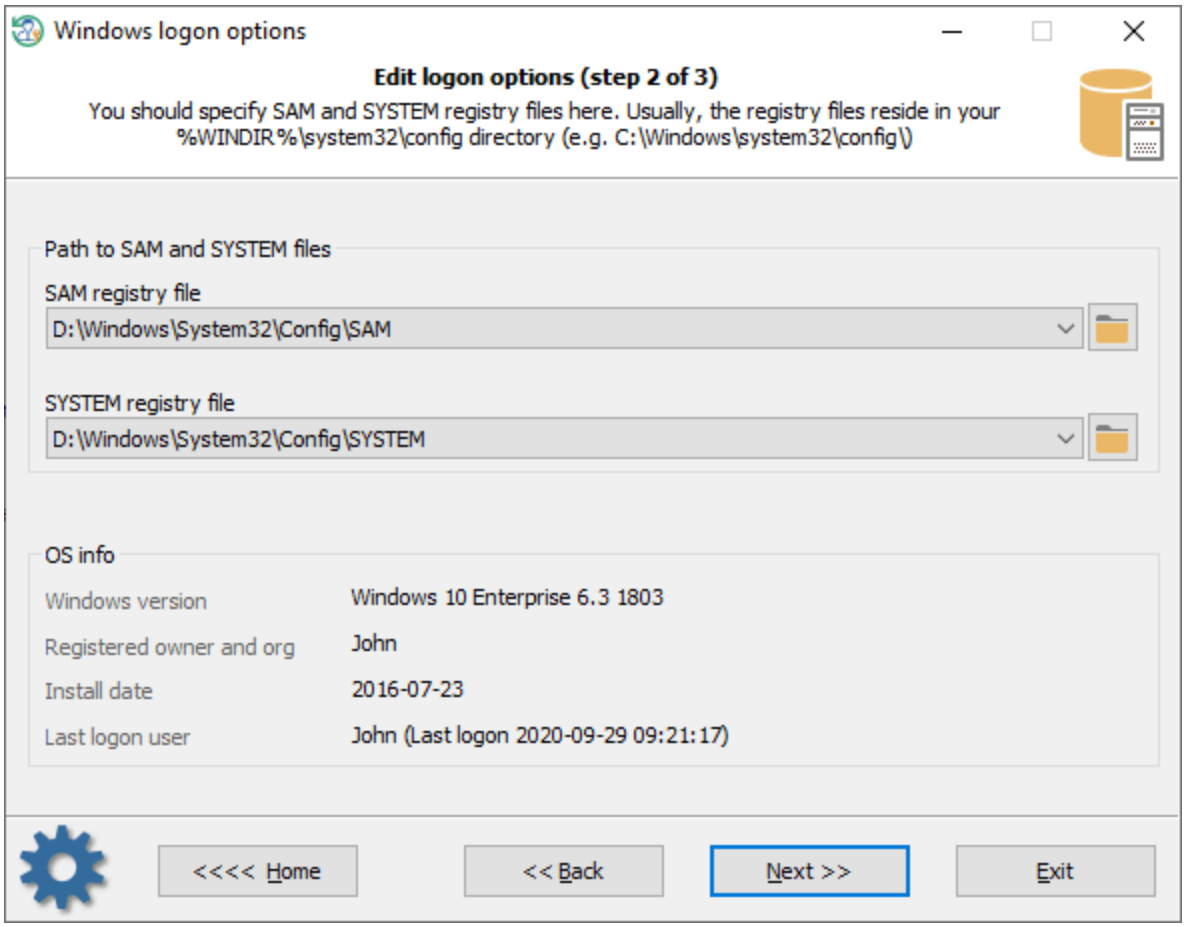
Здесь вы можете устанавливать/сбрасывать разные флаги, управляющие поведением учетной записи.

Будьте осторожны, изменение некоторых свойств может привести к тому, что учетная запись окажется заблокированной, отключенной и т.д.

3.2.4 Редактор настроек входа в систему

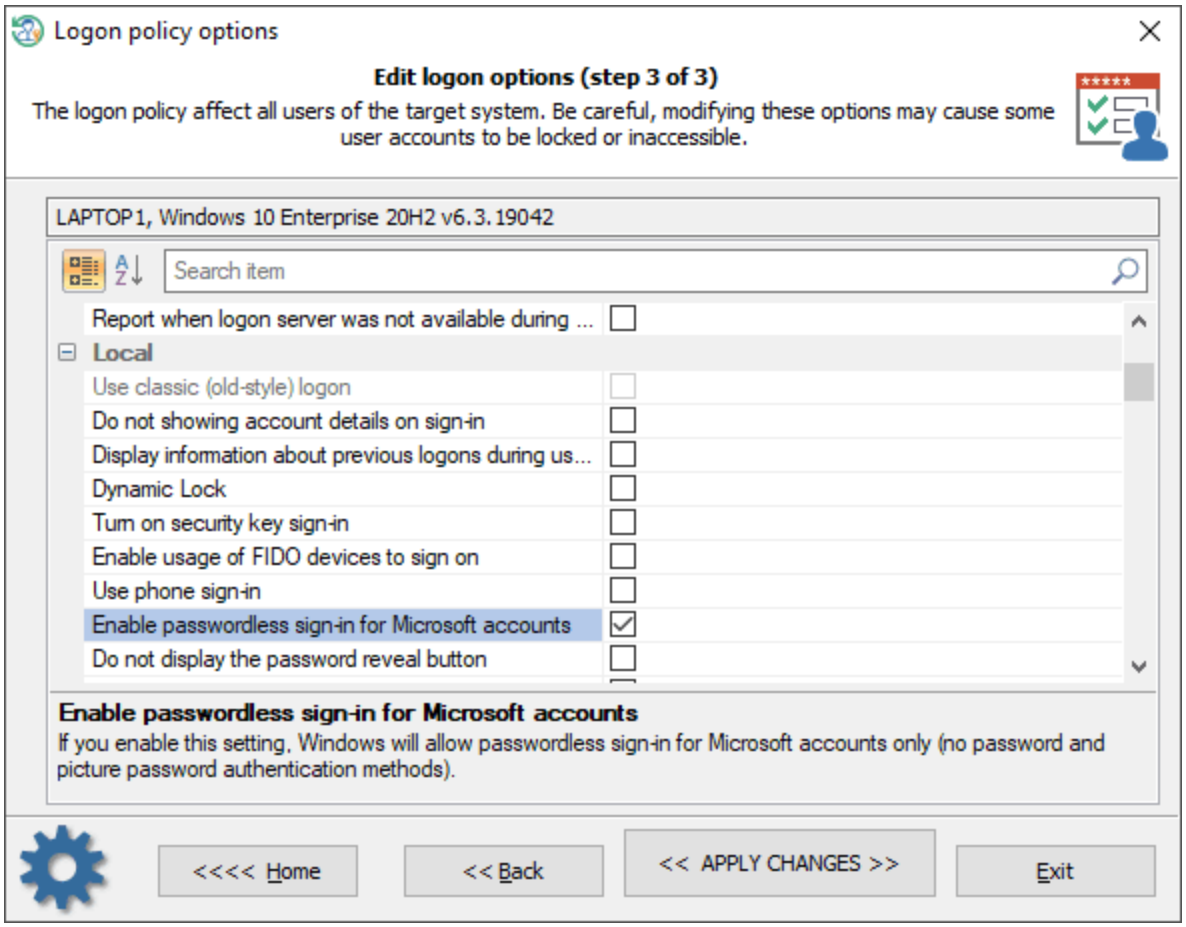
Эти настройки можно использовать чтобы изменить способ входа пользователей в операционную систему. Например, отображать имя последнего пользователя системы, назначить домен входа по умолчанию, включить/отключить вход без пароля и т.д.

Выбор источника данных



Сначала необходимо выбрать файлы реестра SAM и SYSTEM или указать путь к ним вручную, если программа не смогла обнаружить их автоматически.

Изменение параметров входа в систему



После выбора файлов можно приступать к изменению необходимых настроек. Нажмите кнопку << СОХР. ИЗМЕНЕНИЯ >> чтобы применить и сохранить сделанные изменения. Параметры входа влияют на всех локальных пользователей системы.

Будьте осторожны, изменение определенных параметров может привести к недоступности некоторых учетных записей.

Краткое описание настроек входа.

Настройки группы **Domain**:

Имя	Описание
Разрешает пользователям выбирать, необходим ли ввод пароля при возобновлении работы из режима ожидания с подключением	Этот параметр позволяет управлять возможностью изменения пользователем промежутка времени до необходимости ввода пароля в случае, когда экран устройства, поддерживающего режим ожидания с подключением, выключается. Если включить этот параметр, пользователь устройства, поддерживающего режим ожидания с подключением, сможет настраивать промежуток времени после выключения экрана устройства до необходимости ввода пароля при пробуждении устройства. Этот промежуток ограничивается любыми параметрами EAS или групповыми политиками, которые влияют на максимальное время простоя до блокировки устройства. Кроме того, если требуется ввести пароль при включении заставки, время ожидания заставки ограничивает доступные пользователю варианты.

Домен, используемый по умолчанию, для входа	Домен для входа, который будет использоваться по умолчанию. Он может отличаться от домена, к которому принадлежит компьютер.
Не перечислять подключенных пользователей на компьютерах, подключенных к домену.	Если этот параметр включен, пользовательский интерфейс входа в систему не перечисляет подключенных пользователей на компьютерах, подключенных к домену.
Перечислить локальных пользователей на компьютерах, подключенных к домену	Если этот параметр включен, пользовательский интерфейс входа в систему будет перечислять всех локальных пользователей на компьютерах, подключенных к домену.
Выключить вход с графическим паролем	Если этот параметр включен, то пользователь домена может настроить графический пароль и выполнять вход с его помощью.
Включить вход с помощью удобного ПИН-кода	Когда этот параметр включен, пользователь домена может настраивать удобный PIN-код и использовать его для входа.
Сообщать, когда сервер входа недоступен при входе пользователя	Если этот параметр включен, выводится всплывающее уведомление о том, что вход пользователя выполнен с кэшированными учетными данными.

Настройки группы **Local**:

Имя	**Описание**
Использовать классический вход в систему	Всегда использовать классическую (старую) схему входа в систему.
Запретить пользователю отображать данные учетной записи на экране входа	Если этот параметр включен, пользователь не может отображать данные учетной записи на экране входа.
Отображать при входе пользователя сведения о предыдущих попытках входа	Если этот параметр включен, то после входа пользователя появляется сообщение, содержащее дату и время последнего успешного входа этого пользователя, дату и время последней неудачной попытки входа с этим именем пользователя и число неудачных попыток после последнего успешного входа этого пользователя.
Настроить динамическую блокировку	Если этот параметр включен, Windows включает динамическую блокировку для всех пользователей на управляемых устройствах и пользователи не могут отключать ее в своих учетных записях.
Включить вход с ключом безопасности	Если этот параметр включен, пользователи могут входить с помощью внешних ключей безопасности.
Включить использование устройств FIDO для входа	Если этот параметр включен, пользователи могут входить в Windows с помощью устройства FIDO.
Использовать функцию входа на телефоне	Если этот параметр включен, функция входа на телефоне будет включена и телефон можно будет использовать в качестве вспомогательного устройства для проверки подлинности на настольном устройстве.
Включить беспарольный вход для учетных записей Microsoft	Если вы включите этот параметр, Windows разрешит только вход без пароля: оба метода проверки подлинности по паролю и по изображению будут отключены. Этот параметр влияет только на учетные записи Майкрософт.
Не показывать кнопку отображения пароля	Если этот параметр включен, кнопка отображения пароля не будет видна после ввода пользователем пароля в окне ввода пароля.
Предотвращение использования контрольных вопросов	Если этот параметр включен, локальные пользователи не смогут настраивать и использовать контрольные вопросы, чтобы сбрасывать пароли.

для локальных учетных записей	
Разрешить использовать вспомогательное устройство для дополнительной проверки подлинности	Эта настройка позволяет пользователям использовать вспомогательное устройство (например, телефон, фитнес-браслет или устройство IoT) для входа в настольный компьютер под управлением Windows 10. Если этот параметр включен или не настроен, пользователи могут проходить проверку подлинности в Windows Hello с помощью вспомогательного устройства.
азрешить программам использование специального сочетания клавиш	Этот параметр определяет, может ли программное обеспечение имитировать специальное сочетание клавиш (SAS).
Настройка автоматического входа и блокировки последнего пользователя после перезагрузки	Этот параметр управляет конфигурацией, в которой автоматическая перезагрузка и вход с блокировкой происходят после перезагрузки или холодной загрузки.
Автоматически выполнять вход и блокировать последнего текущего пользователя после перезагрузки	Этот параметр указывает, будет ли устройство автоматически выполнять вход и блокировку последнего текущего пользователя после перезагрузки или после завершения работы и холодной загрузки. Это происходит, только если последний текущий пользователь не выполнил выход перед перезагрузкой или завершением работы.

Настройки группы **Misc**:

Имя	**Описание**
Всегда использовать настраиваемый фон входа в систему	Если этот параметр включен, экран входа в систему всегда будет пытаться загружать настраиваемый фон вместо фирменного фона входа в Windows.
Показывать прозрачный экран входа в систему	Если включить этот параметр, фоновый рисунок входа будет отображаться без размытия.
Не показывать экран приветствия «Приступая к работе» при входе в систему	Если этот параметр включен, экран приветствия не виден пользователю, выполняющему вход в систему на компьютере, на котором применяется эта политика. Пользователи по-прежнему могут просмотреть экран приветствия, выбрав его в меню «Пуск» или введя Welcome в диалоговом окне «Выполнить».
Отключить уведомления приложений на экране блокировки	Если этот параметр включен, уведомления приложений не будут отображаться на экране блокировки.
Показать анимацию при первом входе в систему	Если вы включаете этот параметр, пользователи с учетными записями Майкрософт будут получать запрос на использование служб, а для пользователей с другими учетными записями будет отображаться анимация при входе в систему.
Отключить звук запуска Windows	Отключить звук запуска Windows во время входа.
Не обрабатывать список запуска старых программ	Если этот параметр включен, система игнорирует список запуска для Windows Vista, Windows XP Professional и Windows 2000 Professional.
Не обрабатывать список однократного запуска программ	Если этот параметр включен, система игнорирует список программ, выполняемых единожды.
Скрыть точки входа для быстрого переключения пользователей	Если вы включите этот параметр, интерфейс «Сменить пользователя» скрыт от пользователя, выполняющего вход или выход из системы на компьютере, на котором применяется этот параметр. Интерфейс «Сменить пользователя»

	появляется в следующих расположениях: пользовательский интерфейс входа в систему, меню кнопки «Пуск» и диспетчер задач.
Блокировать проверку подлинности всех потребителей учетной записи пользователя Майкрософт	Этот параметр определяет, могут ли пользователи указывать учетные записи Майкрософт для проверки подлинности в приложениях или службах. Если этот параметр включен, всем приложениям и службам на устройстве запрещается использовать учетные записи Майкрософт для проверки подлинности.
Назначить стандартного поставщика учетных данных	Если этот параметр включен, указанный поставщик учетных данных выбирается на плитке "Другой пользователь".
Исключить поставщиков учетных данных	Если этот параметр включен, администратор сможет указать коды CLSID поставщиков учетных данных, чтобы исключить их из списка установленных поставщиков учетных данных, доступных для проверки подлинности.

Настройки группы **Network**:

Имя	Описание
Всегда ждать сеть при запуске и входе в систему	Этот параметр определяет, является ли обработка групповых политик синхронной (то есть должны ли компьютеры ждать завершения полной инициализации сети при запуске компьютера и входе пользователя в систему). По умолчанию на клиентских компьютерах обработка групповых политик происходит не синхронно, клиентские компьютеры обычно не ждут завершения полной инициализации сети при запуске и входе пользователя в систему. Существующие пользователи входят в систему, используя кэшированные учетные данные, что сокращает время входа в систему. Групповые политики применяются фоновым процессом, когда сеть становится доступной.
Не отображать пользовательский интерфейс выбора сети	Если вы включаете этот параметр, то состояние сетевого подключения компьютера нельзя изменить без входа в Windows.

Настройки группы **Biometrics**:

Имя	Описание
Разрешение пользователям домена выполнять вход в систему с использованием биометрии	Этот параметр определяет, могут ли пользователи с учетной записью домена выполнять вход с использованием биометрии или использовать биометрию для повышения уровня разрешений контроля учетных записей (UAC). Если включить этот параметр, Windows позволит пользователям домена использовать биометрию для входа в систему на компьютере, подключенном к домену.
Разрешение пользователям выполнять вход в систему с использованием биометрии	Если вы включаете или не настраиваете этот параметр, все пользователи смогут выполнять вход в систему на локальном компьютере под управлением Windows, а также смогут использовать биометрию для повышения уровня разрешений с помощью контроля учетных записей (UAC).
Разрешение использования биометрии	Если вы включаете или не настраиваете этот параметр, биометрическая служба Windows доступна и пользователи смогут запускать приложения, использующие биометрию в Windows. Если вы хотите включить функцию входа в систему с использованием биометрии, вам потребуется дополнительно настроить параметр «Разрешить пользователям выполнять вход в систему с использованием биометрии».
Настройка расширенной защиты от подделывания	Если этот параметр включен, Windows требует от всех пользователей на управляемых устройствах использовать расширенную защиту от подделывания для проверки подлинности с помощью распознавания лиц Windows Hello. Это

	действие отключает проверку подлинности с помощью распознавания лиц Windows Hello на устройствах, не поддерживающих расширенную защиту от подделывания.
Время ожидания для событий функции быстрого переключения пользователей	Если этот параметр включен, можно задать время ожидания события функции быстрого переключения пользователей, чтобы указать интервал времени, в течение которого событие будет активным. Значение не может превышать 60 секунд.

Настройки группы **PIN**:

Имя	Описание
Срок действия PIN	Этот параметр указывает период времени (в днях), когда PIN-код может использоваться до того, как система потребует от пользователя изменить его. Можно задать, чтобы срок действия PIN-кода истекал через любое количество дней в диапазоне от 1 до 730, или можно задать, чтобы срок действия PIN-кода никогда не истекал, если для параметра установлено значение 0.
Журнал PIN	Этот параметр указывает количество предыдущих PIN-кодов, связанных с учетной записью пользователя, которые нельзя повторно использовать. Значение должно быть в диапазоне от 0 до 50 PIN-кодов.
Максимальная длина PIN-кода	Максимальное число символов в PIN-коде. Максимальное число, которое можно выбрать при настройке этого параметра, — 127.
Минимальная длина PIN-кода	Устанавливает минимальное число символов в PIN-коде. Минимальное число, которое можно выбрать при настройке этого параметра, — 4.
Требовать использование цифр	Если этот параметр включен, Windows будет требовать, чтобы пользователь включил в PIN-код по крайней мере одну цифру.
Требовать использование строчных букв	Если этот параметр включен, Windows будет требовать, чтобы пользователь включил в PIN-код по крайней мере одну строчную букву.
Требовать использование специальных символов	Если этот параметр включен, Windows будет требовать, чтобы пользователь включил в PIN-код по крайней мере один специальный символ.
Требовать использование прописных букв	Если этот параметр включен, Windows будет требовать, чтобы пользователь включил в PIN-код по крайней мере одну прописную букву.

Настройки группы **Windows Hello**:

Имя	Описание
Разрешить перечисление эмулированной смарт-карты для всех пользователей	Windows не дает пользователям на одном и том же компьютере перечислять для других пользователей подготовленные учетные данные Windows Hello для бизнеса. Если включить этот параметр, Windows разрешает всем пользователям компьютера перечислять все учетные данные Windows Hello для бизнеса, но все равно требует от каждого пользователя предоставлять собственные факторы проверки подлинности.
Первый фактор разблокировки поставщиков учетных данных	Первый фактор разблокировки поставщиков учетных данных
Второй фактор разблокировки поставщиков учетных данных	Второй фактор разблокировки поставщиков учетных данных.
Сигнальные правила для разблокировки устройства	Сигнальные правила для разблокировки устройства.

Настройка динамических факторов разблокировки	Настройка разделенного запятыми списка сигнальных правил в форме XML-файла для каждого типа сигнала. Если включить этот параметр, эти сигнальные правила будут проверяться для определения отсутствия пользователя и автоматической блокировки устройства.
Правила для динамической блокировки	Сигнальные правила для динамической блокировки.
Выключить эмуляцию смарт-карт	Если включить этот параметр, Windows Hello для бизнеса подготавливает учетные данные, не совместимые с приложениями, которые поддерживают смарт-карты.
Использование устройства аппаратной защиты	При включении этого параметра подготовка Windows Hello для бизнеса происходит только на устройствах с доступными для использования доверенными платформенными модулями версии 1.2 или 2.0. При необходимости можно исключить устройства безопасности, в результате чего при подготовке Windows Hello для бизнеса не будут использоваться эти устройства.
Не следует использовать устройства безопасности TPM1.2	Не следует использовать следующие устройства безопасности: TPM 1.2
Использование биометрии	Если этот параметр включен или не настроен, Windows Hello для бизнеса разрешит использование биометрических функций.
Использовать сертификат для локальной проверки подлинности	При включении этого параметра Windows Hello для бизнеса регистрирует сертификат входа, используемый для локальной проверки подлинности.
Использовать функцию восстановления PIN-кода	Если включить этот параметр, служба Windows Hello для бизнеса будет использовать службу восстановления PIN-кода.
Использовать сертификаты Windows Hello для бизнеса в качестве сертификатов смарт-карт	Если этот параметр отключен или не задан, сертификаты Windows Hello для бизнеса не будут использоваться в качестве сертификатов смарт-карт при использовании приложениями, а биометрические факторы будут доступны, когда пользователю будет предложено авторизовать использование закрытого ключа сертификата.
Использовать Windows Hello для бизнеса	Если этот параметр включен, устройство предоставит возможность использования Windows Hello для бизнеса с использованием ключей или сертификатов всем пользователям. Если этот параметр не настроен, пользователи смогут использовать Windows Hello для бизнеса, благодаря чему будет зашифрован их пароль в домене.
Не запускать подготовку Windows Hello после входа	Если вы выберете "Не запускать подготовку Windows Hello после входа", Windows Hello для бизнеса не будет автоматически начинать подготовку после того, как пользователь войдет.

Настройки группы **TPM**:

Имя	**Описание**
Уровень сведений авторизации владельца TMP, доступных операционной системе	Этот параметр определяет, сколько сведений об авторизации владельца доверенного платформенного модуля хранится в реестре локального компьютера. В зависимости от того, какая часть сведений об авторизации владельца доверенного платформенного модуля хранится локально, операционная система и приложения, основанные на использовании доверенного платформенного модуля, могут выполнять его определенные действия, требующие авторизации владельца этого модуля, без необходимости ввода пароля. Вы можете выбирать между хранением в операционной системе полного значения авторизации владельца доверенного платформенного модуля, больших двоичных объектов делегирования административных полномочий и делегирования пользовательских полномочий доверенного платформенного

	модуля или ни одного из перечисленных элементов. Если этот параметр включен, то Windows сохраняет сведения об авторизации владельца доверенного платформенного модуля в реестре локального компьютера в соответствии с выбранным вами параметром проверки подлинности доверенного платформенного модуля, управляемым операционной системой.
Настройте систему на очистку TPM, если он не находится в состоянии готовности	Этот параметр настраивает систему на то, чтобы указывать пользователю на необходимость очистки TPM, если обнаруживается, что TPM находится в любом состоянии, отличном от готовности. Данная политика вступит в действие только, если TPM системы будет в состоянии, отличном от готовности, в том числе в тех случаях, когда TPM будет находиться в режиме "Готов, с ограниченной функциональностью". Подсказка относительно очистки TPM будет отображаться после следующей перезагрузки после входа пользователя в систему, только если последний будет являться частью группы "Администраторы" для системы. Подсказку можно отменить, но она будет отображаться после каждой перезагрузки и входа, пока не будет отключена политика или TPM не перейдет в состояние Готовности.
Настройте для системы использование унаследованных параметров защиты от атак на словари для доверенного платформенного модуля 2.0	Этот параметр настраивает доверенный платформенный модуль на использование параметров защиты от атак перебором по словарю (пороговое значение блокировки и время восстановления) со значениями, которые использовались в Windows 10 версии 1607 и ниже. Настройка этой политики вступит в силу, только если а) доверенный платформенный модуль был изначально подготовлен с использованием более поздней версии Windows, чем Windows 10 версии 1607 и б) система использует доверенный платформенный модуль версии 2.0. Обратите внимание, что включение политики вступит в силу только после выполнения задачи по обслуживанию доверенного платформенного модуля (обычно это происходит после перезапуска системы). После включения этой политики в системе и ее вступления в силу (после перезапуска системы) ее отключение не будет иметь эффекта и доверенный платформенный модуль системы останется настроенным с использованием унаследованных параметров защиты от атак перебором по словарю, независимо от значения этой групповой политики. Отключить эту политику в системе, где она однажды была включена, можно только двумя способами: а) отключить ее в групповой политике и б) очистить доверенный платформенный модуль в системе.
Игнорировать список заблокированных команд TPM по умолчанию	Если этот параметр включен, то Windows игнорирует список заблокированных команд доверенного платформенного модуля, определенный по умолчанию, и блокирует только те команды доверенного платформенного модуля, которые указаны групповой политикой или в локальном списке.
Игнорировать локальный список заблокированных команд TPM	Если этот параметр включен, то Windows игнорирует локальный список заблокированных команд доверенного платформенного модуля и блокирует только те команды доверенного платформенного модуля, которые указаны групповой политикой или в списке, определенном по умолчанию.
Индивидуальный порог блокировки обычных пользователей	Этот параметр позволяет управлять максимальным числом ошибок авторизации каждого обычного пользователя доверенного платформенного модуля (TPM). Если число ошибок авторизации пользователя за указанное значение параметра "Длительность блокировки обычных пользователей" достигает этого значения, обычному пользователю запрещается отправлять доверенному платформенному модулю (TPM) команды, требующие авторизации. Благодаря этому параметру снижается скорость, с которой обычные пользователи могут отправлять доверенному платформенному модулю команды, требующие авторизации, что помогает администраторам предотвращать переход оборудования доверенного платформенного модуля в режим блокировки. Если это значение не задано, по умолчанию используется значение 4.

Длительность блокировки обычных пользователей	Этот параметр позволяет управлять длительностью подсчета ошибок авторизации обычного пользователя при выполнении команд доверенного платформенного модуля (TPM), требующих авторизации, в минутах. Если число команд доверенного платформенного модуля с ошибкой авторизации за указанный отрезок времени достигает порога, обычному пользователю запрещается отправлять доверенному платформенному модулю команды, требующие авторизации. Если это значение не задано, по умолчанию используется значение 480 минут (8 часов).
Общий порог блокировки обычных пользователей	Этот параметр позволяет управлять максимальным числом ошибок авторизации всех обычных пользователей доверенного платформенного модуля (TPM). Если число ошибок авторизации всех обычных пользователей за указанное значение параметра "Длительность блокировки обычных пользователей" достигает этого значения, всем им запрещается отправлять доверенному платформенному модулю (TPM) команды, требующие авторизации. Благодаря этому параметру снижается скорость, с которой обычные пользователи могут отправлять доверенному платформенному модулю команды, требующие авторизации, что помогает администраторам предотвращать переход оборудования доверенного платформенного модуля в режим блокировки. Если это значение не задано, по умолчанию используется значение 9.
Включить резервное копирование TPM в доменные службы Active Directory (1 из 2)	Если эти 2 параметра (включая следующий) включены, то при использовании вами Windows для назначения или изменения пароля владельца доверенного платформенного модуля в AD DS будет автоматически и без уведомления создаваться резервная копия данных владельца доверенного платформенного модуля.
Включить резервное копирование TPM в доменные службы Active Directory (2 из 2)	Если эти 2 параметра (включая предыдущий) включены, то при использовании вами Windows для назначения или изменения пароля владельца доверенного платформенного модуля в AD DS будет автоматически и без уведомления создаваться резервная копия данных владельца доверенного платформенного модуля.

Настройки группы **Local security**:

Имя	**Описание**
Учетные записи: Ограничить использование пустых паролей локальных учетных записей только для входа на консоли	Этот параметр безопасности определяет, может ли использоваться локальная учетная запись без пароля для входа с мест, отличных от физической консоли компьютера. Если этот параметр включен, локальные учетные записи без пароля смогут войти только на клавиатуре компьютера.
Аудит: Аудит доступа к глобальным объектам системы	Этот параметр безопасности определяет, следует ли аудитировать доступ к глобальным объектам системы. Если этот параметр включен, вызывает создание глобальных объектов системы, таких как мьютексы, события, семафоры и устройства DOS, средним списком управления доступом системы (SACL). Только именованные объекты имеют SACL; объектам без имен не присваиваются SACL. Если также включена политика аудита доступа к объектам, доступ к этим глобальным объектам системы будет подвергаться аудиту.
Аудит: Аудит использования привилегии Резервное копирование и восстановление	Этот параметр безопасности определяет, следует ли аудитировать использование всех пользовательских привилегий, включая Резервное копирование и восстановление, когда применяется политика использования привилегии аудита. Включение этой опции при также включенной политике использования

	привилегии аудита генерирует событие аудита для каждого файла, который был зарезервирован или восстановлен.0 - Отключено, 1 - Включено
Аудит: Принудительное применение настроек подкатегорий политик аудита к настройкам категорий политик аудита	Windows Vista и более поздние версии Windows позволяют управлять политикой аудита более точно с помощью подкатегорий политики аудита. Установка политики аудита на уровне категории заменит новую функцию политики аудита подкатегорий. Групповая политика позволяет устанавливать политику аудита только на уровне категории, и существующая групповая политика может заменить настройки подкатегорий новых компьютеров при их присоединении к домену или обновлении до Windows Vista и более поздних версий. Чтобы позволить управлять политикой аудита, используя подкатегории, не требуя изменения групповой политики, в Windows Vista и более поздних версиях появилось новое значение реестра, SCENoApplyLegacyAuditPolicy, которое предотвращает применение политики аудита на уровне категории из групповой политики и из инструмента администрирования локальной политики безопасности.
Аудит: Немедленное выключение системы в случае невозможности регистрации аудита безопасности	Этот параметр безопасности определяет, следует ли система выключаться, если она не может регистрировать события безопасности. Если этот параметр безопасности включен, система прекращает работу, если аудит безопасности по какой-либо причине не может быть зарегистрирован. Обычно событие не удается зарегистрировать, когда журнал аудита заполнен, и метод сохранения, указанный для журнала безопасности, - либо Не перезаписывать события, либо Перезаписывать события через дни.
DCOM: Ограничения доступа к машине в языке определения дескриптора безопасности (SDDL)	Этот параметр политики определяет, какие пользователи или группы могут получить доступ к DCOM-приложению удаленно или локально. Этот параметр используется для контроля атак на компьютер, связанных с DCOM-приложениями.
DCOM: Ограничения запуска машины в языке определения дескриптора безопасности (SDDL)	Этот параметр политики определяет, какие пользователи или группы могут запускать или активировать DCOM-приложения удаленно или локально. Этот параметр используется для контроля атак на компьютер, связанных с DCOM-приложениями
Устройства: Разрешить отсоединение без входа в систему	Этот параметр безопасности определяет, может ли портативный компьютер быть отсоединен без предварительного входа в систему. Если эта политика включена, вход не требуется, и для отсоединения компьютера можно использовать внешнюю кнопку извлечения оборудования. Если отключено, пользователь должен войти в систему и иметь привилегию "Удаление компьютера из док-станции" для отсоединения компьютера.
Устройства: Разрешено форматирование и извлечение сменных носителей	Этот параметр безопасности определяет, кто имеет право на форматирование и извлечение сменных носителей NTFS. 0 - Только администраторы компьютера, 1 - Только администраторы и пользователи с правами администратора, 2 - Только администраторы и текущий локальный пользователь.
Устройства: Запретить пользователям устанавливать драйверы принтера	Для печати на общем принтере драйвер этого принтера должен быть установлен на локальном компьютере. Этот параметр безопасности определяет, кто имеет право устанавливать драйвер принтера в качестве части подключения к общему принтеру. Если этот параметр включен, только администраторы могут установить драйвер принтера в качестве части подключения к общему принтеру. Если этот параметр отключен, любой пользователь может установить драйвер принтера в качестве части подключения к общему принтеру.
Устройства: Ограничить доступ к CD-ROM только для локально вошедших пользователей	Этот параметр безопасности определяет, доступен ли CD-ROM как локальным, так и удаленным пользователям одновременно. Если эта политика включена, доступен только вошедший в систему пользователь для доступа к сменным CD-ROM носителям. Если эта политика включена и никто не вошел в систему, CD-ROM может быть доступен через сеть. 1- Включено, 2 - Отключено.

Устройства: Ограничить доступ к гибким дискам только для локально вошедших пользователей	Этот параметр безопасности определяет, доступны ли сменные гибкие диски одновременно локальным и удаленным пользователям. Если эта политика включена, только вошедший в систему пользователь имеет доступ к сменным гибким дискам. 1- Включено, 2 - Отключено.
Устройства: Поведение при установке неподписанных драйверов	Этот параметр безопасности определяет, что произойдет, если будет предпринята попытка установить драйвер устройства (посредством API настройки), который не прошел тестирование Лабораторией качества оборудования Windows (WHQL). Варианты: 0 - Без предупреждения, 1- Предупреждать, но разрешить установку, 2 - Запретить установку
Доменный контроллер: Разрешить операторам сервера планировать задачи	Этот параметр безопасности определяет, разрешено ли операторам сервера отправлять задания с помощью средства планирования AT.
Требования к подписи LDAP-сервера контроллера домена	Этот параметр безопасности определяет, требуется ли для сервера LDAP согласование подписи с клиентами LDAP.
Отказ контроллера домена: Отказ в изменении пароля учетной записи компьютера	Этот параметр безопасности определяет, откажутся ли контроллеры домена от запросов членов компьютеров на изменение паролей учетных записей компьютеров. По умолчанию члены компьютеров меняют свои пароли учетных записей компьютеров каждые 30 дней. В случае включения контролер домена откажет запросам на изменение пароля учетной записи компьютера.
Член домена: Цифровое шифрование или подпись данных безопасного канала (всегда)	Этот параметр безопасности определяет, должен ли весь трафик безопасного канала, инициированный членом домена, быть подписан или зашифрован.
Член домена: Цифровое шифрование данных безопасного канала (при возможности)	Этот параметр безопасности определяет, пытается ли член домена для всего трафика безопасного канала, который он инициирует, договориться о шифровании.
Член домена: Цифровая подпись данных безопасного канала (при возможности)	Этот параметр безопасности определяет, пытается ли член домена для всего трафика безопасного канала, который он инициирует, договориться о подписи.
Член домена: Отключить изменение пароля учетной записи компьютера	Определяет, меняет ли член домена периодически пароль учетной записи компьютера. Если этот параметр включен, то член домена не пытается изменить свой пароль учетной записи компьютера. Если этот параметр отключен, член домена пытается изменить свой пароль учетной записи компьютера в соответствии с параметром "Член домена: Максимальный срок действия пароля учетной записи компьютера", который по умолчанию составляет 30 дней.
Член домена: Требовать сильный (Windows 2000 или более поздняя версия) ключ сеанса	Этот параметр безопасности определяет, требуется ли 128-битная длина ключа для зашифрованных данных безопасного канала.
Интерактивный вход: Не отображать последнее имя пользователя	Этот параметр безопасности определяет, отображается ли имя последнего пользователя, который вошел в систему на экране входа в Windows. Если этот параметр включен, имя последнего пользователя, который успешно вошел, не отображается на экране входа.
Интерактивный вход: Отображать информацию пользователя при блокировке сеанса	Интерактивный вход: Отображение информации пользователя при блокировке сеанса.
Интерактивный вход: Не требовать CTRL+ALT+DEL	Этот параметр безопасности определяет, требуется ли нажатие CTRL+ALT+DEL перед тем, как пользователь сможет войти в систему.

Интерактивный вход: Текст сообщения для пользователей, пытающихся войти в систему	Этот параметр безопасности задает текстовое сообщение, которое отображается пользователям при входе в систему. Этот текст часто используется по юридическим причинам, например, для предупреждения пользователей о последствиях неправильного использования информации компании или для предупреждения их о том, что их действия могут быть проверены.
Интерактивный вход: Заголовок сообщения для пользователей, пытающихся войти в систему	Этот параметр безопасности позволяет указать заголовок, который будет отображаться в заголовке окна, содержащего текст сообщения Интерактивного входа: для пользователей, пытающихся войти в систему.
Интерактивный вход: Количество предыдущих входов, кэшируемых в случае недоступности контроллера домена	Вся информация о предыдущих входах пользователей кэшируется локально, чтобы в случае недоступности контроллера домена в последующих попытках входа они могли войти в систему. В этом параметре политики значение 0 отключает кэширование входа в систему. Любое значение выше 50 кэширует только 50 попыток входа в систему.
Интерактивный вход: Предупреждение пользователя о необходимости изменения пароля перед истечением срока действия	Определяет, за сколько дней заранее пользователей предупреждают, что их пароль скоро истечет. При таком заблаговременном предупреждении пользователь имеет время составить пароль, который будет достаточно надежным.
Требовать аутентификацию контроллера домена для разблокировки рабочей станции	Информация для входа должна быть предоставлена для разблокировки заблокированного компьютера. Для учетной записи домена это параметр безопасности определяет, должен ли контроллер домена быть обращен для разблокировки компьютера. Если этот параметр отключен, пользователь может разблокировать компьютер, используя кэшированные учетные данные. Если этот параметр включен, контроллер домена должен проверить учетную запись домена, используемую для разблокировки компьютера.
Требовать использование смарт-карты при интерактивном входе в систему	Этот параметр безопасности требует, чтобы пользователи входили в систему на компьютер с использованием смарт-карты.
Поведение при удалении смарт-карты при интерактивном входе в систему	Этот параметр безопасности определяет, что происходит, когда смарт-карта для вошедшего пользователя удаляется из считывателя смарт-карт. 0 - Никаких действий, 1 - Заблокировать рабочую станцию, 2 - Принудительный выход из системы, 3 - Отключить при удаленной сеансе службы Remote Desktop Services
Клиент Microsoft Network: Цифровая подпись для связи (всегда)	Этот параметр безопасности определяет, требуется ли подпись пакета компонентом SMB клиента. Протокол SMB (Server Message Block) обеспечивает основу для обмена файлами и печатью Microsoft и многих других операций сетевого взаимодействия, таких как удаленное администрирование Windows. Для предотвращения атак "человек посередине", которые изменяют пакеты SMB во время передачи, протокол SMB поддерживает цифровую подпись пакетов SMB. Этот параметр политики определяет, должна ли быть согласована цифровая подпись пакета SMB, прежде чем разрешается дальнейшее взаимодействие с сервером SMB.
Клиент Microsoft Network: Цифровая подпись для связи (если согласуется сервер)	Этот параметр безопасности определяет, пытается ли клиент SMB согласовать подпись пакета SMB. Протокол SMB (Server Message Block) обеспечивает основу для обмена файлами и печатью Microsoft и многих других операций сетевого взаимодействия, таких как удаленное администрирование Windows. Для предотвращения атак "человек посередине", которые изменяют пакеты SMB во время передачи, протокол SMB поддерживает цифровую подпись пакетов SMB. Этот параметр политики определяет, пытается ли компонент клиента SMB согласовать цифровую подпись пакета SMB при подключении к серверу SMB.

Клиент Microsoft Network: Отправлять незашифрованный пароль сторонним серверам SMB	Если этот параметр безопасности включен, перенаправлятор сообщений сервера блоков (SMB) может отправлять пароли в виде обычного текста на серверы SMB сторонних поставщиков, которые не поддерживают шифрование пароля во время аутентификации.
Сервер Microsoft Network: Время простоя до прерывания сеанса	Этот параметр безопасности определяет количество непрерывного времени простоя (в минутах), которое должно пройти в сеансе SMB (Server Message Block) до прерывания сеанса из-за бездействия. Администраторы могут использовать эту политику, чтобы контролировать, когда компьютер прерывает неактивный сеанс SMB. Если клиентская активность возобновляется, сеанс автоматически восстанавливается.
Microsoft network server: Электронная подпись сетевого сервера: Цифровая подпись связи (всегда)	Этот параметр безопасности определяет, нужно ли обязательно использовать подписание пакетов компонентом сервера SMB. Протокол блоков сообщений сервера (SMB) предоставляет основу для обмена файлами и печатью Microsoft, а также для многих других сетевых операций, таких как удаленное администрирование Windows. Чтобы предотвратить атаки ""человек посередине"", изменяющие пакеты SMB в процессе передачи, протокол SMB поддерживает цифровое подписание пакетов SMB. Этот параметр политики определяет, должно ли подписание пакетов SMB быть согласовано до дальнейшего взаимодействия с клиентом SMB.
Microsoft network server: Электронная подпись сетевого сервера: Цифровая подпись связи (если клиент соглашается)	Этот параметр безопасности определяет, будет ли сервер SMB согласовывать подписание пакетов SMB с клиентами, которые запрашивают это. Протокол блоков сообщений сервера (SMB) предоставляет основу для обмена файлами и печатью Microsoft, а также для многих других сетевых операций, таких как удаленное администрирование Windows. Чтобы предотвратить атаки ""человек посередине"", изменяющие пакеты SMB в процессе передачи, протокол SMB поддерживает цифровое подписание пакетов SMB. Этот параметр политики определяет, будет ли сервер SMB согласовывать подписание пакетов SMB, когда клиент SMB запрашивает это.
Microsoft network server: Отключение клиентов при истечении времени входа в систему	Этот параметр безопасности определяет, следует ли отключать пользователей, подключенных к локальному компьютеру вне времени допустимого входа в систему их учетной записи. Этот параметр влияет на компонент Server Message Block (SMB).
Microsoft network server: Уровень валидации имени целевой службы SPN сервера	Протокол блоков сообщений сервера (SMB) предоставляет основу для обмена файлами и принтерами и для многих других сетевых операций, таких как удаленное администрирование Windows. Протокол SMB поддерживает валидацию имени службы SPN сервера SMB в предоставленном аутентификационном блоке, предоставляемом клиентом SMB, для предотвращения класса атак против серверов SMB, известных как атаки переадресации SMB. Этот параметр затронет как SMB1, так и SMB2.
Доступ к сети: Не разрешать анонимное перечисление учетных записей SAM	Этот параметр безопасности определяет, какие дополнительные разрешения будут предоставлены для анонимных подключений к компьютеру. Windows позволяет анонимным пользователям выполнять определенные действия, такие как перечисление имен учетных записей домена и сетевых ресурсов. Это удобно, например, когда администратор хочет предоставить доступ пользователям в доверенном домене, который не поддерживает взаимное доверие.
Доступ к сети: Не разрешать анонимное перечисление учетных записей SAM и ресурсов	Этот параметр безопасности определяет, разрешено ли анонимное перечисление учетных записей SAM и ресурсов. Windows позволяет анонимным пользователям выполнять определенные действия, такие как перечисление имен учетных записей домена и сетевых ресурсов. Это удобно, например, когда администратор хочет предоставить доступ пользователям в доверенном домене, который не поддерживает взаимное доверие.

Доступ к сети: Не разрешать сохранение паролей и учетных данных для сетевой аутентификации	Этот параметр безопасности определяет, будет ли хранилище имен и паролей сохранять пароли, учетные данные или паспорта .NET для последующего использования при получении аутентификации домена. Если он включен, этот параметр предотвращает сохранение паролей и учетных данных в хранилище имен и паролей.
Доступ к сети: Допустить разрешения для всех для анонимных пользователей	Этот параметр безопасности определяет, какие дополнительные разрешения предоставляются для анонимных подключений к компьютеру.
Доступ к сети: Именованные каналы, к которым можно обращаться анонимно	Этот параметр безопасности определяет, какие сеансы связи (каналы) будут иметь атрибуты и разрешения, позволяющие анонимный доступ.
Доступ к сети: Удаленные доступные пути реестра	Этот параметр безопасности определяет, к каким ключам реестра можно получить доступ через сеть, независимо от пользователей или групп, указанных в списке управления доступом (ACL) ключа реестра winreg.
Доступ к сети: Удаленные доступные пути и подпути реестра	Этот параметр безопасности определяет, к каким путям и подпутям реестра можно получить доступ через сеть, независимо от пользователей или групп, указанных в списке управления доступом (ACL) ключа реестра winreg.
Доступ к сети: Доступные общие ресурсы, к которым можно обратиться анонимно	Этот параметр безопасности определяет, к каким сетевым общим ресурсам могут получить доступ анонимные пользователи.
Доступ к сети: Модель общего доступа и модель безопасности для локальных учетных записей	Этот параметр безопасности определяет, как происходит аутентификация сетевых входов, использующих локальные учетные записи. Если этот параметр установлен в значение «Классическая», сетевые входы, использующие учетные данные локальной учетной записи, аутентифицируются с использованием этих учетных данных. Модель «Классическая» позволяет более тонкую настройку доступа к ресурсам. Используя классическую модель, вы можете предоставить различные типы доступа разным пользователям к одному и тому же ресурсу.
Сетевая безопасность: Не сохранять значение хэш-функции LAN Manager при следующей смене пароля	Этот параметр безопасности определяет, сохраняется ли при следующей смене пароля значение хэш-функции LAN Manager (LM) для нового пароля. Хэш-функция LM относительно слабая и подвержена атакам, по сравнению с криптографически более надежной хэш-функцией Windows NT. Поскольку хэш-функция LM хранится на локальном компьютере в базе данных безопасности, пароли могут быть скомпрометированы в случае атаки на базу данных безопасности.
Сетевая безопасность: Уровень аутентификации LAN Manager	Этот параметр управления безопасностью определяет протокол аутентификации вызов-ответ, используемый для сетевых входов.
Сетевая безопасность: Требования клиента LDAP к подписи	Этот параметр безопасности определяет уровень подписи данных, который запрашивается от клиентов, выполняющих запросы LDAP BIND.
Сетевая безопасность: Минимальная сеансовая безопасность для клиентов NTLM SSP (включая защищенный RPC)	Этот параметр безопасности позволяет клиенту требовать согласования шифрования 128 бит и/или безопасности сеанса NTLMv2. Эти значения зависят от значения параметра установки безопасности Уровень аутентификации LAN Manager.
Сетевая безопасность: Минимальная сеансовая безопасность для серверов NTLM SSP	Этот параметр безопасности позволяет серверу требовать согласования шифрования 128 бит и/или безопасности сеанса NTLMv2. Эти значения зависят от значения параметра установки безопасности Уровень аутентификации LAN Manager.

(включая защищенный RPC)	
Сетевая безопасность: Ограничить NTLM: Исходящий трафик NTLM на удаленные серверы	Этот параметр настройки политики позволяет вам запретить или провести аудит исходящего трафика NTLM с этого компьютера под управлением Windows 7 или этого компьютера под управлением Windows Server 2008 R2 на любой удаленный сервер Windows.
Сетевая безопасность: Ограничить NTLM: Входящий трафик NTLM	Этот параметр настройки политики позволяет вам запретить или разрешить входящий трафик NTLM.
Сетевая безопасность: Ограничить NTLM: Аудит входящего трафика NTLM	Этот параметр настройки политики позволяет вам проводить аудит входящего трафика NTLM.
Сетевая безопасность: Ограничение NTLM: Аутентификация NTLM в этом домене	Этот параметр политики позволяет вам разрешить или запретить аутентификацию NTLM в пределах домена с контроллера домена. Этот параметр не влияет на интерактивный вход в этот контроллер домена.
Сетевая безопасность: Ограничение NTLM: Аудит аутентификации NTLM в этом домене	Этот параметр политики позволяет вам аудитировать аутентификацию NTLM в домене с контроллера домена.
Сетевая безопасность: Ограничение NTLM: Добавление исключений удаленных серверов для аутентификации NTLM	Этот параметр политики позволяет вам создать список исключений удаленных серверов, к которым клиенты могут использовать аутентификацию NTLM, если параметр политики "Сетевая безопасность: Ограничение NTLM: Исходящий трафик NTLM на удаленные серверы" настроен.
Сетевая безопасность: Ограничение NTLM: Добавление исключений серверов в этом домене	Этот параметр политики позволяет вам создать список исключений серверов в этом домене, к которым клиенты могут использовать аутентификацию NTLM с прохождением, если установлен параметр политики "Сетевая безопасность: Ограничение NTLM: Запретить аутентификацию NTLM в этом домене".
Сетевая безопасность: Разрешить откат NTLM к NULL-сеансу в системе LocalSystem	Разрешить NTLM откатиться к NULL-сеансу при использовании с LocalSystem.
Сетевая безопасность: Разрешить запросы аутентификации PKU2U к этому компьютеру для использования онлайн-идентификаторов.	Этот параметр политики будет отключен по умолчанию на компьютерах с присоединением к домену. Это препятствует возможности онлайн-идентификаторов аутентифицировать компьютер, присоединенный к домену, в Windows 7.
Сетевая безопасность: Настройка разрешенных типов шифрования для Kerberos	Этот параметр политики позволяет вам задать типы шифрования, которые разрешено использовать Kerberosy. Если не выбрано, тип шифрования не будет разрешен. Этот параметр может повлиять на совместимость с клиентскими компьютерами или службами и программами.
Консоль восстановления: Разрешить автоматический вход в систему администратора	Этот параметр безопасности определяет, должен ли быть введен пароль для учетной записи администратора перед предоставлением доступа к системе. Если этот параметр включен, консоль восстановления не потребует ввода пароля и автоматически выполнит вход в систему.
Консоль восстановления: Разрешить копирование на диск и доступ ко всем дискам и папкам	Включение этой опции безопасности делает команду SET консоли восстановления доступной, что позволяет установить следующие переменные среды консоли восстановления.
Выключение: Разрешить завершение работы	Этот параметр безопасности определяет, может ли компьютер быть выключен без входа в Windows. Когда это политика включена, команда Выключить доступна на

системы без входа в систему	экране входа в Windows.
Выключение: Очистка файла подкачки виртуальной памяти	Этот параметр безопасности определяет, очищается ли файл подкачки виртуальной памяти при выключении системы.
Система криптографии: Использовать алгоритмы, соответствующие стандартам FIPS для шифрования, хэширования и подписи	Для поставщика службы безопасности Schannel (SSP) этот параметр безопасности отключает более слабые протоколы Secure Sockets Layer (SSL) и поддерживает только протоколы Transport Layer Security (TLS) в качестве клиента и сервера (по возможности). Если этот параметр включен, поставщик службы безопасности Transport Layer Security/Secure Sockets Layer (TLS/SSL) использует только одобренные криптографические алгоритмы FIPS 140: 3DES и AES для шифрования, открытый ключ RSA или ECC для обмена и аутентификации ключей TLS, а также только фукнции хэширования Secure Hashing Algorithm (SHA1, SHA256, SHA384 и SHA512) для требований хэширования TLS.
Система криптографии: Принудительная защита сильными ключами для пользовательских ключей, хранимых на компьютере	Этот параметр безопасности определяет, нужно ли пользователям вводить пароль для использования их собственных ключей.
Объекты системы: Умалчиваемый владелец для объектов, созданных участниками группы Администраторы	Этот параметр безопасности определяет, какой принцип безопасности (SID) будет назначен ВЛАДЕЛЬЦЕМ объектов при создании объекта участником группы Администраторы.
Системные объекты: Требовать нечувствительность к регистру для подсистем Windows, отличных от Windows	Этот параметр безопасности определяет, является ли нечувствительность к регистру обязательной для всех подсистем. Подсистема Win32 нечувствительна к регистру. Однако ядро поддерживает чувствительность к регистру для других подсистем, таких как POSIX.
Системные объекты: Укрепление параметров по умолчанию внутренних системных объектов (например, символических ссылок)	Этот параметр безопасности определяет степень списка управления доступом (DACL) по умолчанию для объектов.
Системные параметры: Дополнительные подсистемы	Этот параметр безопасности определяет, какие дополнительные подсистемы можно запускать для поддержки ваших приложений. С помощью этого параметра безопасности вы можете указать столько подсистем, сколько потребуется для поддержки ваших приложений в вашей среде.
Системные параметры: Использование правил сертификатов для исполняемых файлов Windows для политик ограничения программного обеспечения	Этот параметр безопасности определяет, обрабатываются ли цифровые сертификаты, когда пользователь или процесс пытается запустить программное обеспечение с расширением имени файла .exe. Этот параметр безопасности используется для включения или отключения правил сертификатов, типа правила политики ограничения программного обеспечения. С помощью политики ограничения программного обеспечения вы можете создать правило сертификата, которое позволит или запретит выполнение программного обеспечения, подписанного Authenticode, основываясь на цифровом сертификате, связанном с программным обеспечением. Для того чтобы правила сертификата вступили в силу, необходимо включить этот параметр безопасности.
Управление учетными записями: Режим согласования администратора для	Этот параметр безопасности определяет поведение режима согласования администратора для встроенной учетной записи администратора.

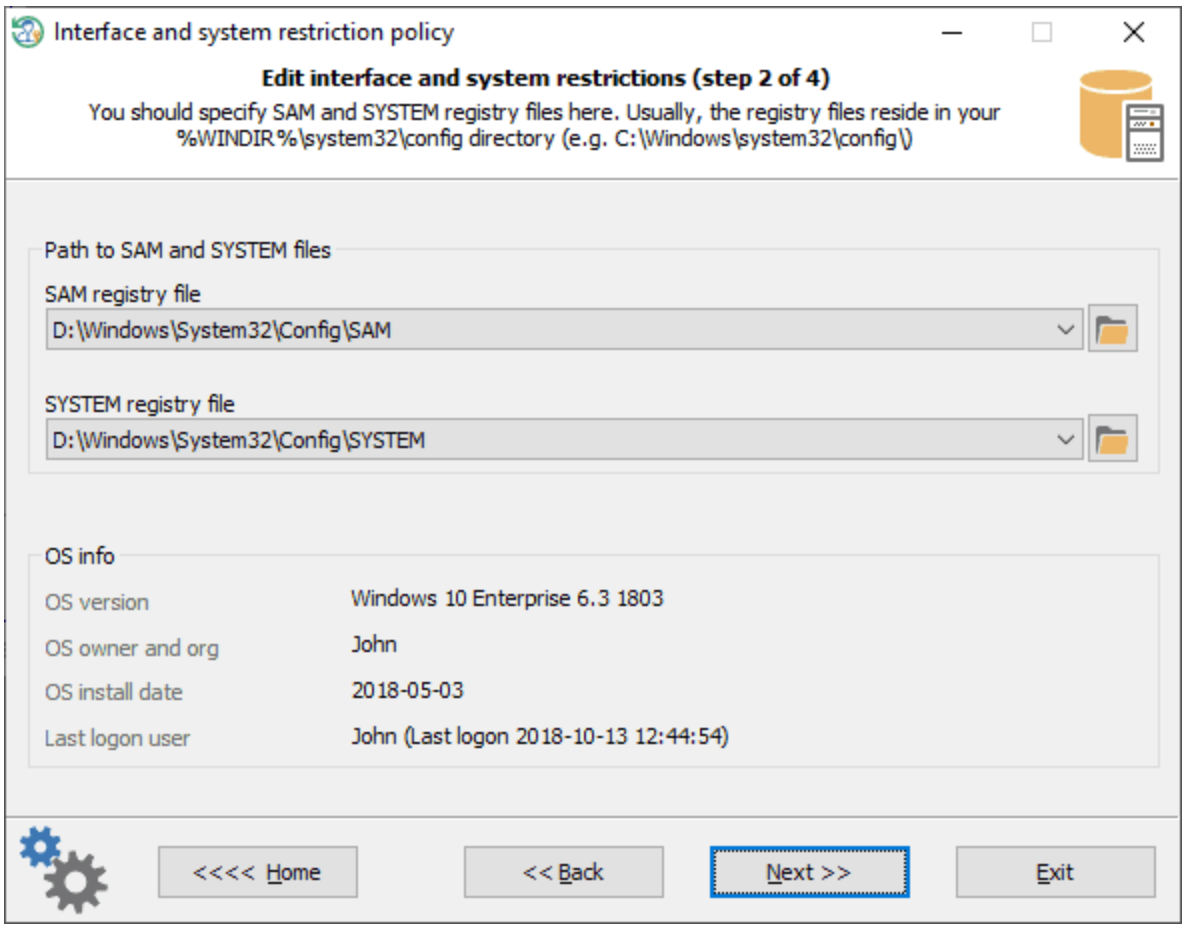
встроенной учетной записи администратора	
Управление учетными записями: Поведение запроса на повышение прав для администраторов в режиме согласования администратора	Этот параметр безопасности определяет поведение запроса на повышение прав для администраторов.
Управление учетными записями: Поведение запроса на повышение прав для стандартных пользователей в режиме согласования администратора	Этот параметр безопасности определяет поведение запроса на повышение прав для стандартных пользователей.
Управление учетными записями: Обнаружение установщика: обнаружение установок приложений и запрос поднятия уровня доступа	Этот параметр безопасности определяет поведение обнаружения установки приложения для всей системы.
Управление учетными записями: Только поднимать уровень доступа для подписанных и проверенных исполняемых файлов	Этот параметр безопасности обеспечит проверку подписей PKI для всех интерактивных приложений, запрашивающих поднятие привилегий. Администраторы предприятий могут контролировать список разрешенных администраторам приложений через добавление сертификатов в хранилище доверенных издателей локального компьютера.
Управление учетными записями: Только поднимать уровень доступа для UIAccess-приложений, установленных в защищенных местах	Этот параметр безопасности обеспечит выполнение требования, согласно которому приложения, запрашивающие выполнение с уровнем целостности UIAccess (посредством установки метки UIAccess=true в своем манифесте приложения), должны находиться в защищенном месте в файловой системе.
Управление учетными записями: Выполнять все администраторы в режиме одобрения администратором	Этот параметр безопасности определяет поведение всех политик UAC для всей системы.
Управление учетными записями: Переключение на защищенный рабочий стол при запросе повышения уровня доступа	Этот параметр безопасности определяет, будет ли запрос на повышение уровня доступа появляться на интерактивном рабочем столе пользователя или на защищенном рабочем столе.
Управление учетными записями: Виртуализировать неудачи записи файлов и реестра в местоположения для каждого пользователя	Этот параметр безопасности включает перенаправление неудачных попыток записи легаси-приложений в определенные местоположения как в реестре, так и в файловой системе. Эта функция смягчает проблемы тех приложений, которые ранее работали с правами администратора и записывали данные приложения во время выполнения обратно в %ProgramFiles%, %Windir%; %Windir%\system32 или HKLM\Software\....
Управление учетными записями: Разрешить UIAccess-приложениям запрашивать повышение уровня доступа без	Этот параметр безопасности определяет, могут ли программы доступности пользовательского интерфейса (UIAccess или UIA) автоматически отключать защищенный рабочий стол при запросах на повышение уровня доступа, используемых обычным пользователем. Если вы включите этот параметр,

использования защищенного рабочего стола	программы UIA, включая удаленную помощь Windows, могут автоматически отключать защищенный рабочий стол для запросов на повышение уровня доступа. Если только вы не отключили запросы на повышение уровня доступа, они будут появляться на интерактивном рабочем столе пользователя, а не на защищенном рабочем столе.

3.2.5 Политика ограничений интерфейса и системы

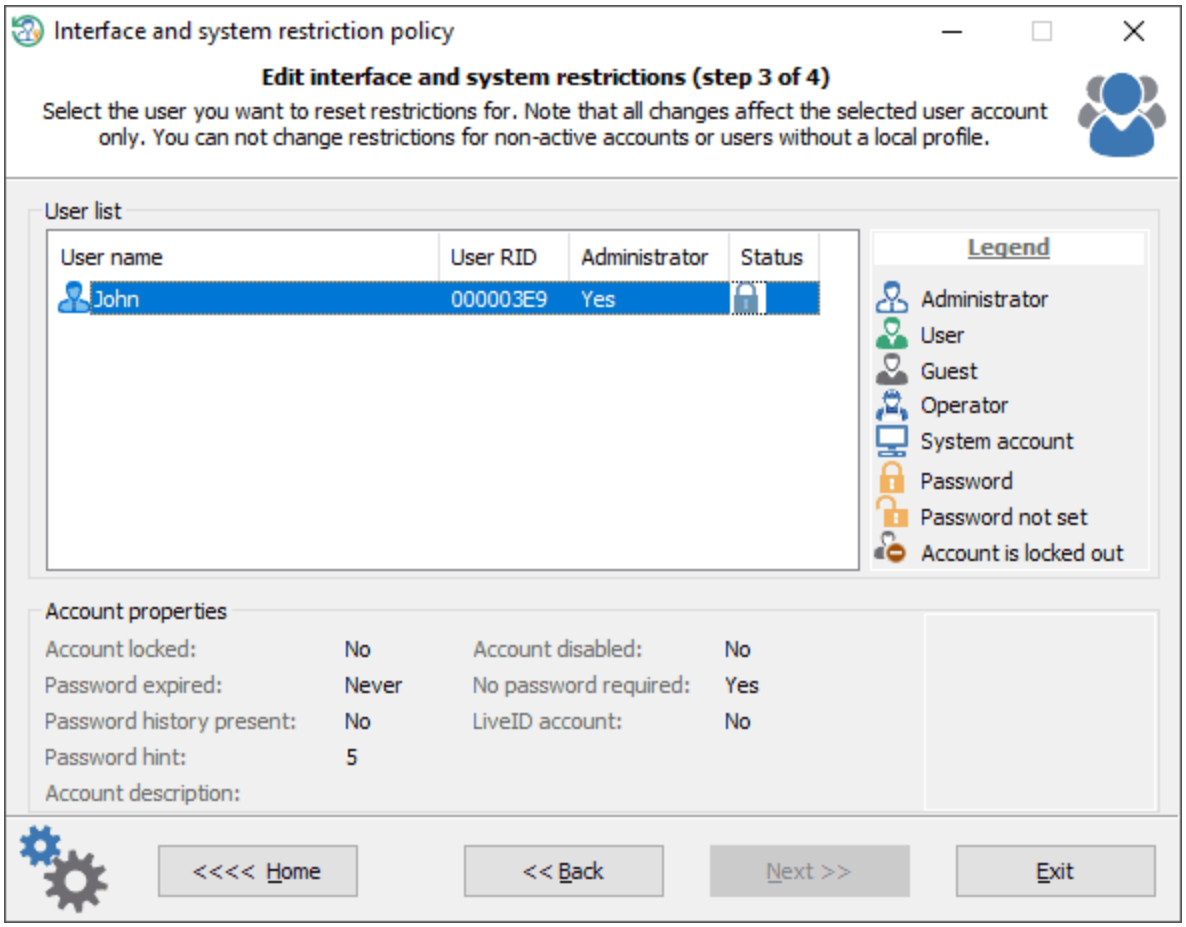
Этот режим работы программы позволяет изменить или сбросить ограничения интерфейса или системы для выбранного пользователя. Например, ограничение на запуск программ, отключение определенных настроек панели управления, блокировку редактора реестра или командной строки, запрет доступа к съемным дискам и т.д.

Выбор файлов реестра



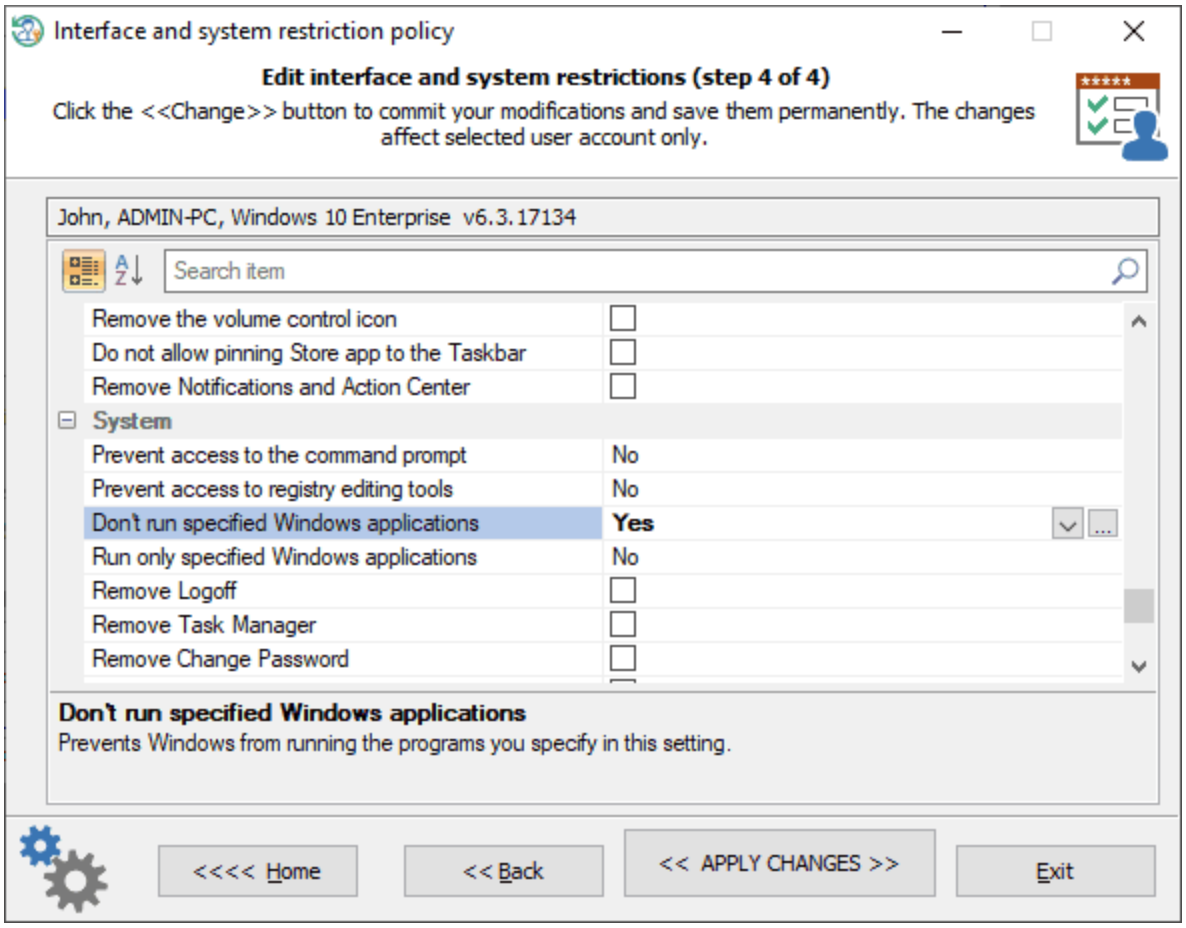
Выберите найденные программой файлы реестра SAM и SYSTEM или укажите путь к ним вручную.

Выбор учетной записи



Выберите учетную запись ограничения которой необходимо изменить или сбросить. Программа отображает только активные учетные записи, имеющие локальный профиль.

Изменение ограничений интерфейса и системы



После выбора учетной записи можно приступать к сбросу ограничений. Нажмите кнопку << *СОХР. ИЗМЕНЕНИЯ* >> чтобы сохранить новые настройки.

Учтите, все сделанные изменения влияют только на выбранную учетную запись.

Краткое описание настроек ограничений интерфейса и системы.

Ограничения **Control panel**:

Имя	Описание
Скрыть указанные элементы панели управления	Этот параметр позволяет отображать или скрывать указанные элементы панели управления, например "Мышь", "Система" или "Персонализация", в окне панели управления и на начальном экране. Этот параметр влияет на начальный экран и окно панели управления, а также на другие возможности доступа к элементам панели управления, например ссылки в центре справки и поддержки или командные строки, использующие control.exe. Этот параметр не оказывает влияния на элементы, отображаемые в окне "Параметры компьютера". Если вы включаете этот параметр, то можете выбрать элементы, которые не будут отображаться в окне панели управления и на начальном экране."Этот параметр позволяет отображать или скрывать указанные элементы панели управления, например "Мышь", "Система" или "Персонализация", в окне панели управления и на начальном экране. Этот параметр влияет на начальный экран и окно панели управления, а также на другие возможности доступа к элементам панели управления, например ссылки в центре справки и поддержки или командные

	строки, использующие control.exe. Этот параметр не оказывает влияния на элементы, отображаемые в окне "Параметры компьютера". Если вы включаете этот параметр, то можете выбрать элементы, которые не будут отображаться в окне панели управления и на начальном экране.
Отображать только указанные элементы панели управления	Этот параметр контролирует, какие элементы панели управления, например "Мышь", "Система" или "Персонализация", отображаются в окне панели управления и на начальном экране. В окне панели управления отображаются только элементы, указанные в этом параметре. Этот параметр влияет на начальный экран и панель управления, а также на другие возможности доступа к элементам панели управления, например ссылки в центре справки и поддержки или командные строки, использующие control.exe. Этот параметр не оказывает влияния на элементы, отображаемые в окне "Параметры компьютера".
Запретить доступ к панели управления и параметрам компьютера	Отключает все программы панели управления и приложение параметры параметров компьютера. Этот параметр запрещает запуск Control.exe и SystemSettings.exe, программных файлов для панели управления и параметры параметров компьютера. В результате пользователи не могут открыть панель управления или окно "Параметры компьютера" либо запустить их элементы.
Отображение страницы параметров	Задается список страниц, которые следует отобразить или скрыть в приложении "Системные параметры". Эта политика позволяет администратору блокировать заданный набор страниц в приложении "Системные параметры". Заблокированные страницы не будут отображаться в приложении, и если все страницы в категории заблокированы, то категория также будет скрыта. При прямом переходе к заблокированной странице через URI-адрес, контекстное меню в проводнике или как-либо по-другому будет показана главная страница параметров. Пример: showonly:about,bluetooth hide:bluetooth
Отключить окно свойств экрана на панели управления	Отключает окно свойств экрана на панели управления. Если этот параметр включен, окно свойств экрана на панели управления использовать невозможно. При попытке открыть окно свойств экрана отображается сообщение о том, что выполнение этого действия запрещено одним из параметров.
Скрыть вкладку "Параметры"	Удаляет вкладку "Параметры" из окна свойств экрана.
Запрет изменения темы	Этот параметр отключает коллекцию тем на панели управления персонализацией.
Запрет изменения стилей оформления окон и кнопок	Запрещает пользователям или приложениям изменять стили оформления диалоговых окон и кнопок, отображаемых на экране компьютера.
Включение заставки	Включает заставку рабочего стола. Если этот параметр отключен, заставки не запускаются. Кроме того, этот параметр отключает раздел "Заставка" в диалоговом окне "Заставка" на панелях управления персонализацией или свойствами экрана. Вследствие этого пользователи не могут изменять параметры заставки.
Запрет изменения цвета и оформления	Отключает страницу "Цвет" (или "Цвет окна") на панели управления персонализацией или диалоговое окно "Цветовая схема" на панели управления экраном, если компонент персонализации недоступен. Этот параметр запрещает пользователям использовать панель управления для изменения цвета панели задач и границы окна (в Windows 8), цвета стеклянного окна (в Windows Vista и Windows 7), системных цветов или цветовых схем для рабочего стола и окон.
Запрет изменения фона рабочего стола	Запрещает изменять или добавлять фон рабочего стола.
Запрет изменения значков рабочего стола	Запрещает пользователям изменять значки рабочего стола.
Запрет изменения указателей мыши	Запрещает пользователям изменять указатели мыши.

Запретить изменение заставки	Запрещает открытие окна "Заставка" на панелях управления персонализацией или свойствами экрана.
Запрет изменения звуков	Запрещает пользователям изменять звуковую схему.
Защита заставки с помощью пароля	Определяет, должна ли использоваться защита заставки с помощью пароля на этом компьютере. Если вы включаете этот параметр, все заставки защищаются паролем. Если вы отключаете этот параметр, включить парольную защиту какой-либо заставки невозможно.
Разрешить обзор сети для поиска принтеров	Этот параметр позволяет пользователям использовать мастер установки принтеров для поиска общих принтеров в сети.
Разрешить обзор общего веб-сайта с целью поиска принтеров	Добавляет ссылку на страницу Интернета или интрасети в окно мастера установки принтеров. Этот параметр политики позволяет направить пользователей на веб-страницу, с которой можно устанавливать принтеры.
Отключить управление принтером, используемым по умолчанию, со стороны Windows	Этот параметр позволяет изменить порядок управления принтером, используемым по умолчанию.
Запретить добавление принтеров	Запрещает использовать известные методы для установки локальных и сетевых принтеров.
Запретить удаление принтеров	Если вы включите этот параметр, пользователи не смогут удалять локальные и сетевые принтеры.
Скрытие страницы доступа к программам и параметров по умолчанию	Данный параметр удаляет страницу "Доступ к программам и параметры по умолчанию" из панели управления "Программы". В результате пользователи не могут просматривать или изменять соответствующую страницу.
Скрыть страницу "Получение программ"	Запрещает пользователям просматривать или устанавливать опубликованные программы из сети. Этот параметр запрещает пользователям доступ к странице "Получение программ" компонента "Программы" на панели управления в виде по категориям, "Программы и компоненты" в классическом виде, а также задачи "Установка новой программы из сети". Страница "Получение программ" содержит список опубликованных программ и позволяет легко устанавливать их.
Скрыть страницу "Установленные обновления"	Данный параметр запрещает пользователям доступ к странице "Установленные обновления" задачи "Просмотр установленных обновлений".
Скрыть страницу "Программы и компоненты"	Данный параметр запрещает пользователям доступ к компоненту "Программы и компоненты" для просмотра, удаления, изменения или восстановления программ, которые уже установлены на компьютере.
Скрыть панель управления "Программы"	Этот параметр предотвращает использование пользователями панели управления "Программы" в виде по категориям и "Программы и компоненты" в классическом виде.
Скрыть "Компоненты Windows"	Этот параметр запрещает использование пользователями задачи "Включение и отключение компонентов Windows" панели управления "Программы" в виде по категориям, "Программы и компоненты" в классическом виде и компонента "Получение программ". В результате пользователи не могут просматривать, включать и выключать различные компоненты и службы Windows.
Скрыть "Windows Marketplace"	Этот параметр запрещает использование пользователями задачи "Получить новые программы с Windows Marketplace" панели управления "Программы" в виде по категориям, "Программы и компоненты" в классическом виде, а также компонента "Получение программ".
Скрыть параметры администрирования в панели "Язык и региональные стандарты"	Этот параметр убирает параметры администрирования из элемента панели управления "Региональные стандарты". К параметрам администрирования относятся интерфейсы для задания языка системы и копирования параметров в учетную запись пользователя по умолчанию. Однако этот параметр не

	запрещает администратору или другому приложению изменять эти значения программным путем.
Скрыть параметр изменения данных о географическом расположении	Этот параметр убирает возможность изменять данные о географическом расположении пользователя из элемента панели управления "Региональные стандарты".
Скрыть параметры выбора языковой группы	Этот параметр убирает возможность изменить язык меню и диалоговых окон пользовательского интерфейса из элемента панели управления "Язык и региональные стандарты".
Скрыть параметры выбора и настройки региональных параметров пользователя	Этот параметр убирает интерфейс региональных форматов из элемента панели управления "Региональные стандарты".

Ограничения **Desktop**:

Имя	**Описание**
Скрыть значок "Сетевые размещения" на рабочем столе	Удаляет значок "Сетевые размещения" с рабочего стола.
Удалить мастер очистки рабочего стола	Запрещает пользователям использовать мастер очистки рабочего стола. Если включить этот параметр, то мастер очистки рабочего стола не запускается автоматически каждые 60 дней на рабочей станции пользователя. Кроме того, пользователь не сможет получить доступ к мастеру очистки рабочего стола.
Удалить значок "Компьютер" с рабочего стола	Эта политика скрывает значок "Компьютер" с рабочего стола и из нового меню "Пуск". Кроме того, она скрывает ссылки на "Компьютер" в веб-представлениях всех окон проводника и скрывает "Компьютер" в области дерева папок проводника. Если пользователь перемещается в папку "Компьютер" с помощью кнопки "Вверх", когда этот параметр включен, то он увидит пустую папку "Компьютер". Этот параметр дает возможность администраторам запретить пользователям просмотр папки "Компьютер" в этой оболочке и позволяет показывать пользователям более простую среду рабочего стола. Если включить этот параметр, то папка "Компьютер" скрывается на рабочем столе, в новом меню "Пуск", в области дерева папок проводника и в веб-представлениях проводника. Если пользователь сумеет перейти в папку "Компьютер", то она окажется пустой.
Удалить пункт "Свойства" из контекстного меню значка "Документы"	Этот параметр скрывает пункт меню "Свойства" в контекстном меню значка "Мои документы".
Запретить добавление, перетаскивание и закрытие панелей инструментов панели задач	Запрещает пользователям манипуляции с панелями инструментов рабочего стола. Если включить этот параметр, то пользователи не смогут добавлять на рабочий стол панели инструментов или удалять их. Кроме того, пользователи не смогут перетаскивать панели инструментов на закрепленную панель или с нее.
Удалить значок "Корзина" с рабочего стола	Удаляет большинство значков "Корзина". Этот параметр удаляет значок "Корзина" с рабочего стола, из проводника, из программ, использующих окна проводника, и из стандартного диалогового окна "Открыть".
Скрыть значок Internet Explorer на рабочем столе	Удаляет значок Internet Explorer с рабочего стола и из панели "Быстрый запуск" на панели задач.
Скрыть и отключить все элементы рабочего стола	Убирает с рабочего стола значки, ярлыки и другие используемые по умолчанию и определенные пользователем элементы, в том числе "Портфель", "Корзина", "Компьютер" и "Сетевые размещения".

Удалить пункт "Свойства" из контекстного меню компонента "Корзина"	Удаляет пункт "Свойства" из контекстного меню компонента "Корзина".
Удалить пункт "Свойства" из контекстного меню значка "Компьютер"	Этот параметр скрывает пункт "Свойства" в контекстном меню значка "Компьютер".
Скрыть папку Active Directory	Скрывает папку Active Directory в папке "Сетевые размещения".
Запретить настройку панелей инструментов рабочего стола	Запрещает пользователям настройку длины панелей инструментов рабочего стола. Кроме того, пользователи не могут изменять положение элементов или панелей инструментов на закрепленных панелях.
Удалить значок "Мои документы" с рабочего стола	Удаляет большинство значков "Мои документы".
Включить Active Desktop	Включает рабочий стол Active Desktop и запрещает пользователям его отключение.
Отключить Active Desktop	Отключает рабочий стол Active Desktop и запрещает пользователям его включение.
Запретить изменения	Запрещает пользователям включать или отключать Active Desktop или изменять конфигурацию Active Desktop.
Запретить добавление элементов	Запрещает пользователям добавлять веб-содержимое на рабочий стол Active Desktop.
Запретить закрытие элементов	Запрещает пользователям удалять веб-содержимое со своих рабочих столов Active Desktop.
Запретить изменение элементов	Запрещает пользователям изменять свойства элементов веб-содержимого на своих рабочих столах Active Desktop.
Запретить удаление элементов	Запрещает пользователям удалять веб-содержимое со своих рабочих столов Active Desktop.
Отключить все элементы	Удаляет содержимое рабочего стола Active Desktop и запрещает пользователям добавление содержимого рабочего стола Active Desktop.
Добавить или удалить элементы	Добавляет и удаляет указанные элементы веб-содержимого.

Ограничения **Network**:

Имя	**Описание**
Запрет подключения и разрыва подключения удаленного доступа	Определяет, могут ли пользователи установить или разорвать подключения удаленного доступа. Если включить этот параметр (и параметр "Включить параметры сетевых подключений для администраторов"), двойной щелчок значка не действует, и пункты меню для включения и разрыва будут запрещены для всех пользователей (включая администраторов).
Запретить удаление подключений удаленного доступа	Определяет, могут ли пользователи удалять подключения удаленного доступа. Если включить этот параметр (и параметр "Разрешить параметры сетевых подключений для администраторов"), пользователи (включая администраторов) не смогут удалять подключения удаленного доступа пользователей. Этот параметр также отключает команду "Удалить" контекстного меню подключений удаленного доступа и меню "Файл" в папке сетевых подключений.
Запретить переименование частных	Определяет, могут ли пользователи переименовать их частные подключения удаленного доступа.

подключений удаленного доступа	
Возможность удалить все подключения удаленного доступа пользователей	Определяет, могут ли пользователи, не являющиеся администраторами, переименовать все подключения удаленного доступа пользователей.
Запрет доступа к пункту "Настройки удаленного доступа" меню "Дополнительно"	Определяет, будет ли включен пункт "Настройки удаленного доступа" меню "Дополнительно" папки сетевых подключений.
Запрет доступа к свойствам подключений локальной сети	Определяет, могут ли пользователи изменять свойства подключений локальной сети. Этот параметр определяет, будет ли включен элемент меню "Свойства" и, соответственно, будет ли доступно пользователям диалоговое окно свойств подключений локальной сети.
Запретить дополнительные настройки TCP/IP	Задает, могут ли пользователи настраивать дополнительные параметры TCP/IP. Если разрешить этот параметр (и разрешить параметр "Разрешить настройки сетевых подключений для администраторов"), кнопка "Дополнительно" в диалоговом окне свойств TCP/IP будет запрещена всем пользователям (включая администраторов). В результате пользователи не смогут открыть страницу свойств дополнительных параметров TCP/IP и изменить параметры IP, например информацию о серверах DNS и WINS.
Запрет доступа к пункту "Дополнительные параметры" меню "Дополнительно"	Задает, будет ли пункт "Дополнительные параметры" меню "Дополнительно" для сетевых подключений разрешен для администраторов.
Возможность переименовать подключения локальной сети	Определяет, могут ли пользователи, не являющиеся администраторами, переименовать подключение локальной сети. Если вы включаете этот параметр политики, функция "Переименовать" включается для подключений локальной сети. Пользователи, не являющиеся администраторами, могут переименовать подключения локальной сети, щелкнув значок подключения или используя меню "Файл".
Запретить добавление и удаление компонентов для локальной сети (LAN) и подключений удаленного доступа	Задает администраторам возможность добавлять и удалять сетевые компоненты для LAN и удаленного подключения. Эта настройка влияет только на администраторов. Если разрешить этот параметр (и разрешить параметр "Разрешить настройки сетевых подключений для администраторов"), кнопки установки и удаления компонентов подключений будут запрещены, и администраторы не получат доступ к сетевым компонентам мастера компонентов Windows.
Возможность удалить все подключения удаленного доступа пользователей	Определяет, могут ли пользователи удалить все подключения удаленного доступа.
Запрет изменения свойств частного подключения удаленного доступа	Определяет, могут ли пользователи просматривать или изменять свойства их частных подключений удаленного доступа.
Возможность изменить свойства всех пользовательских подключений удаленного доступа	Определяет, могут ли пользователи просмотреть или изменить свойства подключений удаленного доступа, доступные всем пользователям компьютера.
Запрет доступа к свойствам компонентов подключений удаленного доступа	Определяет, могут ли пользователи просматривать и изменять свойства компонентов, используемых частными подключениями или подключениями удаленного доступа всех пользователей. Этот параметр определяет, может ли кнопка "Свойства" для компонентов использоваться частными подключениями или подключениями удаленного доступа всех пользователей.

Включение параметров сетевых подключений Windows 2000 для администраторов	Определяет, можно ли параметры семейства Windows 2000 Server применить к администраторам.
Запрет доступа к свойствам компонентов подключений локальной сети	Определяет, могут ли администраторы или операторы настройки сети изменить свойства компонентов, используемых подключением локальной сети. Этот параметр определяет, будет ли включена кнопка "Свойства" для компонентов подключения локальной сети.
Возможность включения/разрыва подключения локальной сети	Определяет, могут ли пользователи включать/разрывать подключения локальной сети. Если включить этот параметр, пользователи (включая неадминистраторов) смогут включать и разрывать подключения локальной сети. Пользователи могут включить/разорвать подключение локальной сети двойным или правым щелчком значка подключения, или используя меню "Файл".
Запретить просмотр состояния активных подключений	Определяет, могут ли пользователи видеть состояние активного подключения. Состояние подключения доступно из значка состояния подключения на панели задач или из диалогового окна состояния. Диалоговое окно состояния отображает информацию о подключении и его активности. Оно также предоставляет кнопки разрыва подключения и настройки его свойств.
Возможность переименовать подключения локальной сети или подключения удаленного доступа, доступные всем пользователям	Определяет, могут ли пользователи переименовать подключения локальной сети или подключения удаленного доступа всех пользователей. Если включить этот параметр, функция "Переименовать" включается для всех пользователей. Пользователи могут переименовать подключения, щелкнув значок подключения или используя меню "Файл".
Запрет включения/отключения компонентов локальной сети	Определяет, могут ли администраторы включать и отключать компоненты, используемые локальными подключениями. Если включить этот параметр (и включить параметр "Включить параметры сетевых подключений для администраторов"), флажки для включения и отключения компонентов отключаются. В результате администраторы не могут включить или отключить компоненты, используемые подключением.
Запрет доступа к мастеру новых подключений	Определяет, могут ли пользователи использовать мастер создания новых подключений.
Запретить пользовательскую настройку автономных файлов	Запрещает пользователям включать, отключать или изменять настройки автономных файлов.
Удалить команду "Работать автономно"	Этот параметр удаляет команду "Работать автономно" из проводника, запрещая пользователям вручную выбирать оперативный или автономный режим использования автономных файлов.
Удалить команду "Сделать доступными автономно"	Этот параметр запрещает пользователям переводить сетевые файлы и папки в автономный режим. Если вы включаете этот параметр политики, пользователи не могут отмечать файлы для сохранения их на компьютере для дальнейшего использования в автономном режиме. Тем не менее, этот параметр не запрещает Windows сохранять локальные копии файлов, хранящихся на общих сетевых ресурсах, для которых задано автоматическое кэширование.
Запретить доступ к мастерам подключений Windows Connect Now	Этот параметр запрещает доступ к мастерам подключений Windows Connect Now (WCN).

Ограничения **Start menu and taskbar**:

Имя	Описание
Удалить кнопку "Отстыковка ПК" из меню "Пуск"	Если этот параметр включен, кнопка "Отстыковка ПК" удаляется из упрощенного меню "Пуск" и компьютер невозможно отстыковать.
Удалить ссылку на папку пользователя из меню "Пуск"	Если эта политика включена, в меню "Пуск" не будет отображаться ссылка на папку пользователя.
Удалить и запретить доступ к командам "Завершение работы", "Перезагрузка", "Сон", "Гибернация" и запрет доступа к ним	Этот параметр запрещает пользователям выполнять из меню "Пуск" или экрана безопасности Windows следующие команды: "Завершение работы", "Перезагрузка", "Сон", "Гибернация". Данный параметр не препятствует пользователям выполнять программы Windows, использующие эти функции.
Удалить папки пользователя из главного меню	Скрывает все папки в пользовательском (верхнем) разделе меню "Пуск". Все остальные элементы отображаются.
Отключить папки программ в меню "Настройка"	Этот параметр позволяет удалять программы из меню "Настройка". Если вы включаете этот параметр политики, папки "Панель управления", "Принтеры" и "Сетевые подключения" удаляются из меню "Настройка" в меню "Пуск", а также из проводника и окна "Компьютер". Кроме того, он запрещает выполнять программы, представленные этими папками (например, CONTROL.EXE).
Удалить ссылку "Ознакомиться с другими результатами" или "Поиск везде"	Если эта политика включена, при выполнении пользователем поиска в поле поиска меню "Пуск" ссылка "Ознакомиться с другими результатами" или "Поиск везде" не будет отображаться.
Удалить меню "Избранное" из главного меню	Запрещает пользователям добавлять меню "Избранное" в меню "Пуск" или классическое меню "Пуск".
Отображение панели "Быстрый запуск" на панели задач	Этот параметр определяет, будет ли панель "Быстрый запуск" отображаться на панели задач.
Добавить команду "Выполнить" в меню "Пуск"	Если этот параметр включен, в меню "Пуск" будет добавлена команда "Выполнить".
Удалить ссылку "ТВ-записи" из меню "Пуск"	Этот параметр позволяет удалить список "Записанные телепередачи" из меню "Пуск".
Отключить контекстные меню в меню "Пуск"	Этот параметр позволяет запретить пользователям открывать контекстные меню в меню "Пуск".
Удалить список всех программ в меню "Пуск"	Если включить этот параметр, меню "Пуск" свернется или из него будет удален список всех приложений.
Закрепить панель задач	Этот параметр влияет на панель задач, которая применяется для переключения между выполняющимися приложениями. Панель задач содержит кнопку "Пуск", список выполняющихся задач и область уведомлений. По умолчанию панель задач располагается внизу экрана, но ее можно переместить к любому краю. Если панель задач закреплена, изменить ее расположение или размер невозможно.
Скрыть область уведомлений	Этот параметр влияет на вид области уведомлений (которая раньше называлась "системной областью") на панели задач.
Удалить часы из системной области уведомлений	Отключает отображение часов в системной области уведомлений. Если этот параметр включен, часы в системной области уведомлений не отображаются.
Показывать команду "Запуск от имени другого	Этот параметр отображает или скрывает команду "Запуск от имени другого пользователя" на панели приложения при запуске. Если этот параметр

пользователя" при запуске	установлен, у пользователя есть доступ к команде "Запуск от имени другого пользователя" при запуске для приложений, поддерживающих эту функцию.
Запретить доступ к контекстному меню для панели задач	Этот параметр позволяет отключить доступ к контекстным меню для панели задач. Если вы включаете данный параметр политики, меню, обычно появляющиеся при щелчке правой кнопкой мыши панели задач и ее элементов, таких как кнопки "Пуск", часов и кнопок панели задач, скрываются.
Удалить команду "Выполнить" из меню "Пуск"	Позволяет удалить команду "Выполнить" из меню "Пуск", браузера Internet Explorer и диспетчера задач.
Удалить значок "Документы" из меню "Пуск"	Этот параметр позволяет удалить значок "Документы" из меню "Пуск" и его подменю. Если вы включаете данный параметр политики, значок "Документы" удаляется из меню "Пуск" и его подменю. При включении этого параметра удаляется только сам значок. Он не запрещает использовать другие методы доступа к содержимому папки "Документы".
Удалить раздел "Люди" с панели задач	Эта политика позволяет удалить панель "Люди" с панели задач и отключить интерфейс "Близкие люди".
Удалить справку из главного меню	Этот параметр позволяет удалить команду "Справка" из меню "Пуск". Если вы включаете данный параметр политики, команда "Справка" удаляется из меню "Пуск".
Запретить изменение параметров панели задач и меню "Пуск"	Этот параметр позволяет запретить изменение параметров панели задач и меню "Пуск". Если вы включаете этот параметр политики, пользователь не сможет открыть окно "Свойства панели задач".
Удалить ссылку "Загрузки" из меню "Пуск"	Этот параметр позволяет удалить список "Загрузки" из меню "Пуск". Если вы включаете этот параметр политики, в меню "Пуск" не отображается ссылка на папку "Загрузки".
Удалить ссылку "Видео" из меню "Пуск"	Этот параметр позволяет удалить ссылку "Видео" из меню "Пуск". Если вы включаете этот параметр политики, в меню "Пуск" не отображается ссылка на библиотеку видео.
Удалить список часто используемых программ в меню "Пуск"	Если этот параметр включен, список часто используемых программ будет удален из меню "Пуск".
Удалить ссылку "Игры" из меню "Пуск"	Если эта политика включена, в меню "Пуск" не будет отображаться ссылка на папку "Игры".
Удалить ссылку "Поиск" из меню "Пуск"	Этот параметр позволяет удалить ссылку "Поиск" из меню "Пуск" и отключает некоторые функции поиска проводника. Обратите внимание на то, что он не удаляет поле поиска из меню "Пуск" в новом стиле. Если вы включаете этот параметр политики, элемент "Поиск" удаляется из меню "Пуск" и из контекстного меню, которое появляется при щелчке правой кнопкой мыши кнопки "Пуск". Кроме того, система не реагирует на нажатие сочетания клавиш Windows+F.
Запретить пользователям настраивать начальный экран	Этот параметр позволяет запретить пользователям изменять макет начального экрана. Если вы включаете этот параметр политики, то пользователь не может выбирать приложение, изменять размер плитки, закреплять и откреплять обычную или вспомогательную плитку, переходить в режим настройки, а также изменять расположение плиток на начальном экране и в разделе "Приложения".
Скрыть общие группы программ в меню "Пуск"	Удаляет элементы для профиля All Users из меню "Программы" в меню "Пуск". По умолчанию меню "Программы" содержит элементы не только из профиля пользователя, но и профиля All Users. Если этот параметр включен, в меню "Программы" отображаются только элементы из профиля пользователя.
Запретить пользователям удалять приложения из меню "Пуск"	Если этот параметр включен, пользователи не могут удалять приложения из меню "Пуск".

Удалить "Сетевые подключения" из меню "Пуск"	Этот параметр позволяет удалить элемент "Сетевые подключения" из меню "Пуск". Если вы включаете этот параметр политики, пользователи не могут открывать папку "Сетевые подключения".
Удалить список программ, закрепленных в меню "Пуск"	Если этот параметр включен, список закрепленных программ удаляется из меню "Пуск". Пользователи не смогут закреплять программы в меню "Пуск".
Добавить пункт выхода из системы в главное меню	Эта политика применяется только к классической версии меню "Пуск" и не влияет на меню "Пуск" нового стиля. Добавляет команду "Завершение сеанса <имя_пользователя>" в меню "Пуск" и запрещает ее удаление.
Удалить ссылку "Программы по умолчанию" из меню "Пуск"	Этот параметр позволяет удалить список "Программы по умолчанию" из меню "Пуск". Если вы включаете этот параметр политики, список "Программы по умолчанию" удаляется из упрощенного меню "Пуск".
Удалить меню "Недавние документы" из меню "Пуск"	Удаляет меню "Недавние документы" из меню "Пуск". Удаляет меню "Недавние документы" из меню "Пуск" классического вида.
Удалить значок "Музыка" из меню "Пуск"	Этот параметр позволяет удалить значок "Музыка" из меню "Пуск". Если вы включаете данный параметр политики, значок "Музыка" удаляется из меню "Пуск".
Удалить список "Недавно добавленные" из меню "Пуск"	Этот параметр позволяет отключить отображение списка недавно установленных программ в меню "Пуск".
Удалить "Завершение сеанса" из меню "Пуск"	Этот параметр позволяет удалить команду "Завершение сеанса <имя_пользователя>" из меню "Пуск" и запретить пользователям ее восстановление. Если вы включаете этот параметр политики, команда "Завершение сеанса <имя_пользователя>" не отображается в меню "Пуск". Данный параметр также удаляет значок "Отображать команду "Завершение сеанса"" из параметров меню "Пуск". В результате пользователи не могут восстановить команду "Завершение сеанса <имя_пользователя>" в меню "Пуск".
Удалить ссылку "Домашняя группа" из меню "Пуск"	Если эта политика включена, в меню "Пуск" не будет отображаться ссылка "Домашняя группа". Кроме того, из параметров меню "Пуск" удаляется элемент домашней группы. Поэтому пользователи не смогут добавлять ссылку на домашнюю группу в меню "Пуск".
Удалить ссылку "Поиск на компьютере"	Если эта политика включена, при выполнении пользователем поиска в поле поиска меню "Пуск" ссылка "Показать все результаты" не будет отображаться.
Добавить ссылку "Поиск в Интернете" в меню "Пуск"	Если эта политика включена, при выполнении пользователем поиска в поле поиска меню "Пуск" ссылка "Поиск в Интернете" будет отображаться. С помощью этой ссылки открывается установленный по умолчанию браузер с соответствующим поисковым запросом.
Удалить значок "Сеть" из меню "Пуск"	Этот параметр позволяет удалить значок "Сеть" из меню "Пуск". Если вы включаете данный параметр политики, значок "Сеть" удаляется из меню "Пуск".
Удаляет ссылки на веб-сайт Центра обновления Windows и запрещает доступ к нему	Этот параметр позволяет отключить ссылки на Центр обновления Windows и доступ к нему.
Отобразить дополнительный календарь	По умолчанию календарь устанавливается согласно языкового стандарта операционной системы, а пользователи могут отображать дополнительный календарь. Для языковых стандартов zh-CN и zh-SG дополнительный календарь отображает лунный месяц и дату и названия праздников на китайском, упрощенное письмо (лунный календарь) по умолчанию. Для языковых стандартов zh-TW, zh-HK и zh-MO дополнительный календарь отображает лунный месяц и дату и название праздников на китайском, традиционное письмо (лунный календарь) по умолчанию.

Запретить перемещение панелей инструментов	Этот параметр позволяет запретить пользователям перемещать панели инструментов. Если этот параметр включен, пользователи не могут перетаскивать панели инструментов на панели задач.
Закрепить все параметры панели задач	Этот параметр позволяет закрепить все параметры панели задач. Если этот параметр включен, пользователи не имеют доступа к панели управления панели задач. Также они не могут изменять размеры, перемещать или изменять расположение панелей инструментов на панели задач.
Удалить индикатор батарей	Этот параметр позволяет удалить индикатор батарей из системной области. Если этот параметр включен, индикатор батарей не будет отображаться в области системных уведомлений.
Удалить закрепленные программы с панели задач	Этот параметр позволяет удалить закрепленные программы с панели задач. Если этот параметр включен, закрепленные программы не отображаются на панели задач. Пользователи не могут закреплять программы на панели задач.
Удалить значок "Безопасность и обслуживание"	Этот параметр позволяет удалить значок "Безопасность и обслуживание" из области управления системой. Если этот параметр включен, значок "Безопасность и обслуживание" не отображается в области системных уведомлений.
Запретить закрепление программ на панели задач	Этот параметр позволяет контролировать закрепление программ на панели задач. Если этот параметр включен, пользователи не могут изменять список программ, закрепленных на панели задач. Если какие-либо программы уже закреплены на панели задач, они останутся в ней. Однако пользователи не смогут откреплять программы, ранее закрепленные на панели задач, а также закреплять на ней новые программы.
Запретить добавление и удаление панелей инструментов	Этот параметр позволяет запретить пользователям добавлять или удалять панели инструментов. Если этот параметр включен, пользователь не может ни добавлять, ни удалять панели инструментов на панели задач. Приложениям также запрещено добавление панелей инструментов.
Запретить изменять расположение панели задач на экране	Этот параметр позволяет запретить пользователям перемещать панель задач в другое расположение на экране. Если этот параметр включен, пользователи не могут перетаскивать панель задач в другую область на мониторе (мониторах).
Удалить значок сети	Этот параметр позволяет удалить значок сети из системной области. Если этот параметр включен, значок сети не будет отображаться в области системных уведомлений.
Запретить изменение размера панели задач	Этот параметр позволяет запретить пользователям изменять размер панели задач. Если этот параметр включен, пользователи не могут изменять размер панели задач.
Показывать приложения Магазина Windows на панели задач	Этот параметр позволяет пользователям видеть приложения Магазина Windows на панели задач. Если этот параметр политики включен, пользователи будут видеть приложения Магазина Windows на панели задач.
Удалить значок регулятора громкости	Этот параметр позволяет удалить значок регулятора громкости из системной области. Если этот параметр включен, значок регулятора громкости не будет отображаться в области системных уведомлений.
Не разрешать закрепление значка Store на панели задач	Этот параметр позволяет управлять закреплением значка Store на панели задач. Если этот параметр включен, пользователи не могут закреплять значок Store на панели задач. Если значок Store уже закреплен на панели задач, он будет удален при следующем входе в систему.
Удалить уведомления и значок центра уведомлений	Этот параметр удаляет уведомления и значок центра уведомлений из области уведомлений на панели задач.

Ограничения **System**:

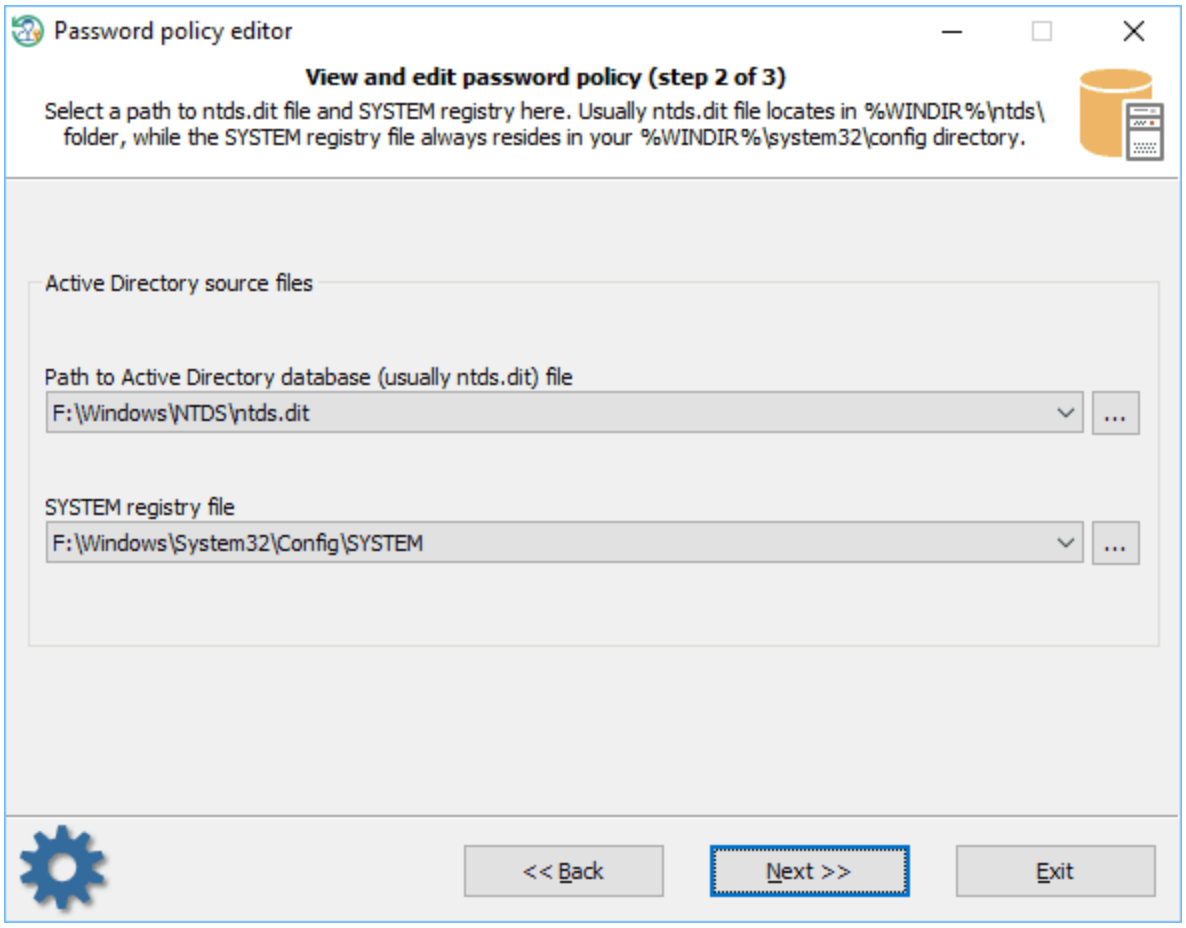
Имя	Описание
Запретить использование командной строки	Запрещает пользователям запускать окно командной строки Cmd.exe. Этот параметр также определяет, могут ли на этом компьютере выполняться пакетные файлы (.CMD и .BAT). Если этот параметр включен и пользователь пытается открыть окно командной строки, система выводит сообщение о том, что это действие запрещено.
Запретить доступ к средствам редактирования реестра	Отключает использование редактора реестра Regedit.exe. Если этот параметр политики включен, а пользователь попытается запустить редактор реестра Regedit.exe, выводится сообщение о том, что выполнение этого действия запрещено.
Не запускать указанные приложения Windows	Запрещает Windows запускать программы, которые вы указываете в данном параметре политики. Если вы включаете этот параметр политики, пользователи не могут запускать программы, которые вы добавляете в список запрещенных приложений.
Выполнять только указанные приложения Windows	Ограничивает список программ Windows, которые могут быть запущены пользователями на компьютере. Если вы включаете этот параметр политики, пользователи могут запускать только те программы, которые вы добавляете в список разрешенных приложений.
Запретить выход из системы	Этот параметр отключает или удаляет все команды меню и кнопки, которые позволяют пользователю выполнить выход из системы. Если этот параметр включен, после нажатия клавиш CTRL+ALT+DEL команда меню "Выйти из системы" не будет видна. При этом все способы выхода из системы будут невозможны, за исключением перезагрузки или выключения компьютера.
Удалить диспетчер задач	Этот параметр запрещает пользователям запускать диспетчер задач.
Запретить изменение пароля	Этот параметр запрещает пользователям изменять свой пароль по собственному желанию. Включение этого параметра отключает кнопку "Смена пароля" в диалоговом окне "Безопасность Windows" (которое появляется при нажатии клавиш CTRL+ALT+DEL).
Запретить блокировку компьютера	Этот параметр запрещает пользователям блокировать систему. Когда система блокирована, рабочий стол скрыт и система использоваться не может. Блокировку может отменить только пользователь, заблокировавший систему, либо системный администратор. Если этот параметр включен, пользователи не могут блокировать компьютер с помощью клавиш CTRL+ALT+DEL.
Съемные запоминающие устройства всех классов: Запретить любой доступ	Настроить доступ к съемным запоминающим устройствам всех классов.
Съемные диски: Запретить чтение	Этот параметр запрещает чтение со съемных дисков.
Съемные диски: Запретить запись	Этот параметр запрещает запись на съемные диски.
Компакт-диски и DVD-диски: Запретить чтение	Этот параметр запрещает чтение с дисководов для компакт-дисков и DVD-дисков.
Компакт-диски и DVD-диски: Запретить запись	Этот параметр запрещает запись на дисководы для компакт-дисков и DVD-дисков.
WPD-устройства: Запретить чтение	Этот параметр запрещает чтение со съемных дисков, в том числе с проигрывателей, сотовых телефонов, дополнительных дисплеев и CE-устройств.
WPD-устройства: Запретить запись	Этот параметр запрещает запись на съемные диски, в том числе на проигрыватели, сотовые телефоны, дополнительные дисплеи и CE-устройства.
Накопители на гибких дисках: Запретить чтение	Этот параметр запрещает чтение с дисководов для гибких дисков, в том числе и с USB-дисководов.

Накопители на гибких дисках: Запретить запись	Этот параметр запрещает запись на дисководы для гибких дисков, в том числе и на USB-дисководы.
Ленточные накопители: Запретить чтение	Этот параметр запрещает чтение с ленточных накопителей.
Ленточные накопители: Запретить запись	Этот параметр запрещает запись на ленточные накопители.

3.2.6 Редактор политики паролей

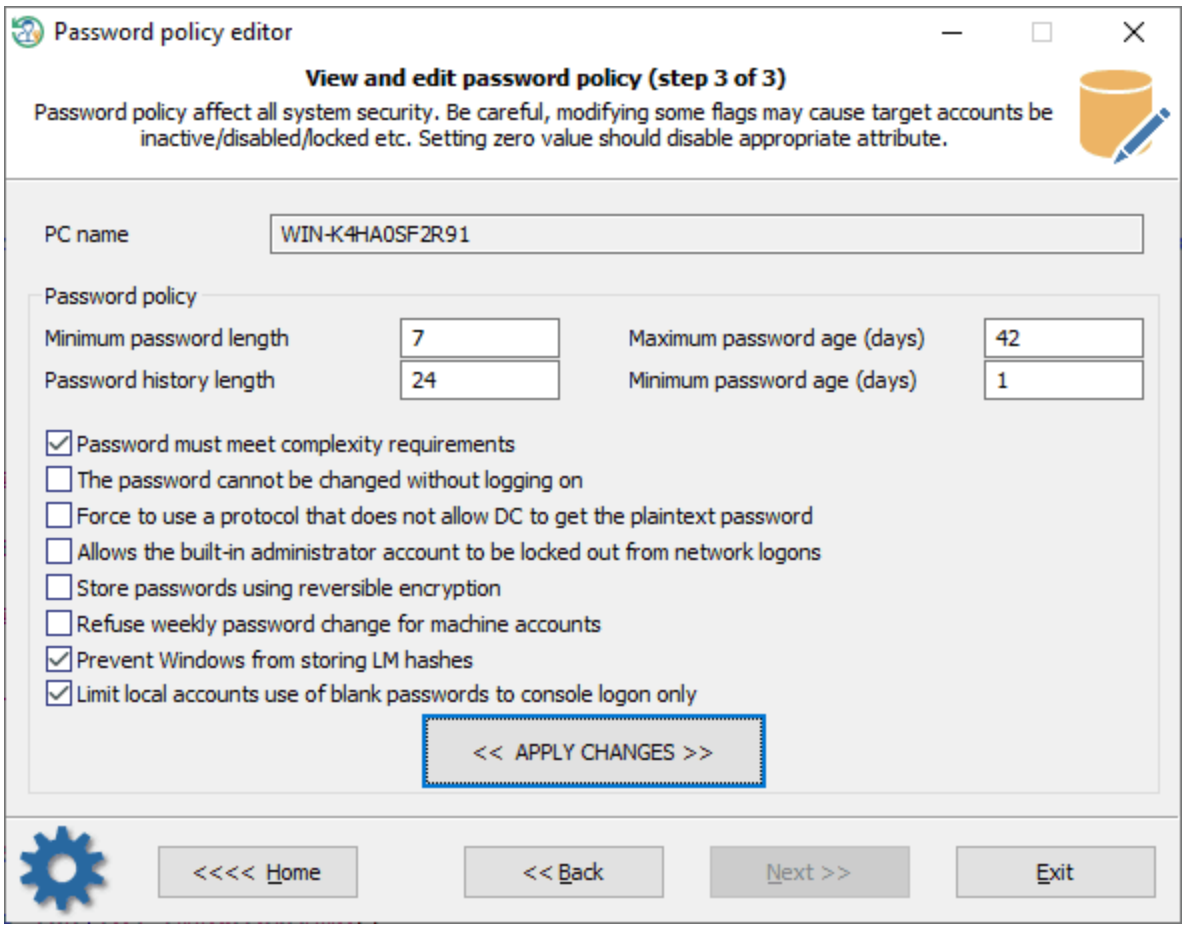
Иногда для безопасного функционирования системы требуется изменить локальную или доменную политику паролей. Например, для предотвращения доступа пользователей к системе без предоставления сложного и устойчивого к взлому пароля. Тем не менее, это может быть довольно затруднительно, если отсутствует администраторский доступ к системе. Функция редактирования политики паролей поможет преодолеть проблему доступа и задать, установить или изменить необходимый атрибут политики паролей любой операционной системы Windows.

Выбор источника данных



Прежде всего, необходимо указать программе два системных файла:
- либо **SAM** и **SYSTEM,** в случае, если редактируется политика паролей рабочей станции или обычного ПК
- либо **NTDS.DIT** и **SYSTEM, если надо изменить политику паролей** домена.
Программа автоматически находит требуемые файлы, но вы можете указать пути к ним и в ручном режиме.

Редактор политики паролей



Краткое описание доступных для редактирования атрибутов политики паролей:

- Minimum password length - минимальное количество знаков, которое должно содержаться в пароле пользователя.
- Password history length - длина истории предыдущих паролей. Пользователю не разрешается использовать старые пароли из этого списка. Число паролей в истории должно составлять от 0 до 25.
- Maximum password age - максимальный срок действия пароля (в днях). Этот параметр безопасности определяет период времени, в течение которого можно использовать пароль, пока система не потребует от пользователя сменить его.
- Minimum password age - период времени (в днях), в течение которого необходимо использовать пароль, прежде чем пользователь сможет его изменить. Можно установить значение от 1 до 999 дней либо разрешить изменять пароль сразу, установив значение 0 дней.
- Password must meet complexity requirements - если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям: не содержать имени учетной записи пользователя или его частей, не соответствовать одному из используемых ранее паролей, хранящихся в истории паролей (если она задана), иметь длину не менее 6 знаков, содержать символы как минимум из трех разных наборов.

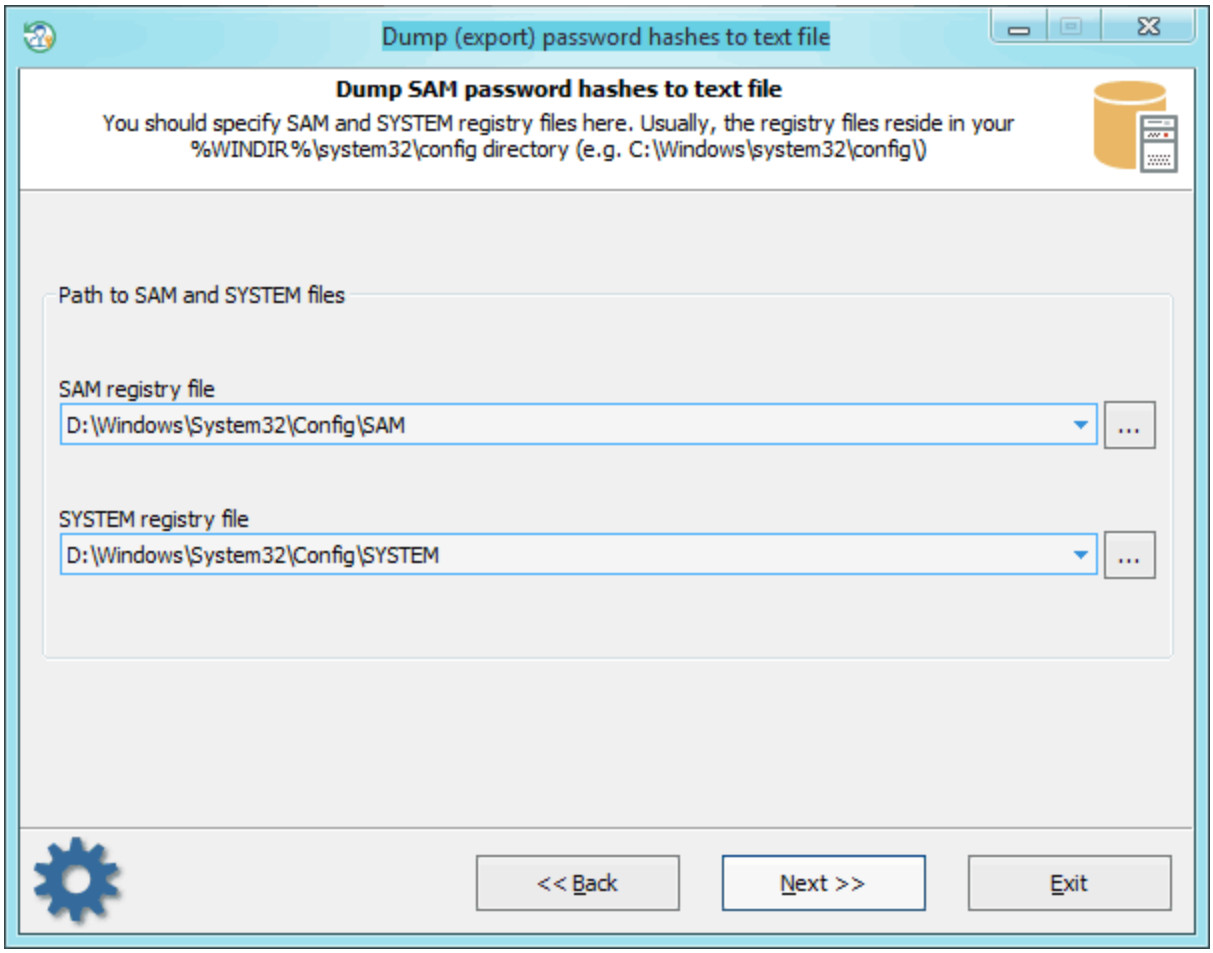
- The password cannot be changed without logging on - пароль не может быть изменен без входа в систему. В противном случае, если вышел срок действия пароля, вы можете изменить его, а затем войти в систему.
- Force to use a protocol that does not allow DC to get the plaintext password - заставляет клиента использовать протокол, не позволяющий контроллеру домена получать текстовые пароли.
- Allows the built-in administrator account to be locked out from network logons - позволяет блокировать встроенную учетную запись администратора от доступа к сети.
- Store passwords using reversible encryption - хранить пароли, используя обратимое шифрование (вместо парольных хэшей).
- Refuse weekly password change for machine accounts - устраняет необходимость автоматической еженедельной смены пароля для учетных записей компьютера.
- Запретить хранение LM хэшей. При хэшировании LAN Manager используется чрезвычайно слабый алгоритм шифрования. Эта опция определяет, может ли LM-хэш пароля храниться в Active Directory и локальной базе данных SAM (при создании нового или изменении пароля текущего пользователя). Этот параметр включен по умолчанию в Windows Vista и более поздних операционных системах.
- Ограничить использование пустых паролей локальными учетными записями только для консольного входа в систему. Не допускать существования в системе учетных записей с пустыми паролями. Однако если локальная учетная запись с пустым паролем уже существует, включение этого параметра предотвратит доступ к сети, ограничив учетную запись только входом в локальную консоль.

Для отключения редактируемого атрибута, просто введите ноль в поле ввода.

Внимание, изменение любого значения политики паролей влияет на безопасность всей системы Windows!

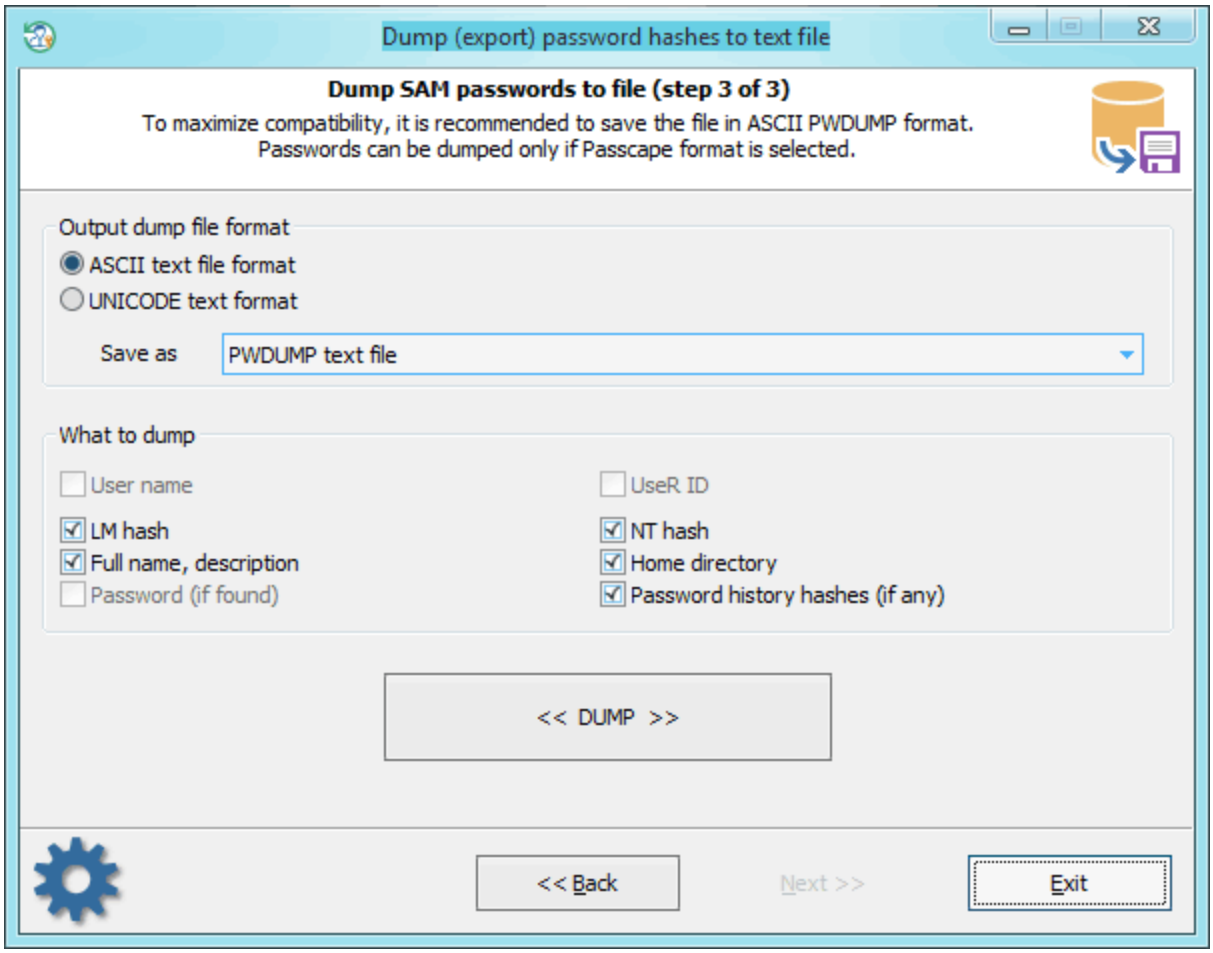
3.2.7 Дамп (экспорт) парольных хэшей

Выбор источника данных



На этом этапе вам следует указать месторасположение SAM и SYSTEM файлов. Или, в случае с пользователями домена, файлы ntds.dit и SYSTEM.

Дамп парольных хэшей



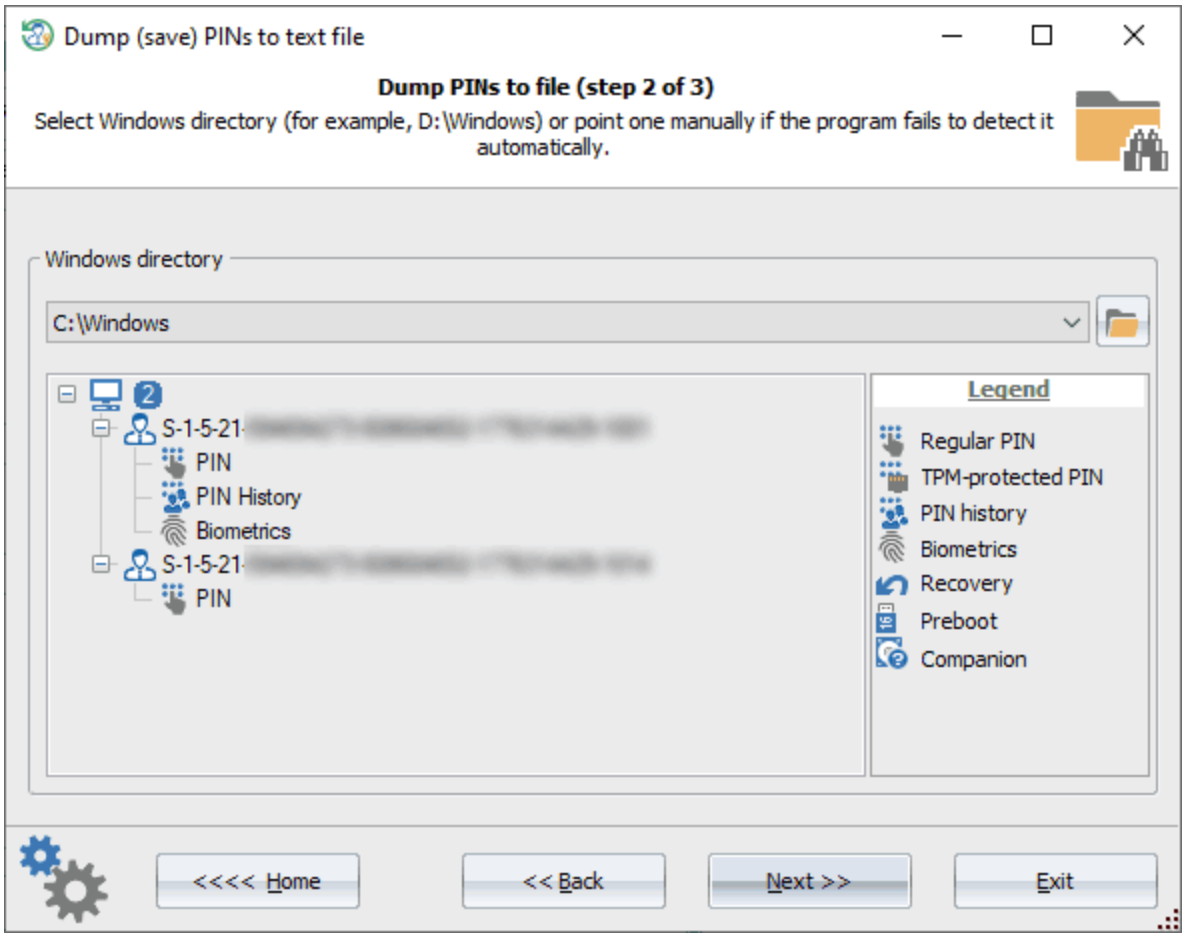
Выбираем формат и тип дамп-файла. При генерации дампа, можно также удалить, если это не имеет для вас никакого значения, отдельные ненужные атрибуты учетной записи. Если выбран формат Passcape, то имеется возможность дампа plaintext паролей. Программа сканирует ваш компьютер на предмет наличия оных и, если таковые имеются, сопоставляет их с учетными записями, сохраняя в дамп-файл.

Текстовые пароли хранятся в домене, при установленной опции 'Store passwords using reversible encryption for all users in the domain', которую можно найти в консоли групповой политики.

В дальнейшем, дамп-файл можно использовать в различных программах для аудита и восстановления паролей. Заметьте также, что Reset Windows Password, благодаря технологии AI attack, разработанной в Passcape Software, позволяет расшифровывать пароли некоторых учетных записей практически мгновенно, без перебора. Подробности смотрите в разделе Поиск паролей пользователей.

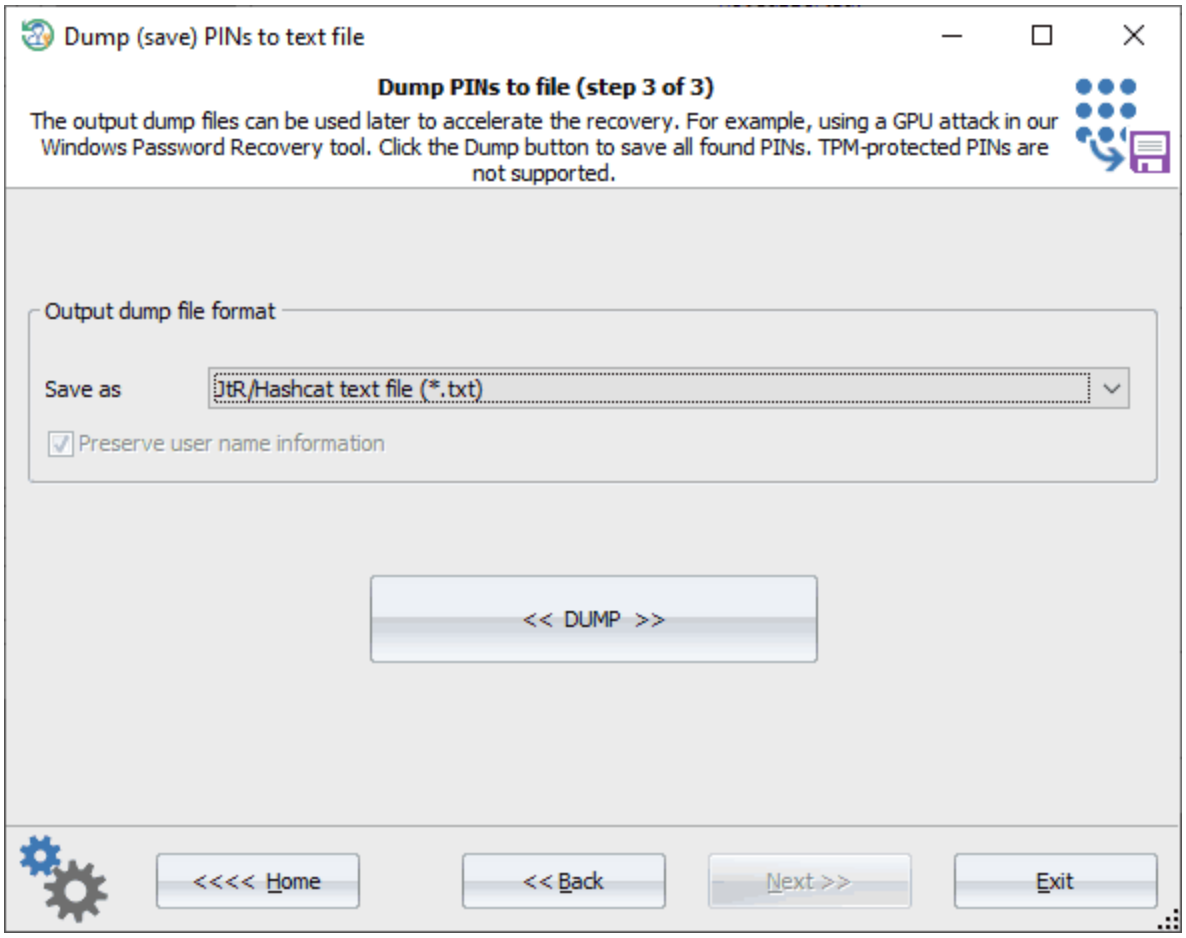
3.2.8 Дамп (сохранение) PIN в файл

Выбор каталога Windows



После выбора каталога Windows, будет доступен информационный список пользователей, у которых установлен вход по PIN-коду.

Дамп Windows PIN

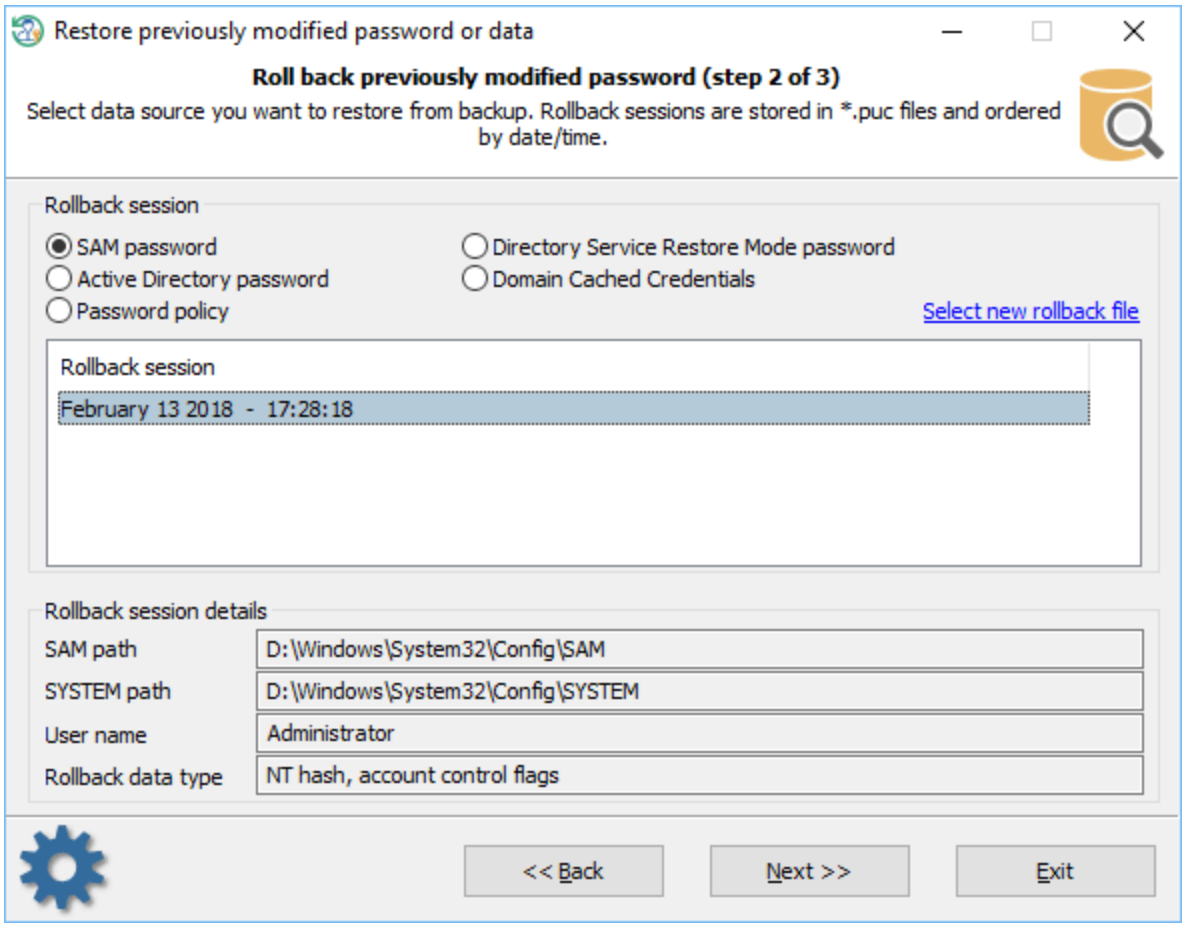


Программа умеет сохранять PIN коды Windows в формате hashcat (*.txt) и Elcomsoft (*.pin). Оба формата частично совместимы.

В последствие вы можете использовать сохраненные дампы для загрузки в сторонние программы. Например, наша утилита для аудита паролей Windows Password Recovery поддерживает оба формата и имеет поддержку GPU для ускорения поиска.

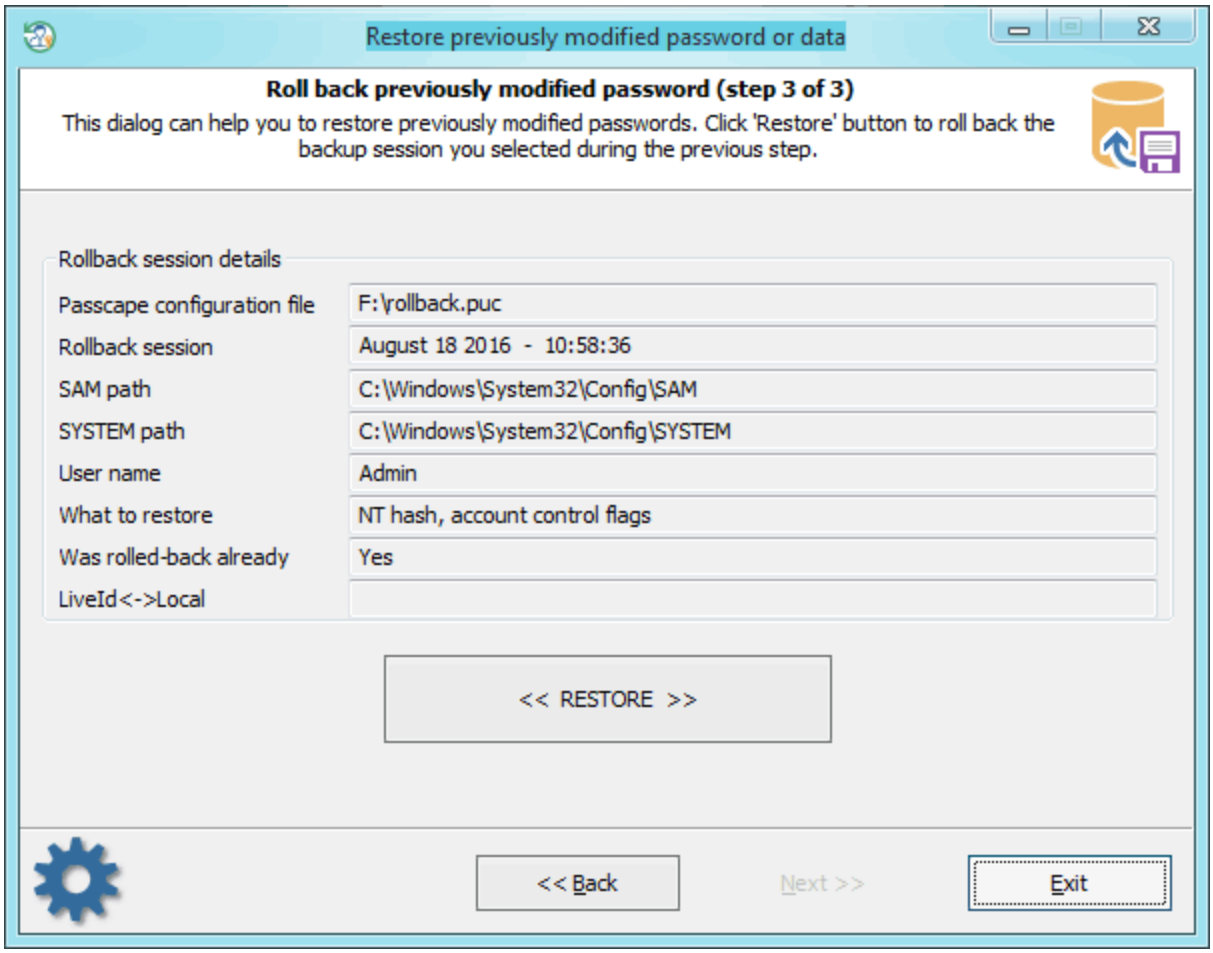
3.2.9 Откат сделанных ранее изменений

Выбор файла отката



Если вам по какой-либо причине требуется откатить (т.е. вернуть на место) пароль, который уже был сброшен или изменен раннее, на втором шаге Мастера необходимо указать программе *.puc файл с сессиями отката. Активируйте соответствующий тип пароля, которые требуется восстановить: пароль обычной учетной записи SAM, Active Directory, пароль DSRM или кэшированный пароль домена, настройки политики паролей. После этого выберите дату, когда было произведено изменение.

Восстановление измененного ранее пароля



На третьем шаге программа предложит вам изучить детали сессии отката из которых особое внимание следует уделить последним трем пунктам:

- Имя учетной записи, над которой производится действо.
- Данные, подлежащие откату. Это та информация, которую вы уже изменили когда-то.
- Была ли текущая сессия отката уже использована вами ранее.

Рассмотрим, например, такую ситуацию:
Эксперту по компьютерной безопасности необходимо произвести вход в Windows по определенной учетной записи. Пароль учетной записи неизвестен. При этом необходимо сделать так, чтобы пароль этой учетной записи остался не измененным.

Порядок действий:

- Загружаем Reset Windows Password, выбираем соответствующую учетную запись и сбрасываем ее пароль. При этом сохраняем сессию отката в *.puc файл (программа сама предложит это сделать во время изменения пароля).
- Закрываем Reset Windows Password и загружаем Windows. Входим под измененной учетной записью с пустым паролем. Производим соответствующие действия.
- Теперь необходимо восстановить старый пароль для учетной записи. Для этого опять перезагружаемся и запускаем Reset Windows Password. В главном меню выбираем пункт 'Восстановление ранее

измененного пароля', указываем путь к файлу отката, в котором были запомнены внесенные ранее изменения, и время, когда они были произведены. Переходим на третий этап и убеждаемся, что это именно та учетная запись, которая нам необходима. Нажимаем на кнопку **<< Восстановить >>** и старый пароль будет восстановлен.

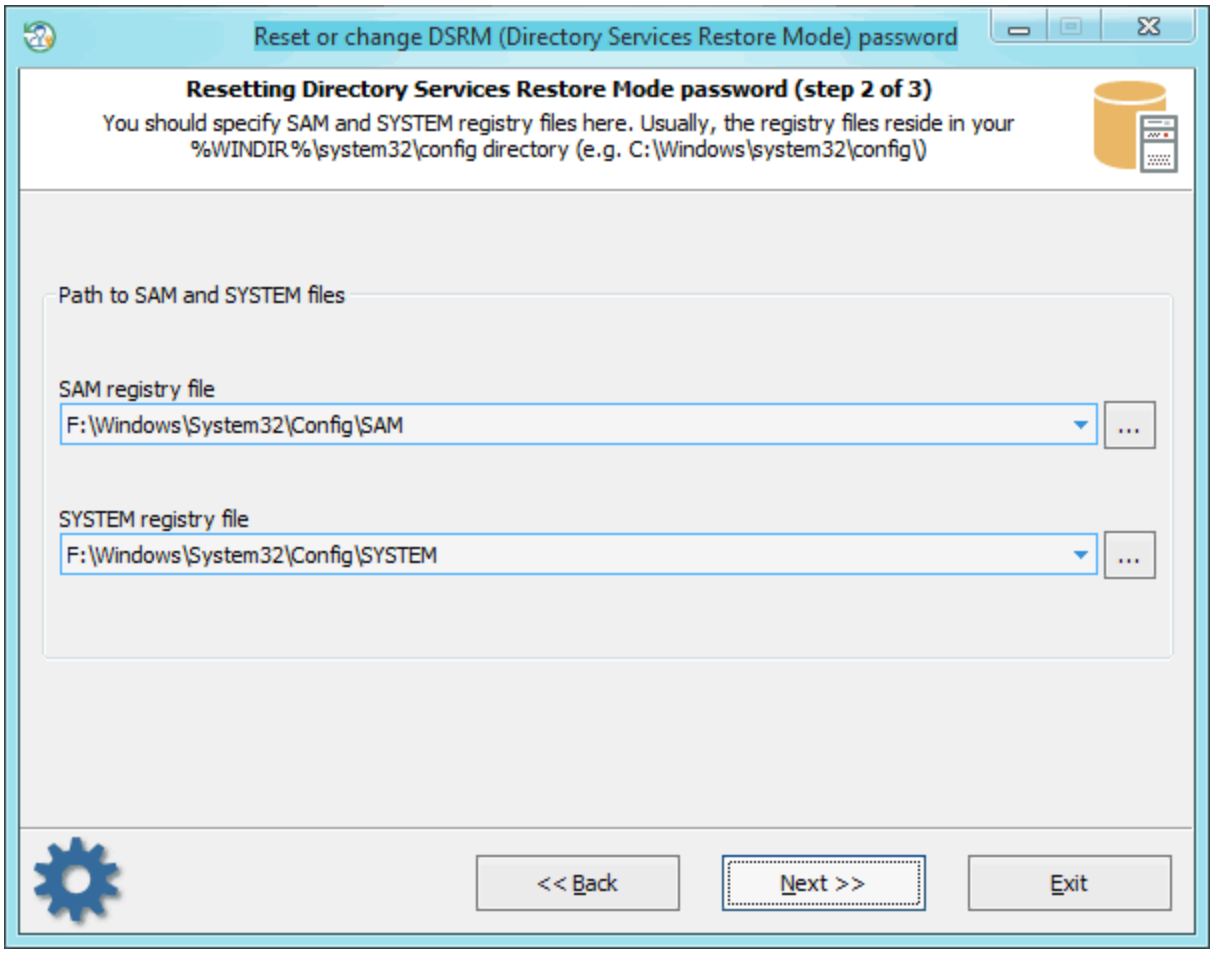
3.3 Учетные записи Active Directory

3.3.1 Сброс пароля DSRM

Что такое DSRM

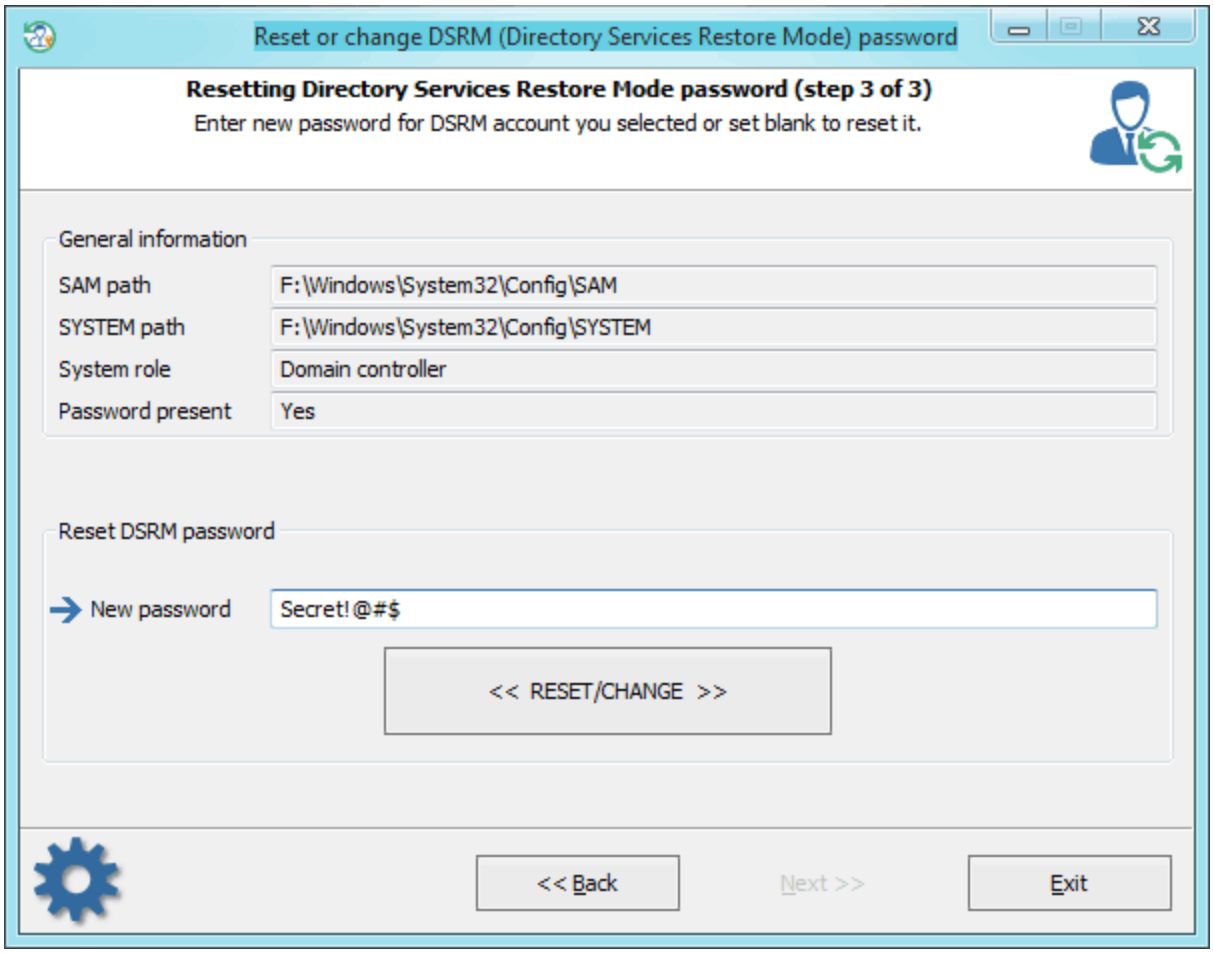
DSRM (аббревиатура от **Directory Services Repair Mode** или **Directory Services Restore Mode** в старых версиях Windows до Windows Server 2012) это специальный режим работы операционной системы Windows, предназначенный для восстановления Active Directory. Например, когда Active Directory повреждена и нуждается в исправлении. DSRM используется для восстановления Active Directory из резервных копий, исправления различных ситуаций и проблем с AD, а также для сброса забытых паролей пользователей и администраторов.
В этом плане DSRM чем то похож на безопасный режим с поддержкой сети, но с отключенной Active Directory. Также, как и в безопасном режиме, чтобы попасть в него, необходимо несколько раз нажать на F8 во время загрузки Windows (после BIOS/UEFI POST, но до появления логотипа с загрузкой Windows). В Windows Server 2012 и более поздних Операционных Системах для этого есть соответствующие пункты в меню **Advanced Boot Options** и **Windows Recovery Environment**.

Выбор источника данных



Учетная запись Directory Service Restore Mode является по сути обычной учетной записью. Поэтому в качестве исходного пути к ней следует указать месторасположение двух системных файлов реестра: **SAM** и **SYSTEM**. Обычно они находятся в каталоге C:\Windows\system32\config.

Сброс пароля

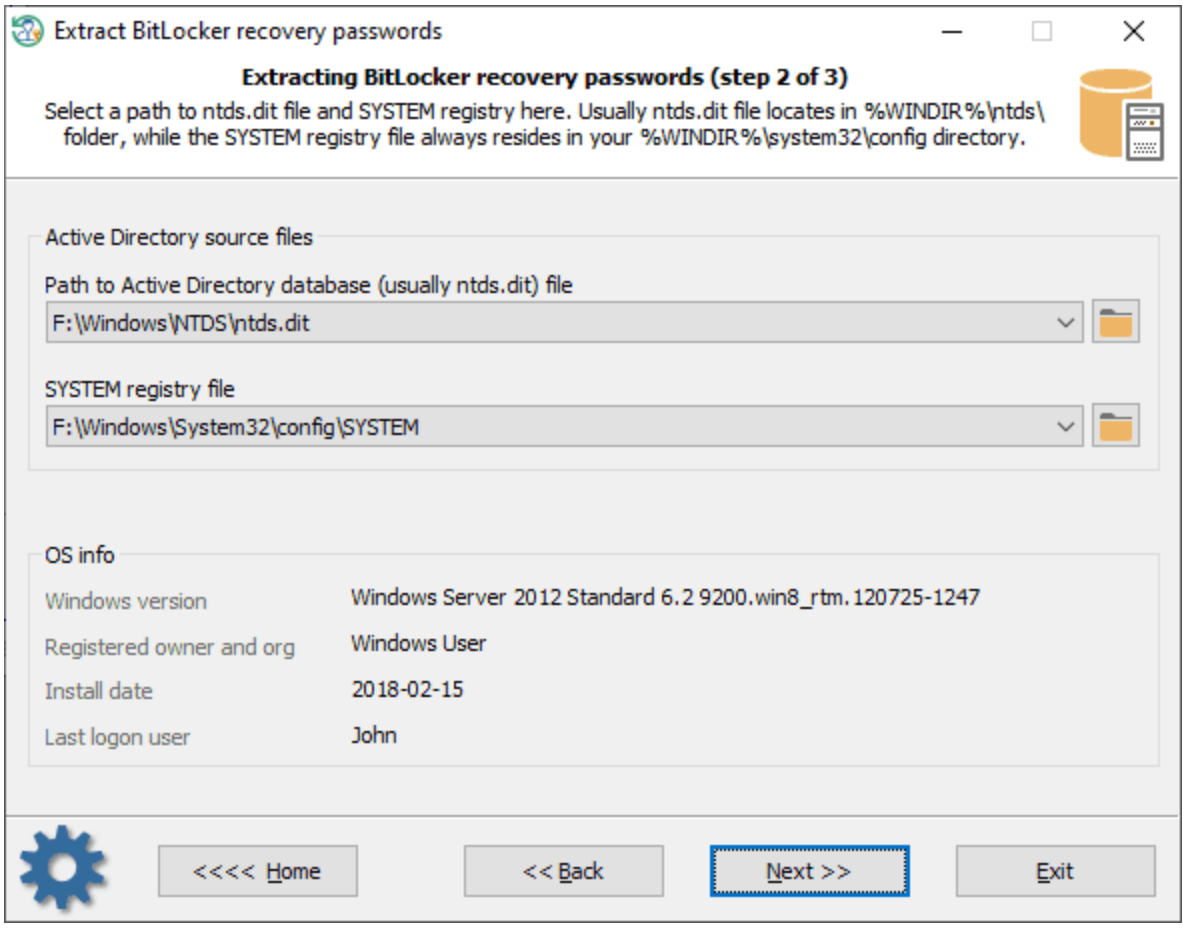


Очистите поле ввода (для сброса) или введите другой пароль для изменения. Затем нажмите на кнопку 'RESET/CHANGE' чтобы начать процедуру изменения. Программа может попросить вас о создании файла отката, в котором будет сохраниться сделанные в системе изменение. Впоследствии вы можете использовать данный файл для восстановления старого пароля DSRM.

3.3.2 Поиск ключей BitLocker

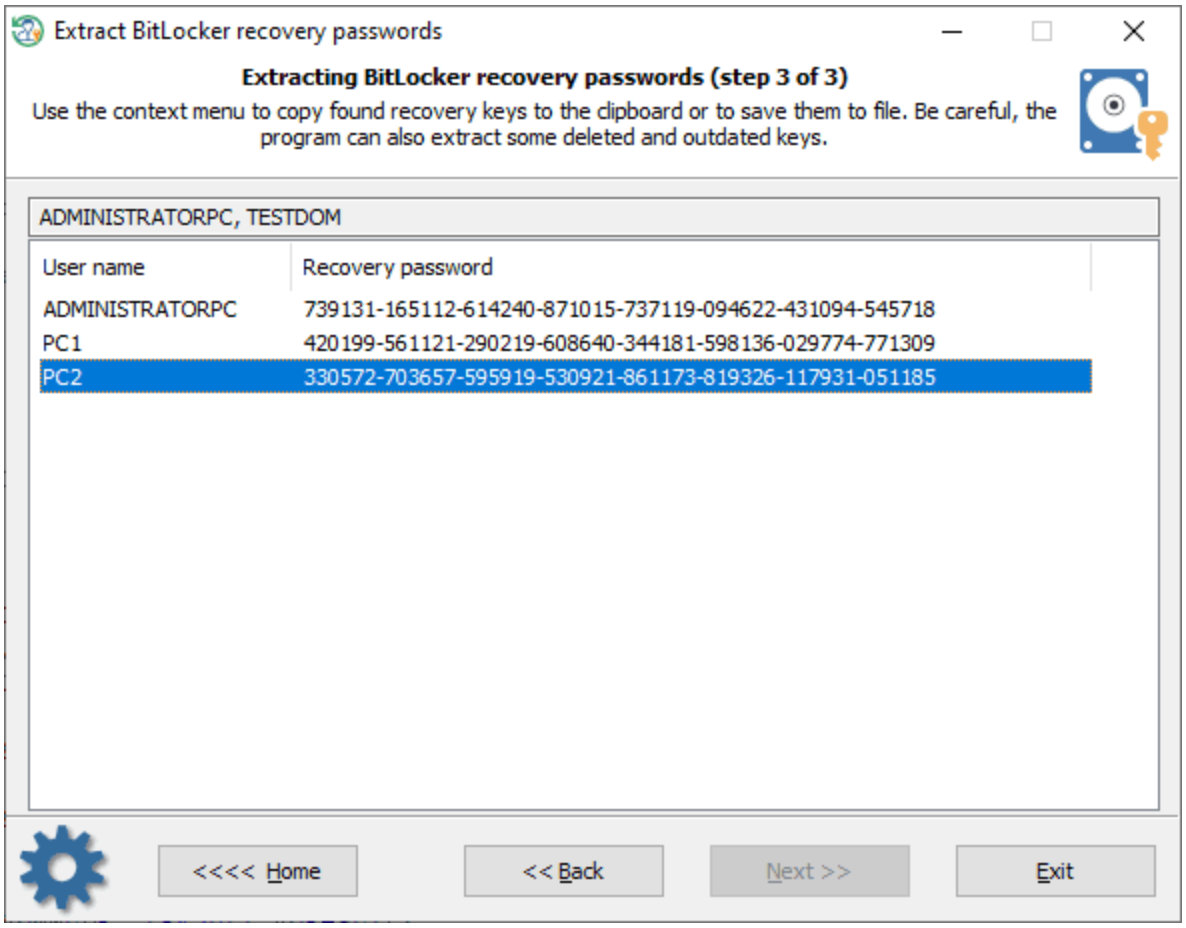
Очень часто пароли восстановления BitLocker хранятся в домене в базе данных Active Directory. Данная функция программы предназначена для извлечения паролей BitLocker даже из неработающего домена.

Выбор источника данных



В начале необходимо указать путь к реестру **SYSTEM** и файлу **NTDS.DIT**. Программа автоматически находит требуемые файлы, но можно указать пути к ним вручную.

Восстановление паролей BitLocker



Будьте осторожны, не всегда есть возможность получить реальные имена пользователей, владельцев ключей. Кроме того, программа может дополнительно извлекать просроченные и удаленные ключи BitLocker.

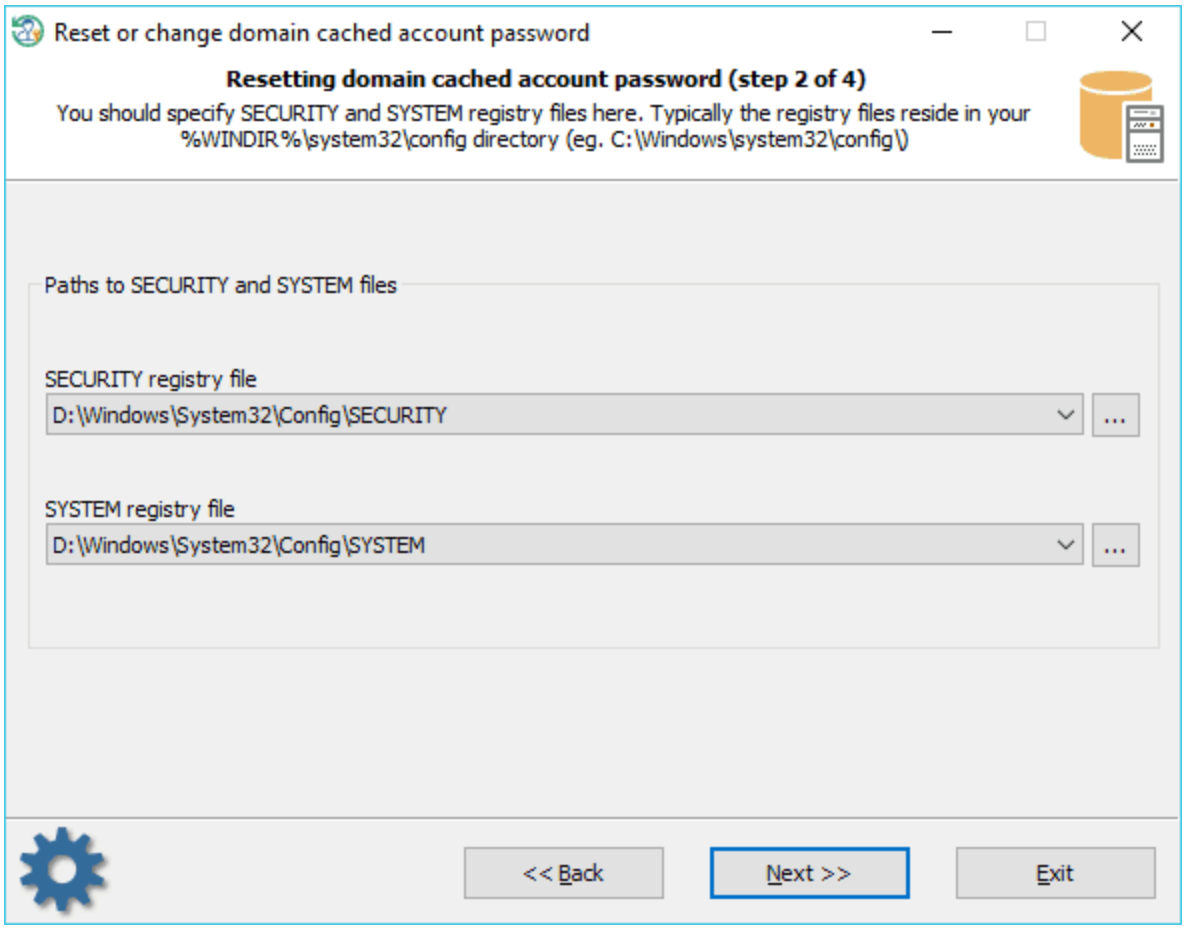
Необходимый ключ можно скопировать в буфер обмена или сохранить в файл.

3.4 Кэшированные записи домена

3.4.1 Сброс кэшированного пароля домена

При входе пользователя в домен Windows, учетные данные пользователя могут кэшироваться и сохраняться на локальном компьютере. Кэширование позволяет пользователям входить в домен, когда локальная рабочая станция отключена от сети или если контроллер домена недоступен. Однако, если пароль домена потерян или забыт, можно обойти эту проблему и войти в учетную запись домена, просто сбросив кэш домена при помощи Reset Windows Password.

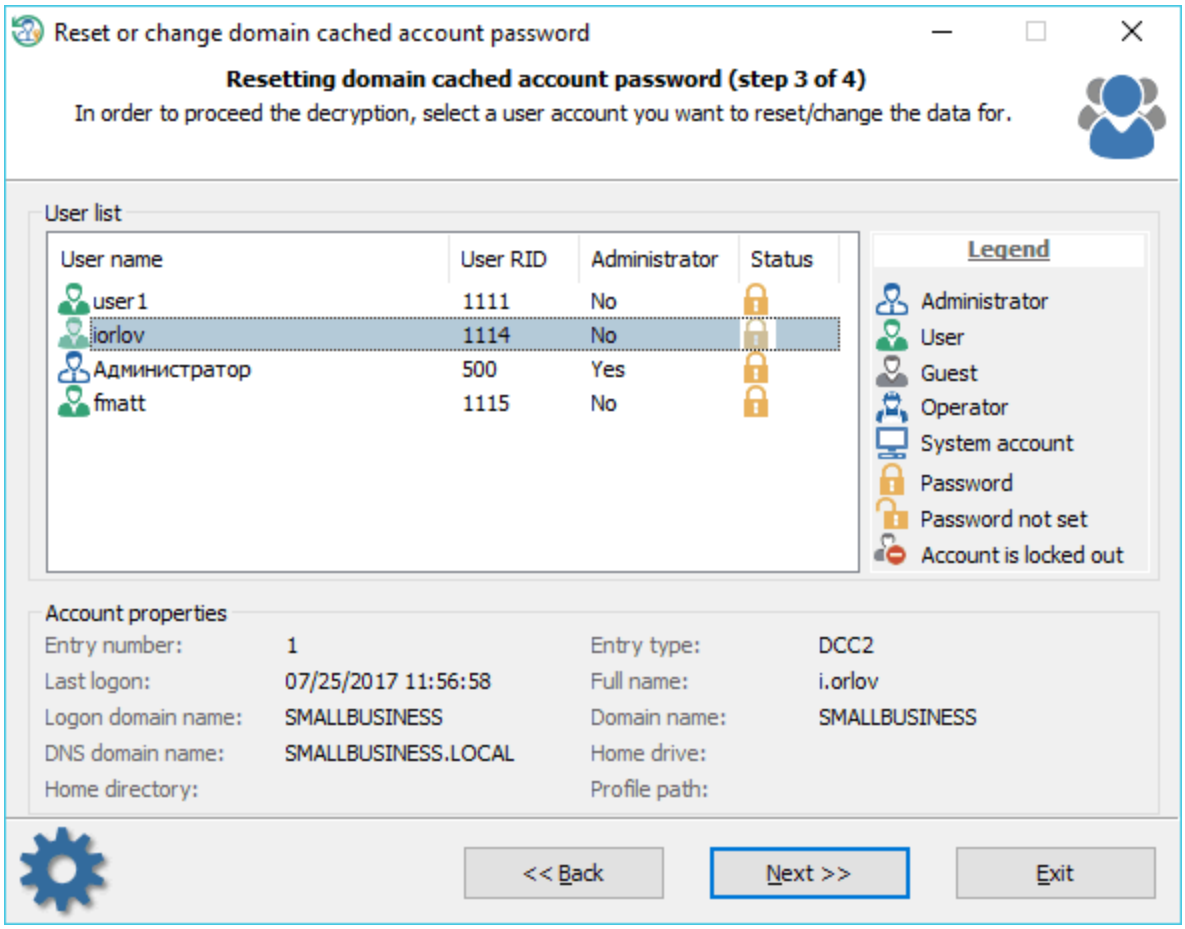
Выбор файлов реестра



Для работы с кэшированными записями домена необходимо указать путь к файла реестра **SECURITY** и **SYSTEM**, которые находятся в каталоге **%WINDIR%\system32\config**. Где **%WINDIR%** - каталог Windows. Как правило, программа определяет эти файлы автоматически.

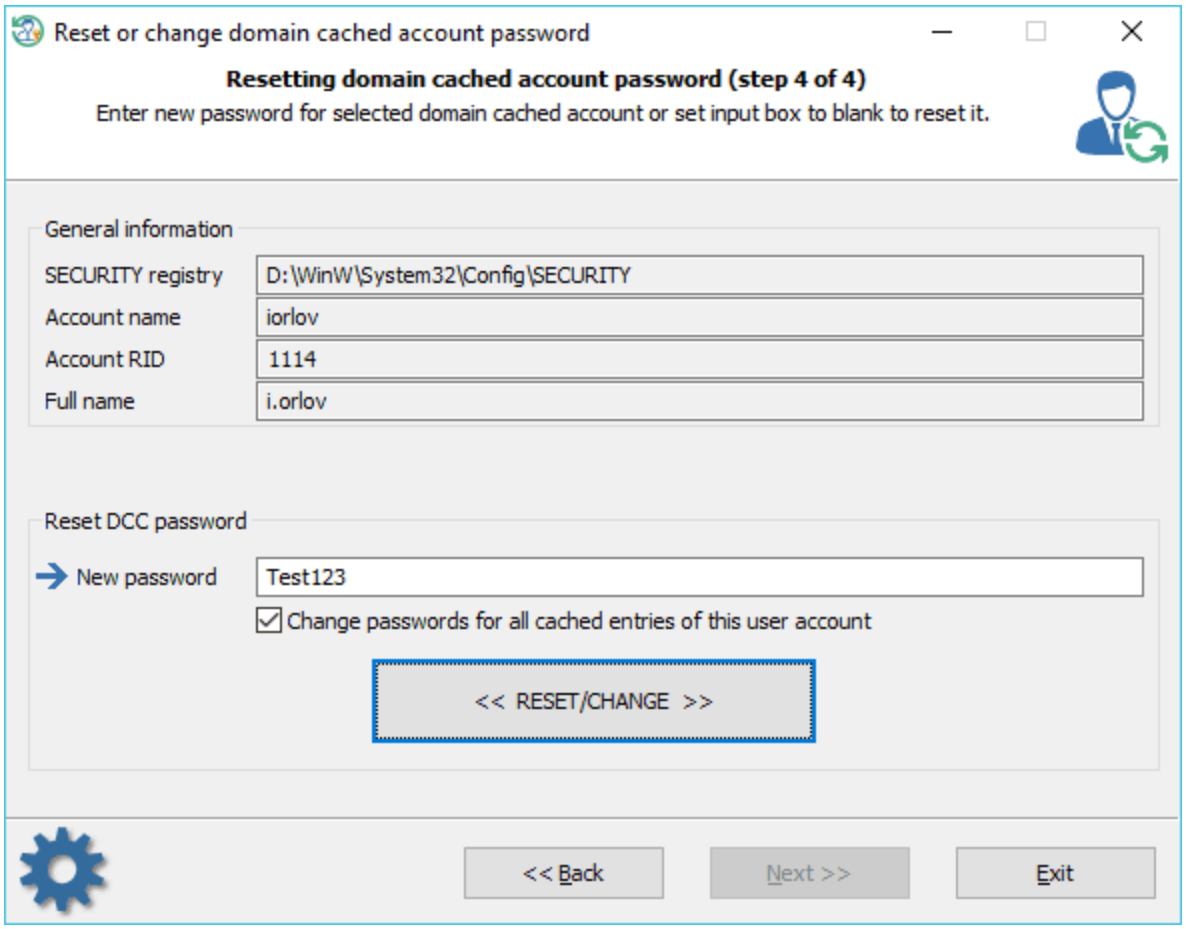
Перед тем, как продолжить работу, обязательно убедитесь, что файлы реестра были выбраны правильно.

Выбор кэшированной записи домена



В верхней части диалога отображается список найденных записей с именами пользователей. Выбрав одну из записей, можно просмотреть ее свойства: полное имя пользователя, последнюю дату входа, домен входа, домашний каталог и др.

Сброс пароля



Для сброса, оставьте поле ввода 'Новый пароль' пустым и нажмите на кнопку '*Сбросить/Изменить*'. Обратите внимание на дополнительную опцию. Кэш домена устроен таким образом, что может содержать несколько записей одного и того же пользователя. Если установлена опция '*Изменять пароли всех кэшированных записей для этого пользователя*', то программа изменит/сбросит пароли всех найденных записей выбранного пользователя с указанным RID. Иначе будет сброшен пароль только одной выбранной записи. Рекомендуется оставлять эту опцию включенной.

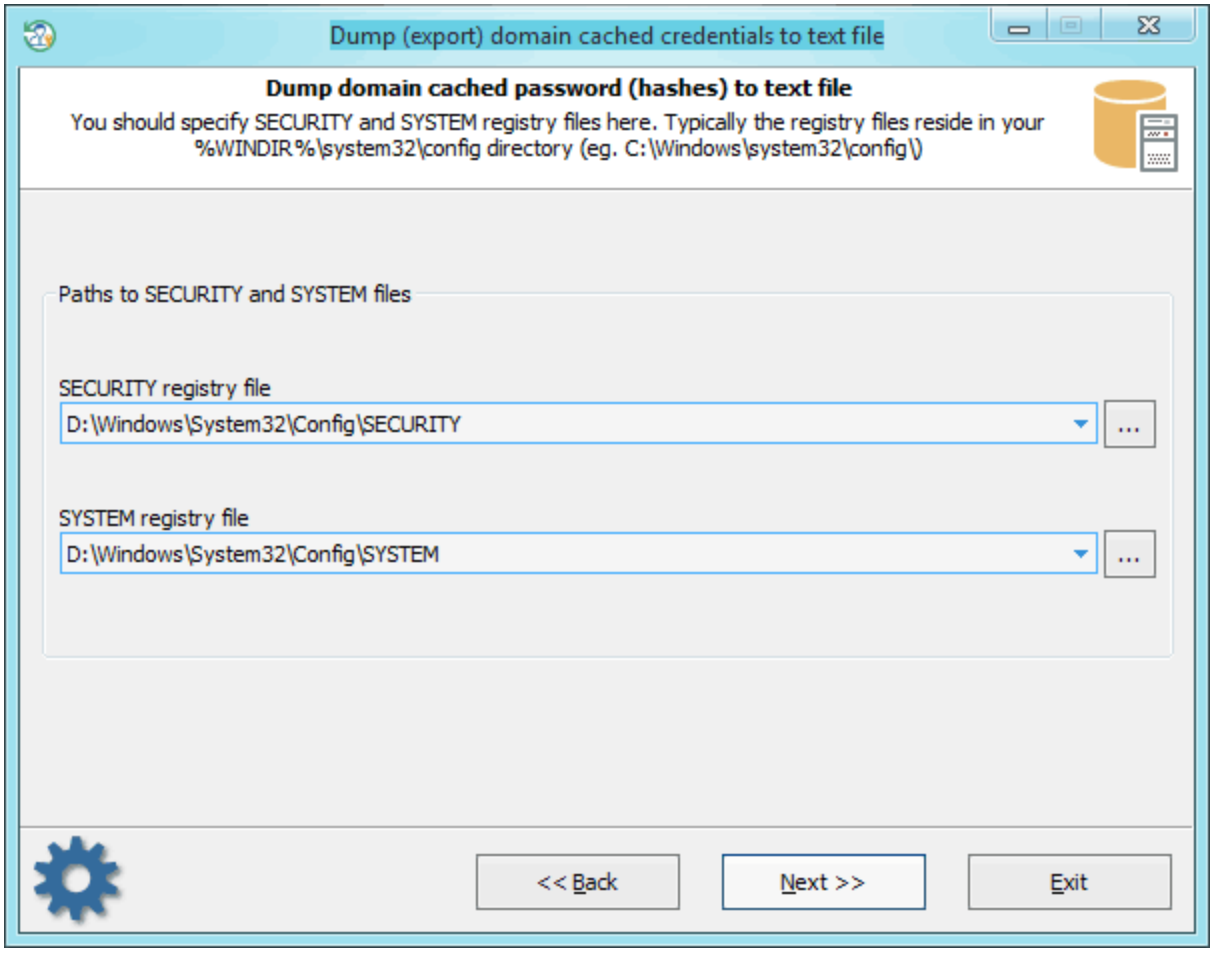
Если в домене используется политика безопасности, убедитесь, что новый пароль соответствует требованиям длины и сложности и не совпадает ни с одним из введенных ранее паролей. В противном случае, Windows может отказать в доступе, даже если пароль был успешно изменен.

Обратите внимание, для успешного входа в учетную запись после сброса кэшированного пароля домена, необходимо временно отключить ПК с учетной записью от домена. В противном случае, система не будет использовать кэшированные записи и вход с новым паролем будет невозможен!

Имейте в виду, вход в домен с кэшированным паролем дает доступ только к локальным ресурсам.

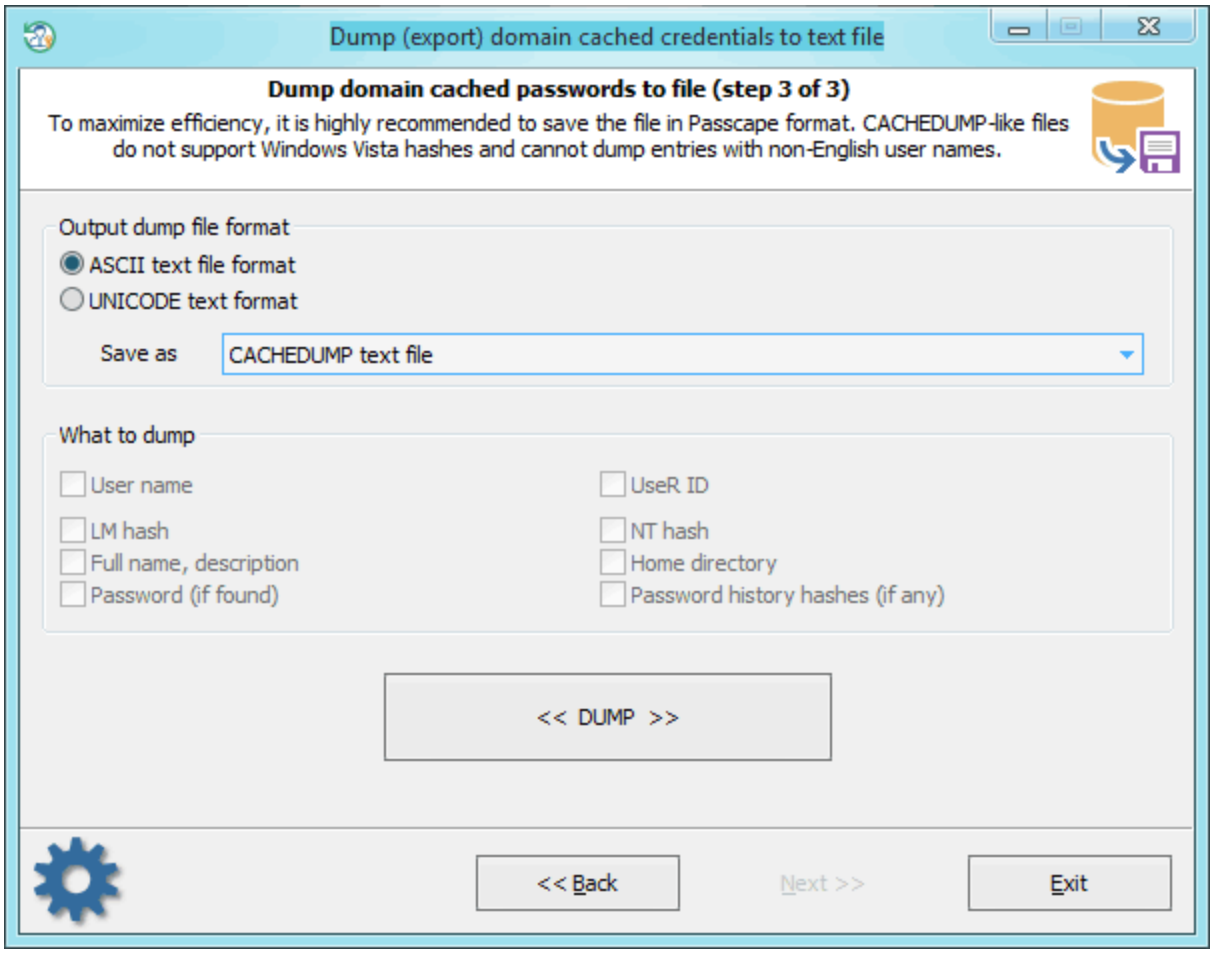
3.4.2 Дамп (экспорт) кэшированных паролей домена

Выбор источника данных



Для расшифровки кэшированных паролей домена, программе требуется знать расположение двух системных файлов реестра: SECURITY и SYSTEM. Выбирете их из списка, либо, если программа по какой-то причине не смогла их найти, укажите путь к ним в ручную.

Дамп кэшированных паролей домена



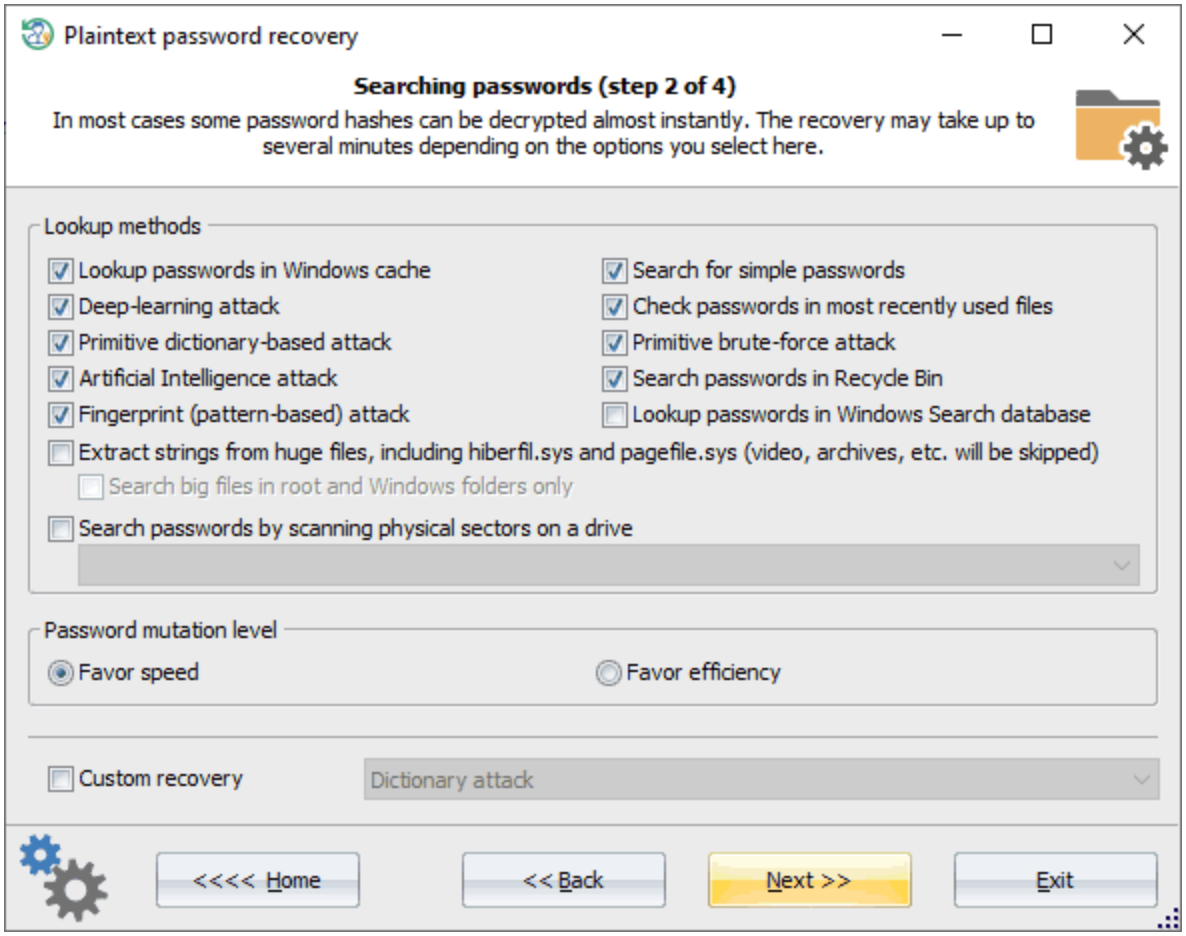
В финальном диалоге доступны всего две опции:
- **Формат дамп файла**. ASCII хорош для всех случаев, но могут быть проблемы с неанглийскими именами пользователей и, соответственно, с дальнейшим анализом и расшифровкой этих хэшей. UNICODE поддерживает все языки, но могут быть проблемы совместимости с чтением этого формата в различных программах.
- **Тип дамп-файла** может быть либо CACHEDUMP - простой, но широко распространенный формат. Не будет проблем совместимости. Однако этот фрмат накладывет ряд ограничений. Во-первых, он не поддерживает неанглийские имена пользователей. Соответственно, в дальнейшем, невозможно будет расшифровать пароль учетной записи, т.к. он привязан к этому имени. Во вторых, текущая версия формата CACHEDUMP не поддерживает операционные системы Windows Vista и выше.

Формат Passcape лишен этих недостатков и может быть с успехом использован в таких программах для аудита и восстановления паролей как, например, Network Password Recovery Wizard.

3.5 Пароли

3.5.1 Поиск паролей пользователей

Установка опций поиска и методов восстановления



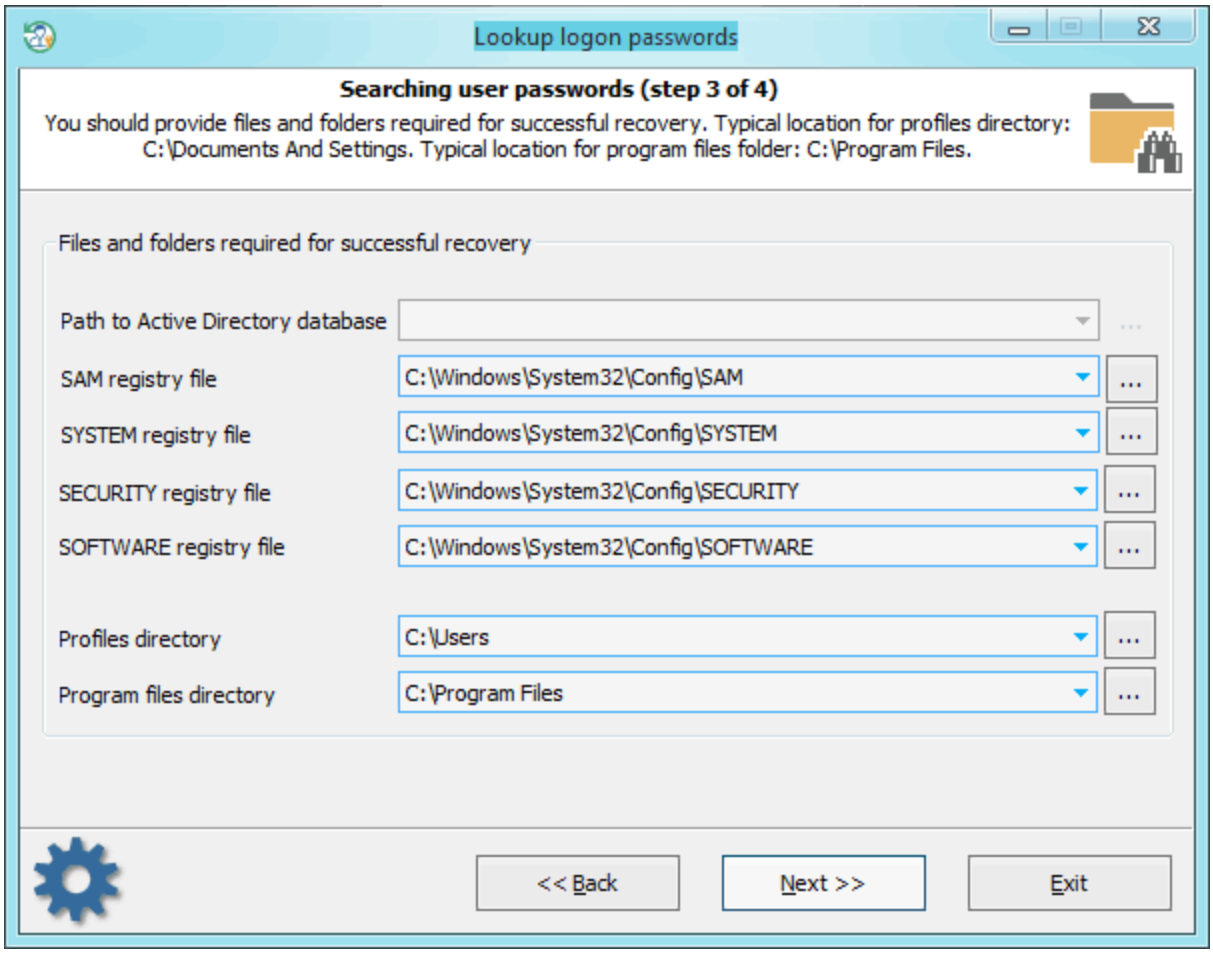
Поиск паролей пользователя происходит последовательно в 11 основных этапов:

1. Поиск информации в системном кэше Windows. Данный метод в свою очередь состоит из более чем дюжины мини-атак в ходе которых происходит анализ всевозможных системных паролей, от секретов, до паролей DSL, VPN, FTP, IM, паролей браузеров, паролей почты, sticky notes, буфера обмена Windows, базы данных Windows Search и т.д. Чтобы гарантировать сохранность системных данных, программа не использует функцию автоматического восстановления баз Windows Search, находящихся в незакрытом состоянии и автоматически пропускает такие базы (во время поиска паролей). Чтобы проверить, является ли база данных Windows Search правильно закрытой или нет, попробуйте открыть ее из утилиты ESE Explorer. Если программа предложит восстановить базу данных, то она не была закрыта должным образом. Например, не был завершен выход из операционной системы.
2. Анализ простых, коротких паролей, клавиатурных комбинаций и т.д.
3. Поиск паролей при помощи алгоритмов глубокого обучения. Несмотря на то, что эти алгоритмы значительно сокращены для удовлетворения ограничений процессора, они работают намного лучше по сравнению с атакой по таблицам Passcape, которая была ими заменена.
4. Сканирование, анализ и обработка всех последних открываемых файлов целевой системы.
5. Простая атака по словарю. Проверяются все пароли из встроенного словаря для Light и Standard редакций или из нескольких словарей (Арабский, Китайский, Английский, Французский, Немецкий, Португальский, Русский, Испанский) для Advanced Edition. Если установлена опция глубокого поиска, то при проверке используются простейшие мутации слов.

6. Простая атака методом перебора.
7. Интеллектуальная атака. Наше небольшое ноу-хау, разрабатывающееся специалистами в течении нескольких лет. Данная атака анализирует сетевую активность пользователя на компьютере. Этим занимаются более трех десятков мини-модулей. На основе анализа создаются предпочтения пользователя и производится создание семантического словаря атаки, который затем используется при подборе и угадывании паролей.
8. Поиск паролей в удаленных файлах, временных каталогах и т.д.
9. Примитивная Идентификационная атака на составные Латинские пароли.
10. Поиск слов и паролей в больших файлах: RAM дисках, hiberfil.sys, pagefile.sys и т.д. Если эта опция установлена, программа автоматически будет пропускать файлы, обработка которых бесполезна с точки зрения поиска паролей пользователя: видео и аудио файлы, огромные файловые архивы и т.д.
11. Поиск паролей путем индексирования и анализа физических секторов выбранного диска. Этот пункт работает и для LM, и для NTLM хэшей, производится поиска как ASCII, так и UNICODE паролей. Если опция 'Password mutation level' выставлена в 'Deep search', то программа дополнительно попытается выполнить мутацию всех найденных слов. Используйте эту настройку аккуратно, т.к. проход по всем секторам с дополнительной мутацией слов может занять очень много времени. Этот алгоритм может быть чрезвычайно эффективен, т.к. позволяет вытаскивать пароли даже если соответствующий файл был давно удален с диска. С другой стороны, алгоритм индексации секторов неэффективен для поиска паролей в сложных файлах (например, документах Microsoft Office), а также если на целевом диске установлено шифрование. Например, при помощи Bitlocker или TrueCrypt.

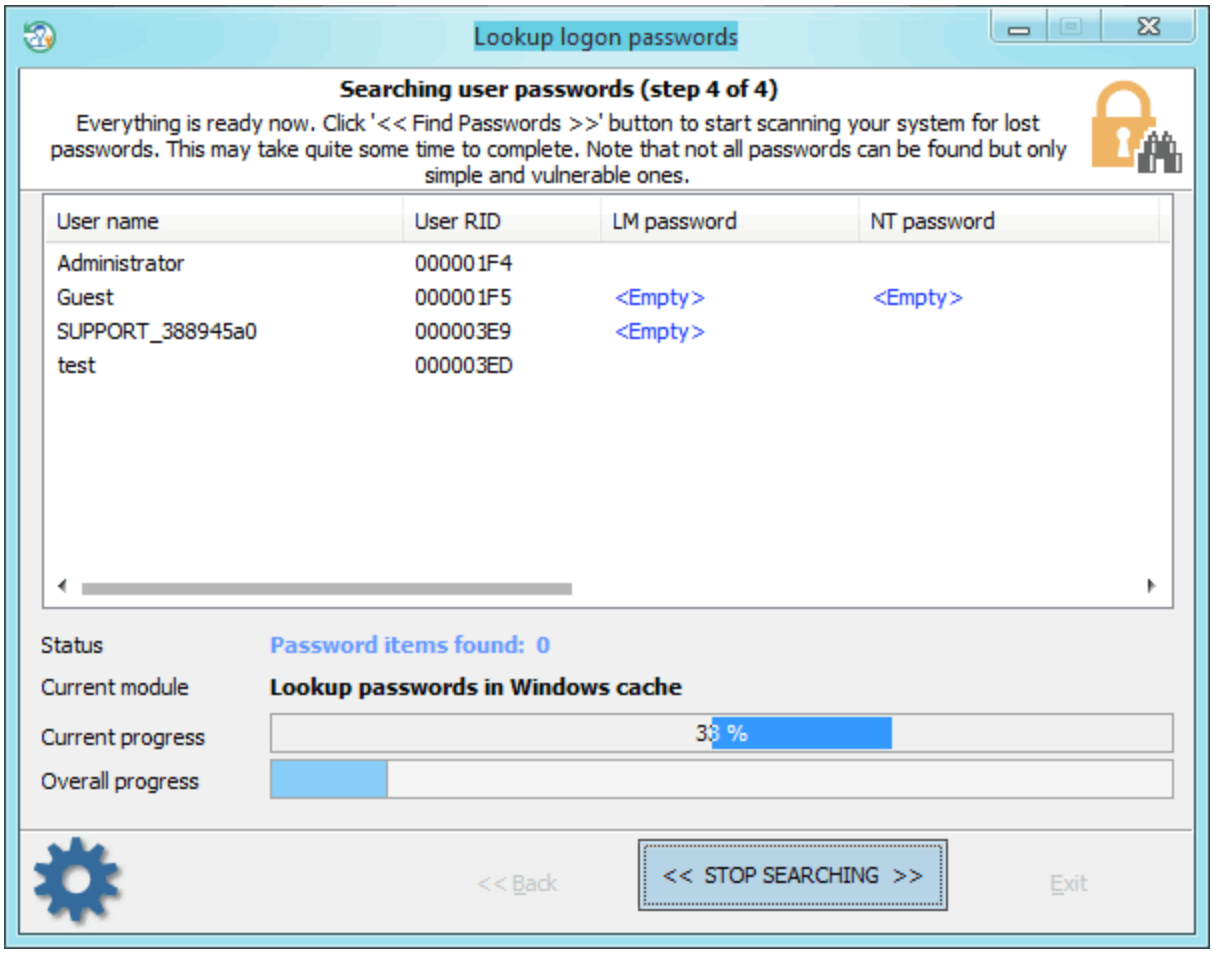
Чтобы запустить свое собственное восстановление, установите галочку напротив 'Настраиваемые атаки' и выберите тип атаки. На одном из следующих шагов вам будет предложено настроить опции выбранной атаки.

Выбор источника данных



При поиске паролей особое внимание следует уделить правильному заполнению всех необходимых в процессе анализа файлов и каталогов. Без них подбор паролей будет неэффективен. Программа автоматически производит поиск файлов, но иногда, например, если на компьютере было установлено несколько операционных систем, требуется 'ручное управление'. Имейте также в виду, что при наличии 2-х или более жестких дисков, порядок букв для этих дисков (после загрузки с диска Reset Windows Password) может быть совершенно иной, нежели чем на оригинальной системе.

Поиск и расшифровка паролей



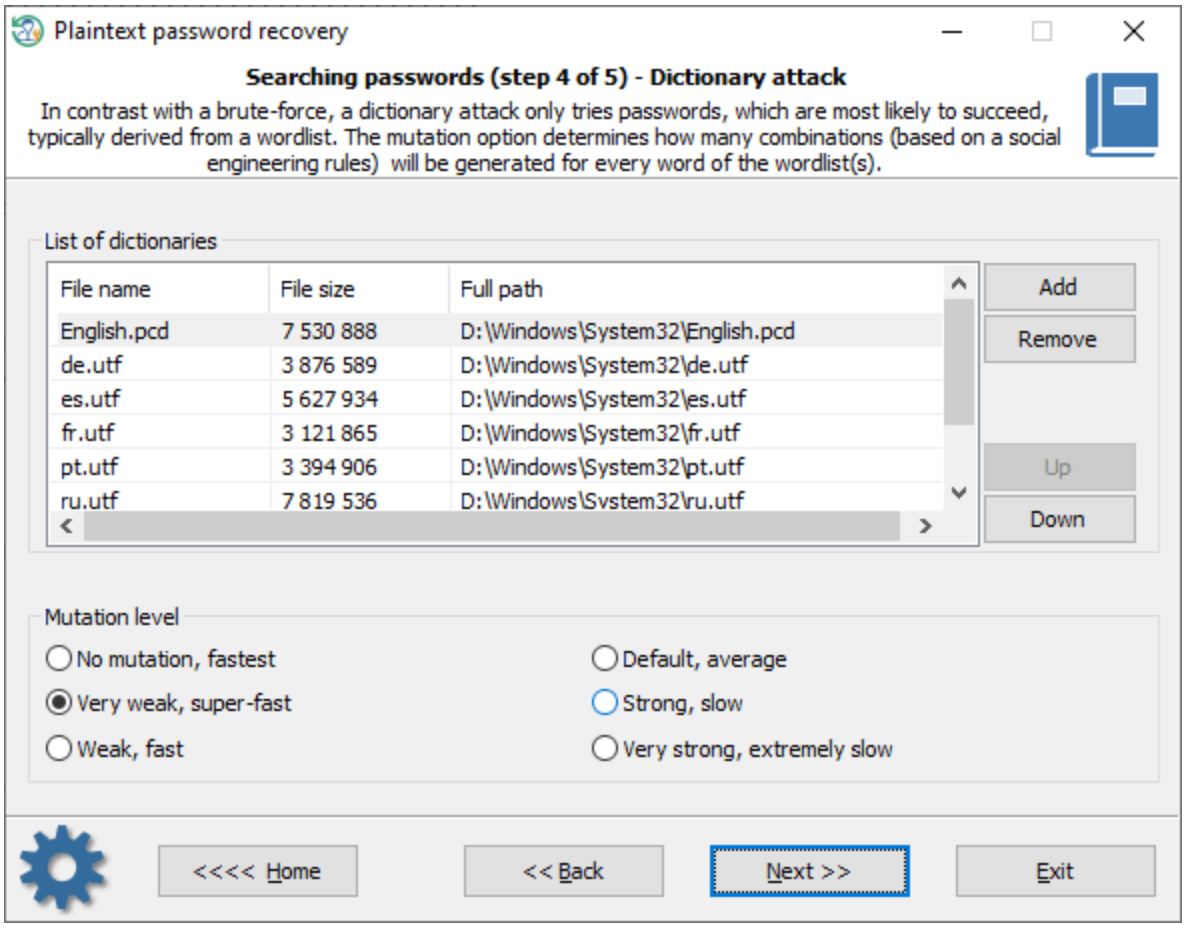
Поиск/анализ паролей может занять некоторое время, которое зависит от настроек атаки и особенностей вашей системы. Обычно весь поиск занимает менее получаса без использования поиска по таблицам Passcape. Подбор паролей по таблицам может занять намного больше времени. Это зависит от мощности вашего процессора и количества восстанавливаемых хэшей. Так, на 2-х ядерном ПК поиск пароля для одного хэша обычно занимает до 3-4 минут.

3.5.1.1 Настраиваемые атаки

Если выбрана опция 'Настраиваемая атака', то программа предлагает 3 дополнительных инструмента для угадывания паролей:

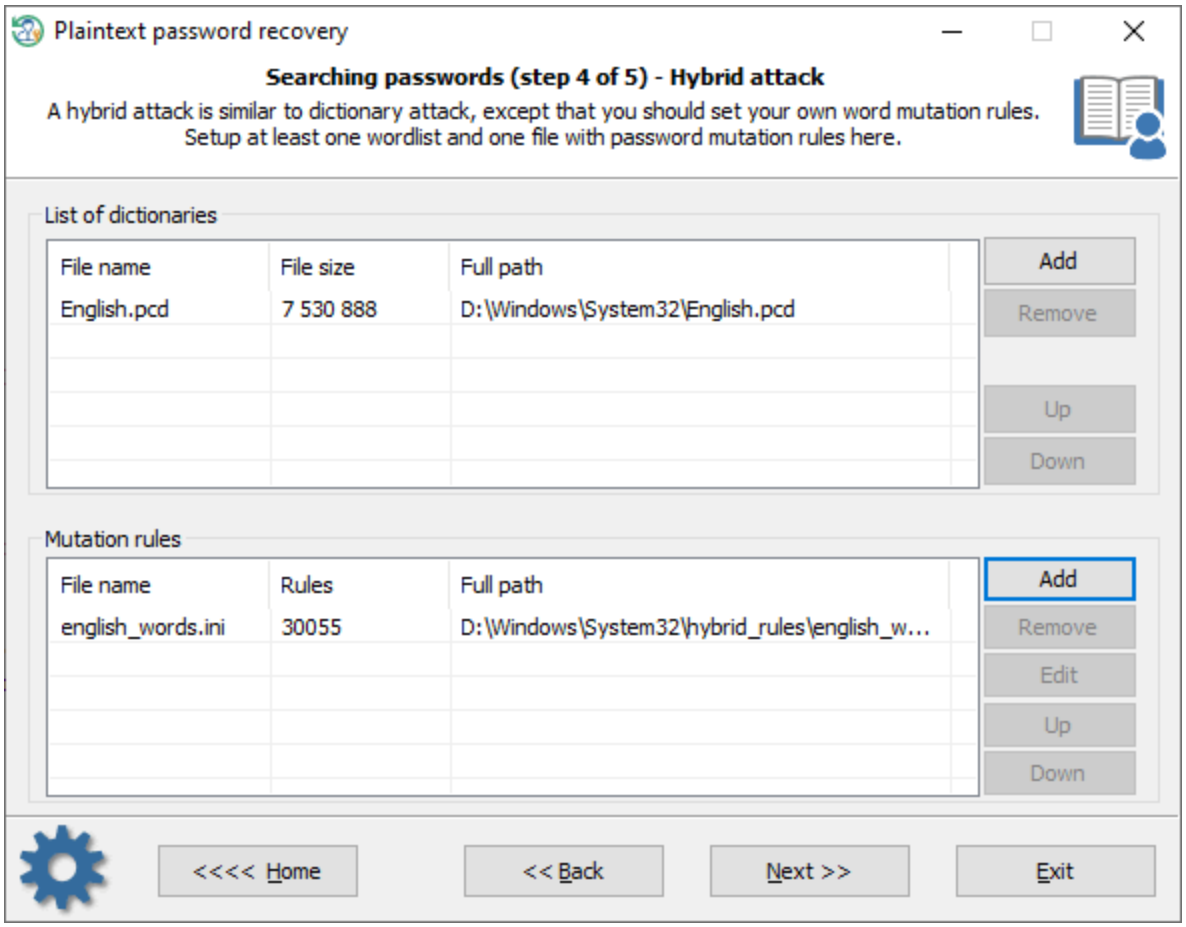
- Словарная атака
- Гибридная атака
- Атака по маске

Словарная атака



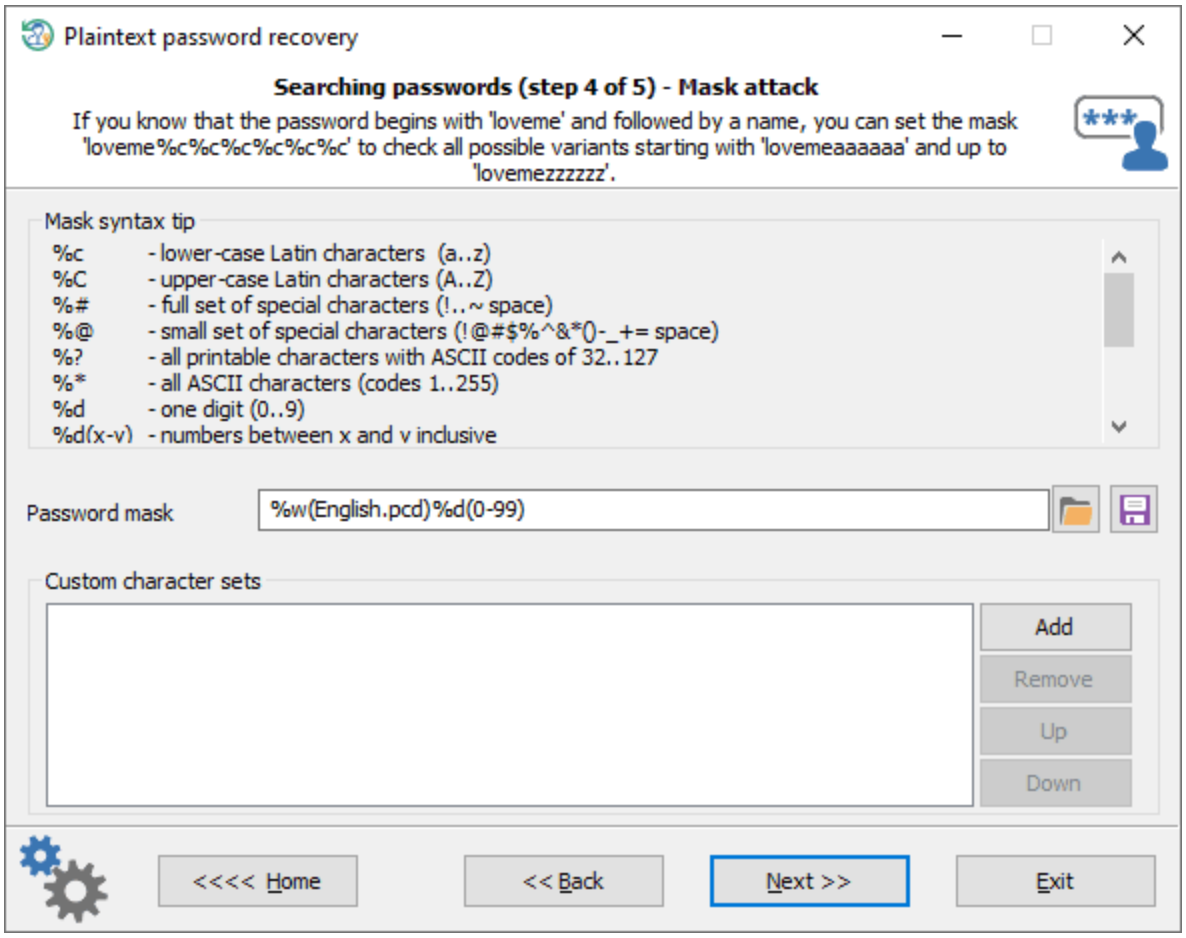
Атака по словарю использует слова из заданного списка для подбора наиболее вероятных кандидатов в пароли. RWP поддерживает различные типы словарей: ASCII, UNICODE, UTF8, а также зашифрованные/сжатые словари в собственном формате PCD. Вы можете использовать как стандартные, поставляемые вместе с программой, так и свои собственные словари. Чтобы использовать свой словарь, скопируйте его на USB-носитель и подключите его к целевому компьютеру. Уровень мутации определяет, сколько комбинаций на основе правил социальной инженерии будет создано для каждого слова из исходного словаря.

Гибридная атака



Гибридная атака похожа на словарную, за исключением того, что можно устанавливать свои собственные правила мутации слов. Программа поставляется с огромным набором файлов с правилами. Просто используйте тот, который лучше всего подходит для вашей задачи. Кроме того, гибридная атака позволяет дополнительно создавать, редактировать или изменять правила мутации в соответствии с вашими потребностями.

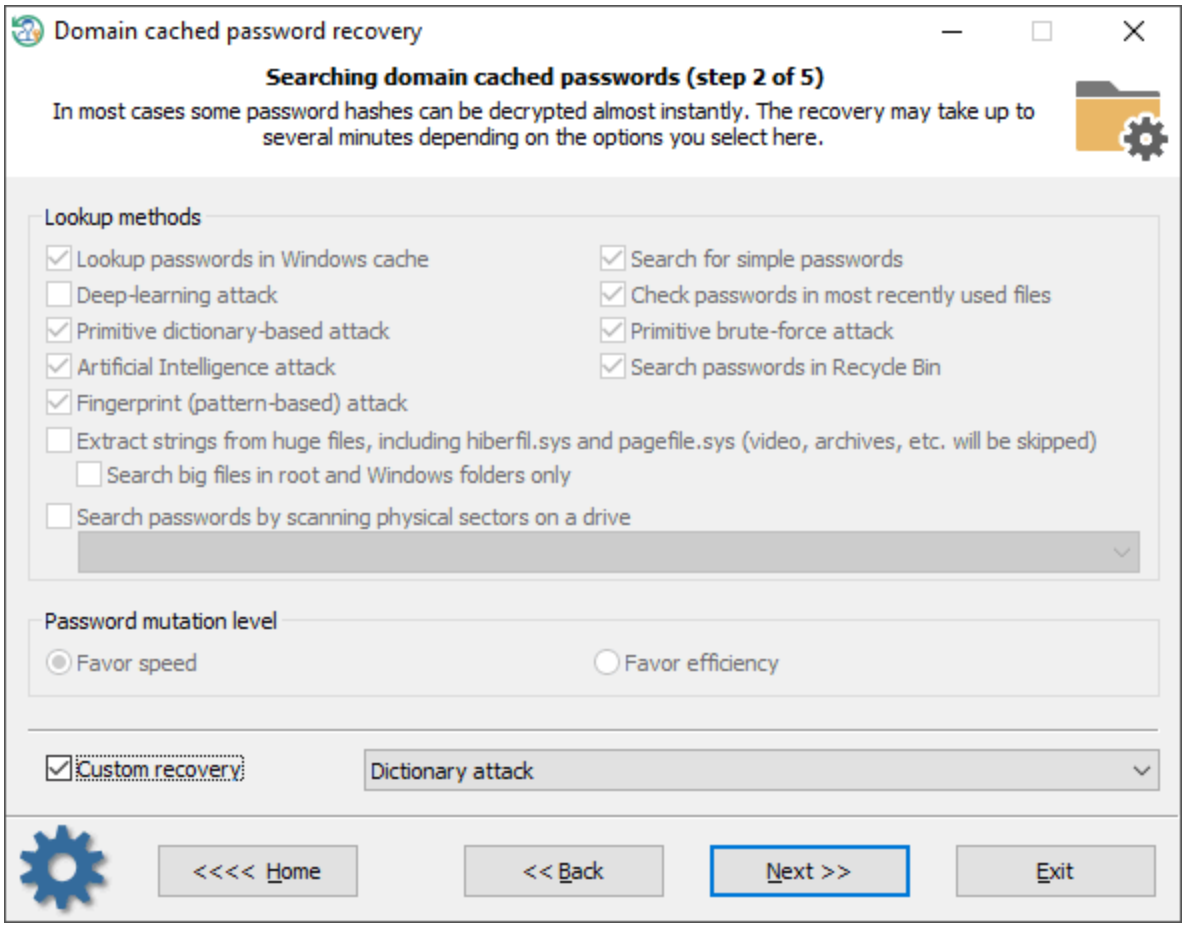
Атака по маске



Атака по маске является незаменимым инструментом, когда вы знаете часть пароля или имеете какую-либо информацию о нем. Например, если известно, что пароль состоит из 12 символов и начинается с 'loveme', то достаточно перебрать последние 6 символов пароля чтобы угадать весь пароль. Вот для чего нужна атака по маске. В нашем примере можно установить такую маску: loveme%c%c%c%c%c%c
Для получения более подробной информации о том, как работает маска, обратитесь к нашей онлайн-документации.

3.5.2 Поиск кэшированных паролей домена

Установка опций поиска и методов восстановления



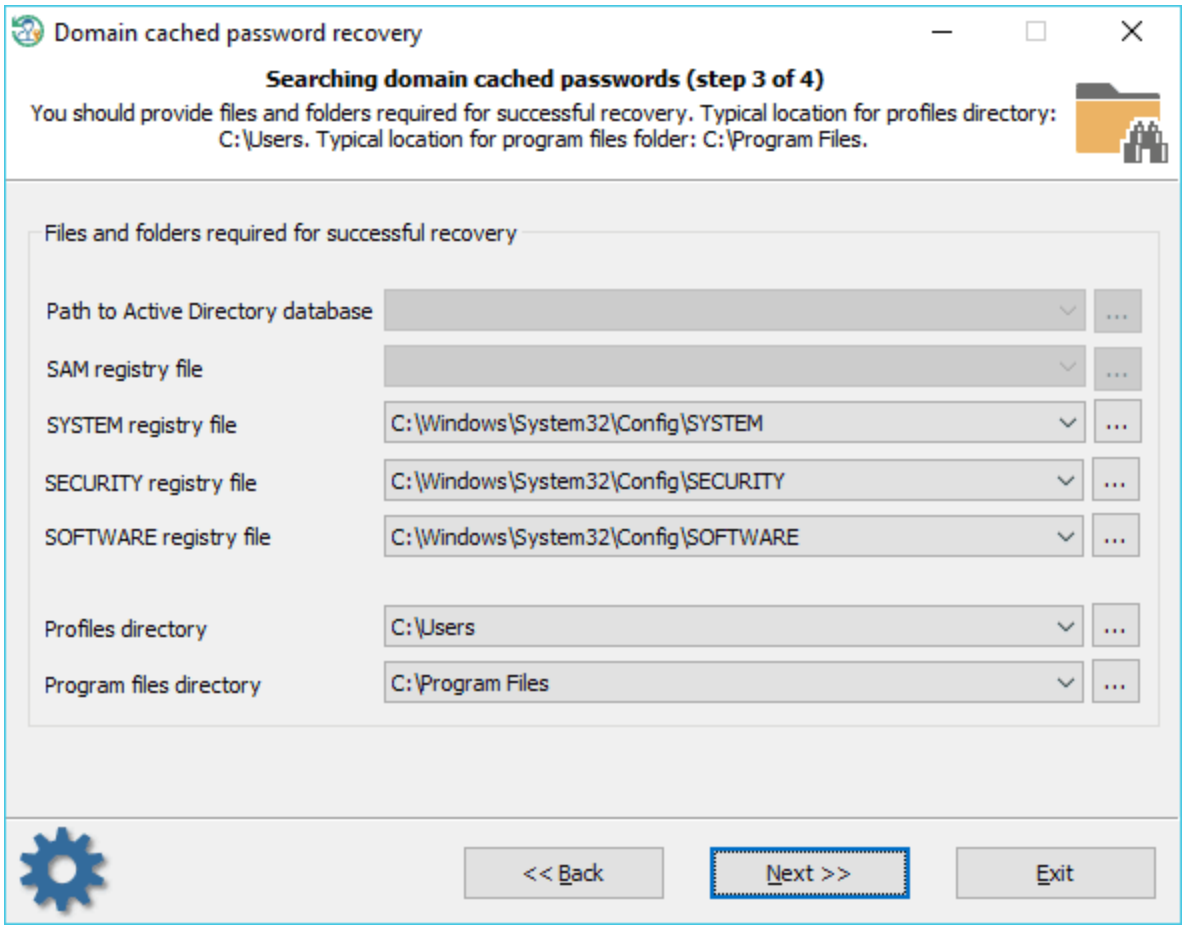
Поиск кэшированных паролей домена состоит из нескольких модулей каждый из которых можно включать/выключать отдельно:

1. Модуль поиска информации в системном кэше Windows. Данный модуль в свою очередь состоит из более чем полутора десятка мини-атак в ходе которых происходит анализ всевозможных системных паролей, от секретов LSA, до паролей DSL, VPN, FTP, WiFi, сетевых паролей, паролей браузеров, почты, базы данных Windows Search и т.д. В дальнейшем эта информация используется программой для создания и проверки более сложных паролей.
2. Модуль проверки коротких, простых, цифровых паролей, клавиатурных комбинаций и т.д. Всего более 20 мини-атак.
3. Сканирование, анализ и обработка последних открываемых файлов целевой системы. Создание списка слов и их проверка в качестве паролей.
4. Простая атака по словарю в ходе которой проверяются пароли из встроенного словаря для Light и Standard редакций или из нескольких словарей (Арабский, Китайский, Английский, Французский, Немецкий, Португальский, Русский, Испанский) для Advanced редакции.
5. Простая атака методом перебора. Состоит из нескольких мини-атак на кроткие пароли.
6. Интеллектуальная атака, анализирующая сетевую активность пользователя на компьютере. На основе анализа создаются предпочтения пользователя и производится создание семантического словаря атаки, который затем используется при подборе паролей.
7. Поиск паролей в удаленных файлах, временных каталогах и др.
8. Идентификационная атака на составные пароли. Может занять очень много времени.
9. Поиск слов и паролей в больших файлах: RAM дисках, hiberfil.sys, pagefile.sys и т.д. Программа автоматически пропускает файлы, обработка которых бесполезна с точки зрения поиска паролей: видео и аудио файлы, огромные файловые архивы и т.д.

10. Поиск паролей путем индексирования и анализа физических секторов выбранного диска. Если опция 'Password mutation level' выставлена в 'Deep search', то программа дополнительно попытается выполнить мутацию всех найденных слов. Используйте эту настройку аккуратно, т.к. проход по всем секторам с дополнительной мутацией слов может занять чрезвычайно много времени. Алгоритм индексации секторов бесполезен если на целевом диске установлено шифрование.

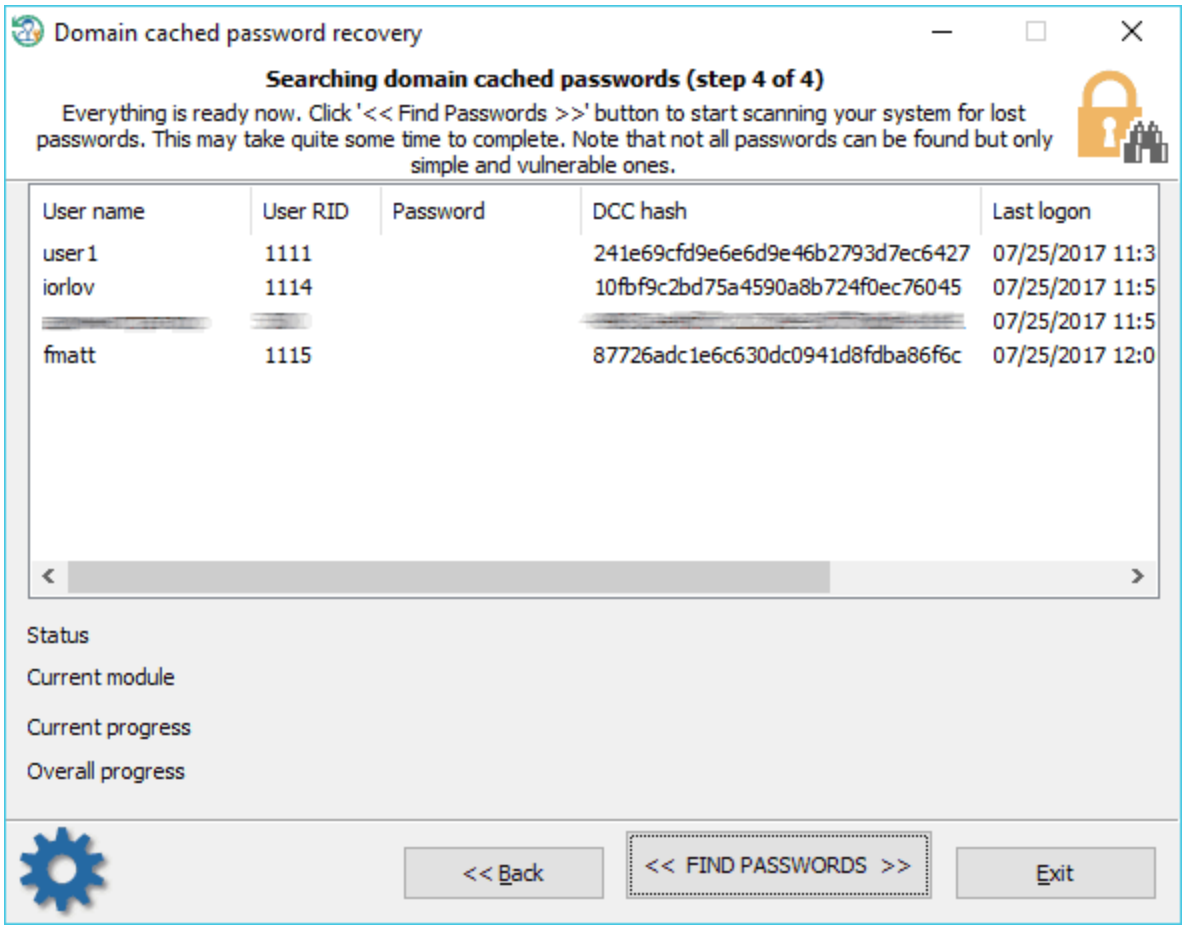
Для запуска своего собственного, настраиваемого восстановления, установите галочку напротив 'Настраиваемые атаки' и выберите тип атаки. На одном из следующих шагов вам будет предложено настроить опции выбранной атаки.

Выбор источника данных



При поиске паролей особое внимание следует уделить правильному заполнению всех необходимых в процессе анализа файлов и каталогов. Без них подбор паролей может быть неэффективен. Программа сама производит поиск необходимых файлов, но иногда требуется ручной выбор. Например, если на компьютере было установлено несколько операционных систем. Учтите, при наличии двух или более жестких дисков, порядок букв для этих дисков может быть совершенно иной, нежели чем на оригинальной системе.

Поиск кэшированных паролей домена



Кэшированные пароли домена бывают двух типов. Первый тип использовался в операционных системах Windows 2000, Windows XP и Windows 2003. Пароли этого типа отличаются слабым шифрованием. При их подборе скорость угадывания может исчисляться миллионами или даже миллиардами паролей в секунду. Второй тип (используется начиная с Windows Vista) имеет довольно стойкий ко взлому алгоритм шифрования. Скорость перебора паролей не превышает сотни/ тысячи паролей в секунду. Насколько это много или мало, просто представьте, что для взлома 8 символьного пароля, состоящего из 8 заглавных и строчных букв, при такой скорости потребуется более 1000 лет.

Важно учесть некоторые нюансы:

- Поиске кэшированных паролей второго типа происходит очень медленно. Полная отработка некоторых модулей (например, Идентификационной атаки) может занять часы или даже дни.
- Для увеличения скорости поиска, оставьте только ту учетную запись, пароль к которой требуется найти. Для этого щелкните правой кнопкой мыши на интересуемой записи и выберите пункт '*Исключить из поиска все записи, кроме выбранной*'. В противном случае, скорость перебора паролей уменьшится кратно количеству кэшированных записей.

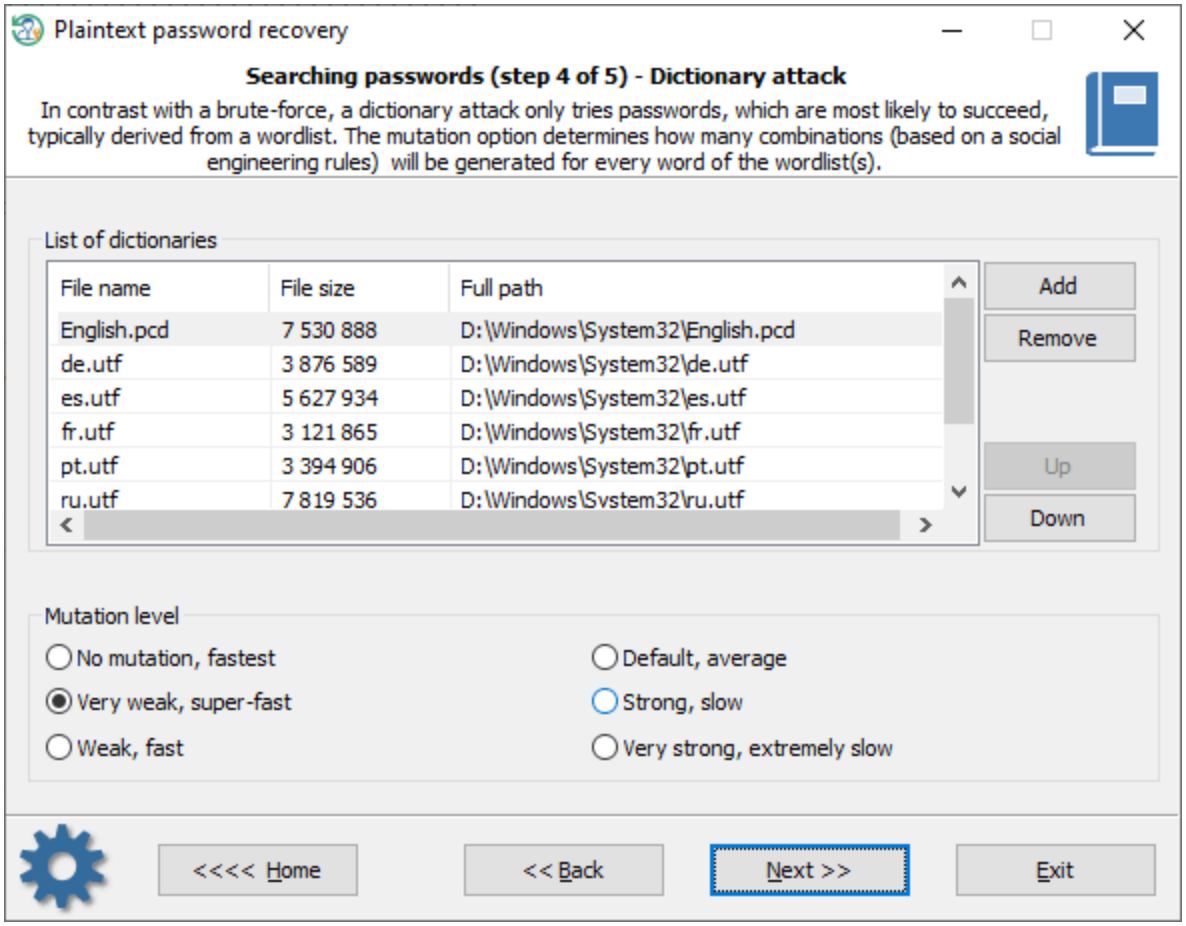
3.5.2.1 Настраиваемые атаки

Если выбрана опция 'Настраиваемая атака', то программа предлагает 3 дополнительных инструмента для угадывания паролей:

- Словарная атака

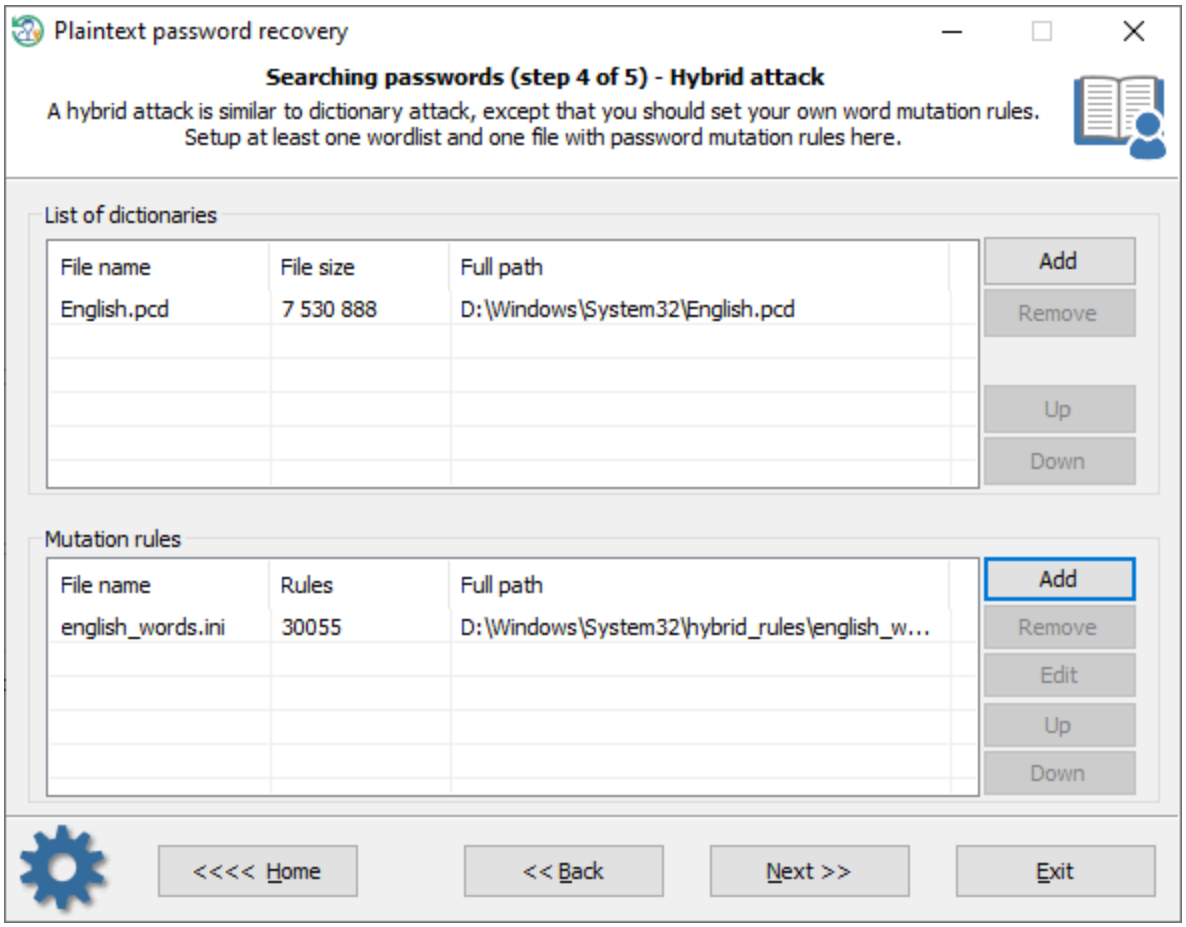
- Гибридная атака
- Атака по маске

Словарная атака



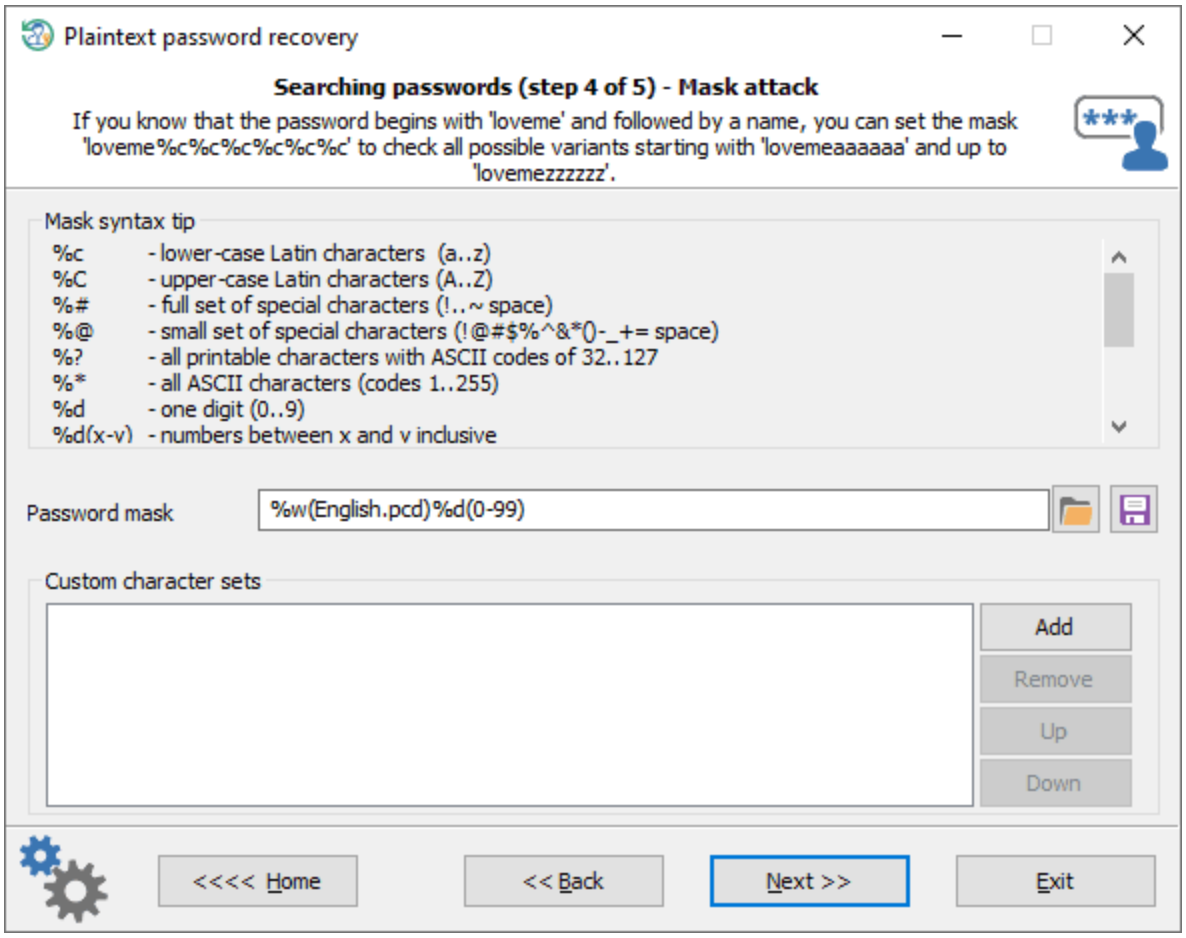
Атака по словарю использует слова из заданного списка для подбора наиболее вероятных кандидатов в пароли. RWP поддерживает различные типы словарей: ASCII, UNICODE, UTF8, а также зашифрованные/сжатые словари в собственном формате PCD. Вы можете использовать как стандартные, поставляемые вместе с программой, так и свои собственные словари. Чтобы использовать свой словарь, скопируйте его на USB-носитель и подключите его к целевому компьютеру. Уровень мутации определяет, сколько комбинаций на основе правил социальной инженерии будет создано для каждого слова из исходного словаря.

Гибридная атака



Гибридная атака похожа на словарную, за исключением того, что можно устанавливать свои собственные правила мутации слов. Программа поставляется с огромным набором файлов с правилами. Просто используйте тот, который лучше всего подходит для вашей задачи. Кроме того, гибридная атака позволяет дополнительно создавать, редактировать или изменять правила мутации в соответствии с вашими потребностями.

Атака по маске

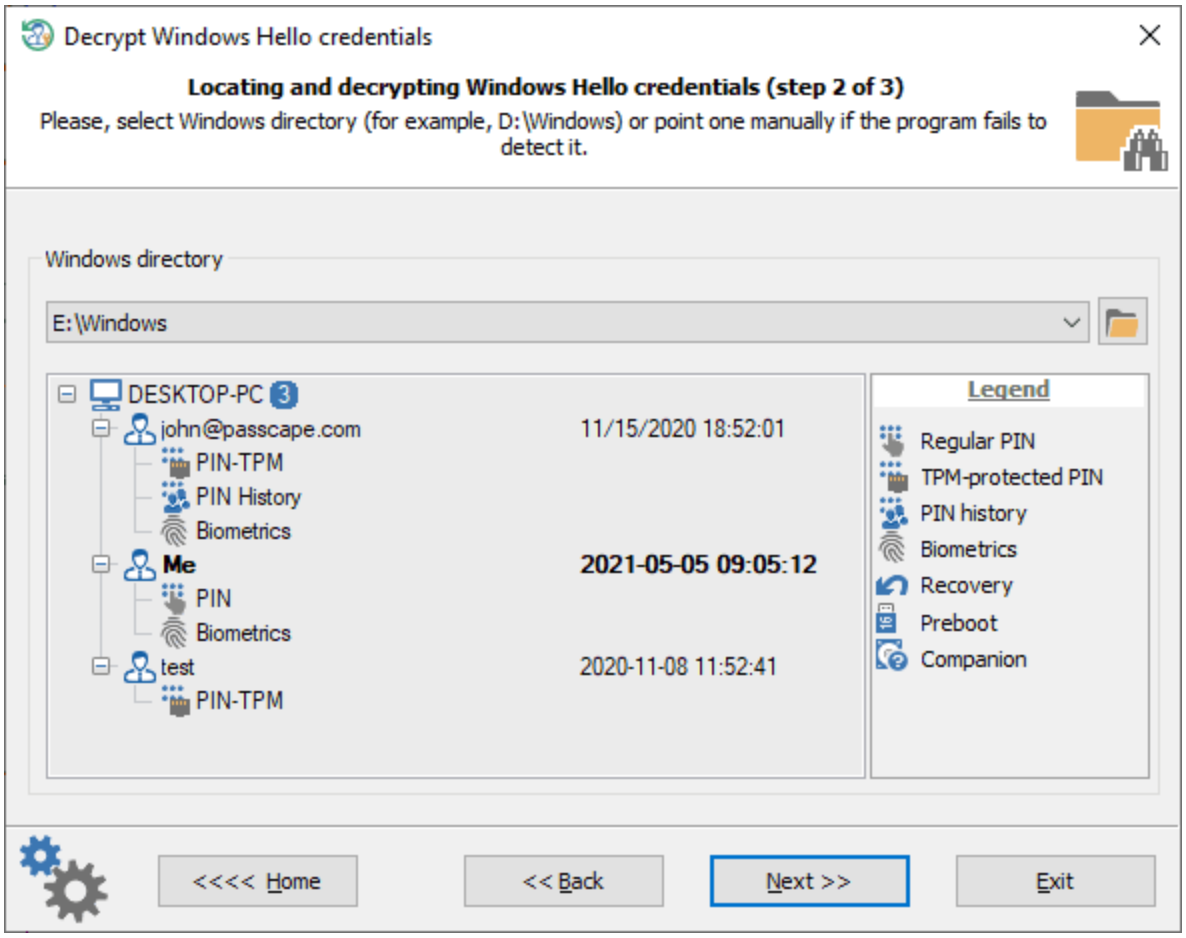


Атака по маске является незаменимым инструментом, когда вы знаете часть пароля или имеете какую-либо информацию о нем. Например, если известно, что пароль состоит из 12 символов и начинается с 'loveme', то достаточно перебрать последние 6 символов пароля чтобы угадать весь пароль. Вот для чего нужна атака в маске. В нашем примере можно установить такую маску: loveme%c%c%c%c%c%c
Для получения более подробной информации о том, как работает маска, обратитесь к нашей онлайн-документации.

3.5.3 Расшифровка паролей Windows Hello

Windows Hello - система биометрической, беспарольной аутентификации пользователей. Windows Hello хранит разные типы персональной информации: цифровые идентификаторы, PIN-коды, зашифрованные текстовые пароли пользователей.

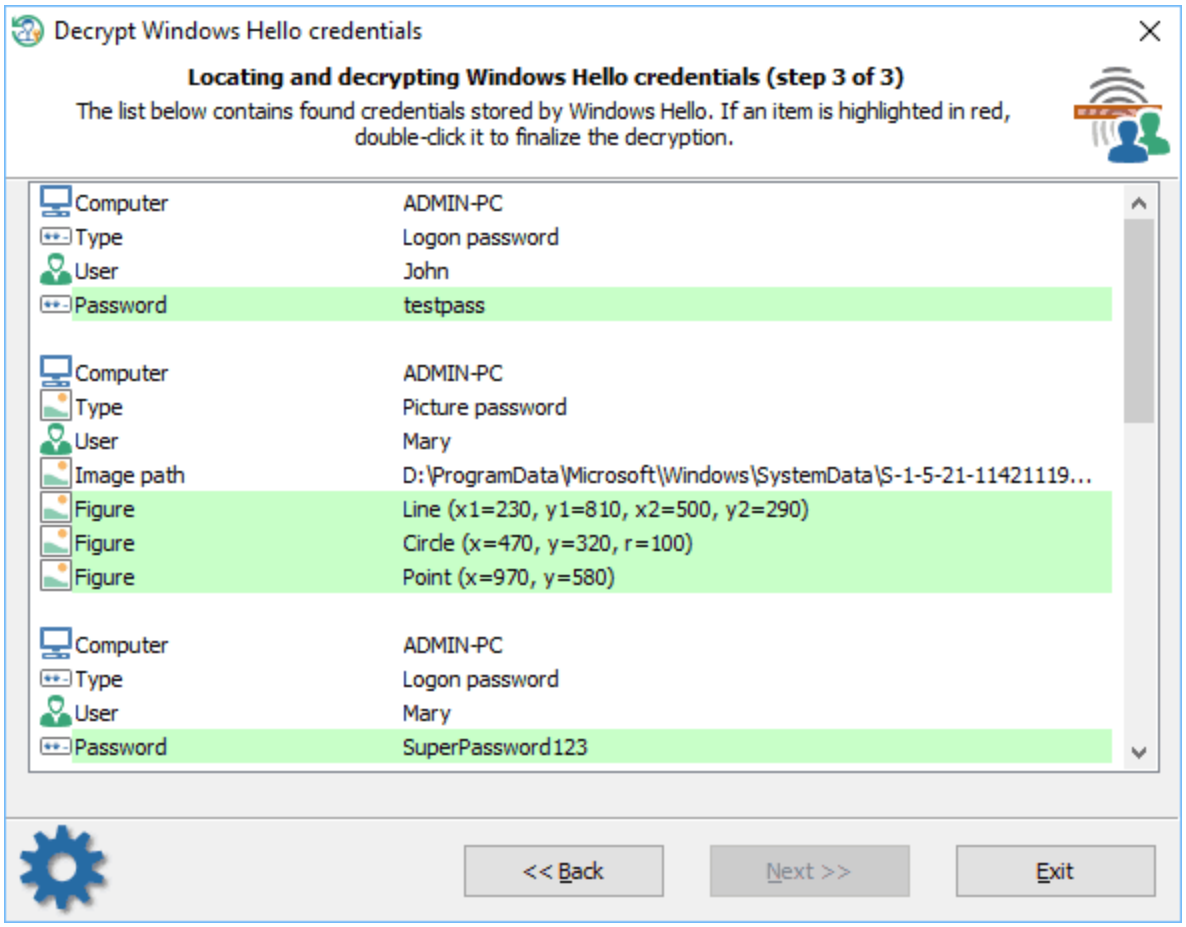
Выбор каталога Windows



Reset Windows Password позволяет восстанавливать все типы персональных данных, которые хранятся в Windows Hello. Для этого сначала необходимо задать каталог Windows с целевой операционной системой Windows 10. При выборе каталога программа производит анализ установленной Операционной Системы и отображает список найденных учетных записей Windows Hello, а также используемые ими методы аутентификации. Последний пользователь, выполнивший вход в систему, выделен жирным шрифтом. Основные методы аутентификации Windows Hello:

- **PIN** - доступен вход по ПИН-коду
- **PIN-TPM** - установлен ПИН-код с защитой TPM
- **PIN History** - присутствует история введенных ранее ПИН-кодов
- **Biometrics** - доступен вход по отпечаткам пальцев

Расшифровка паролей



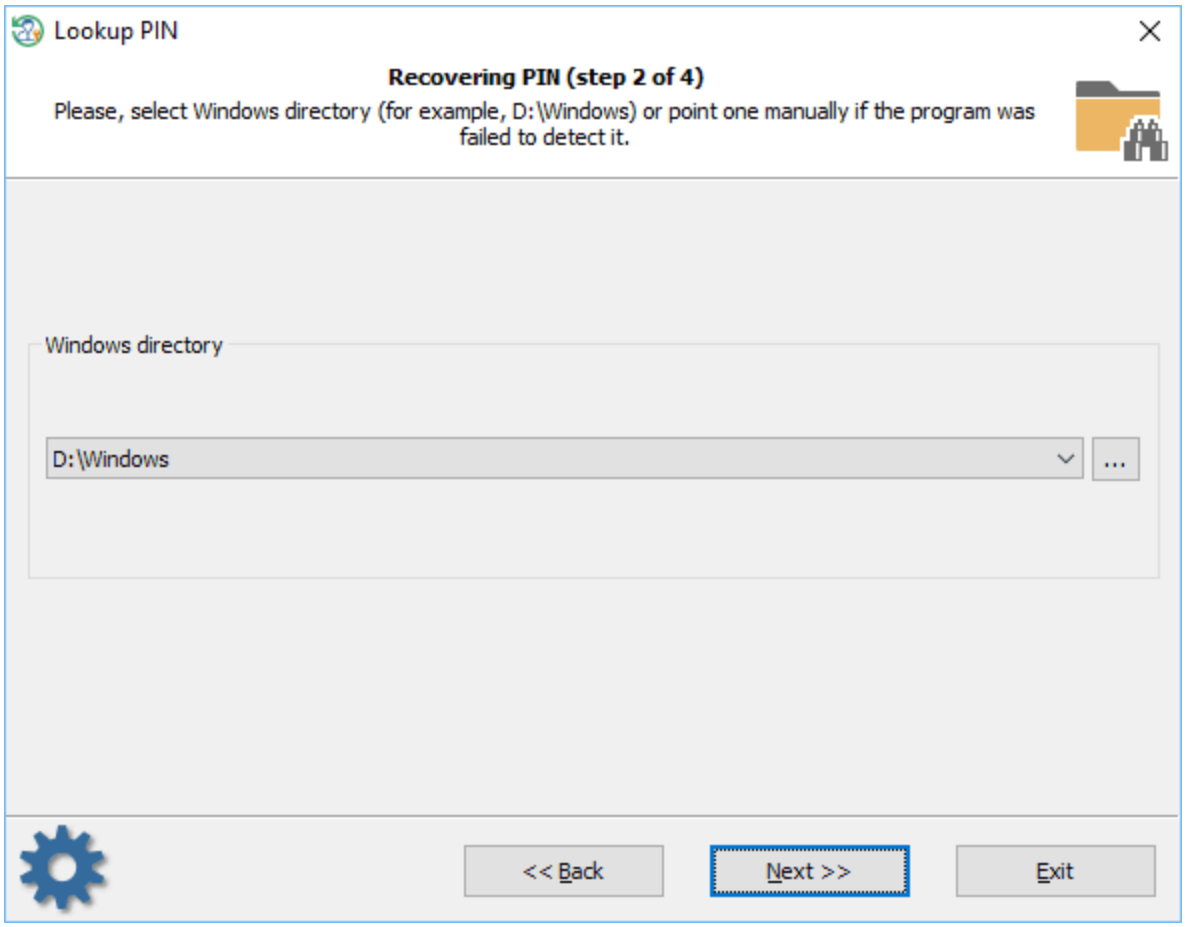
Программа выведет список всех найденных в Windows Hello паролей на экран. Если учетная запись была настроена на вход в систему при помощи биометрической аутентификации, например, отпечатка пальцев или сканирования лица, то Reset Windows Password автоматически расшифрует текстовый пароль.

Некоторые записи в таблице могут быть выделены красным цветом. Это означает, что для финальной расшифровки пароля необходимо дополнительное знание PIN-кода. Дважды щелкните на такой записи и введите PIN-код, соответствующий пользователю.

3.5.4 Восстановление PIN

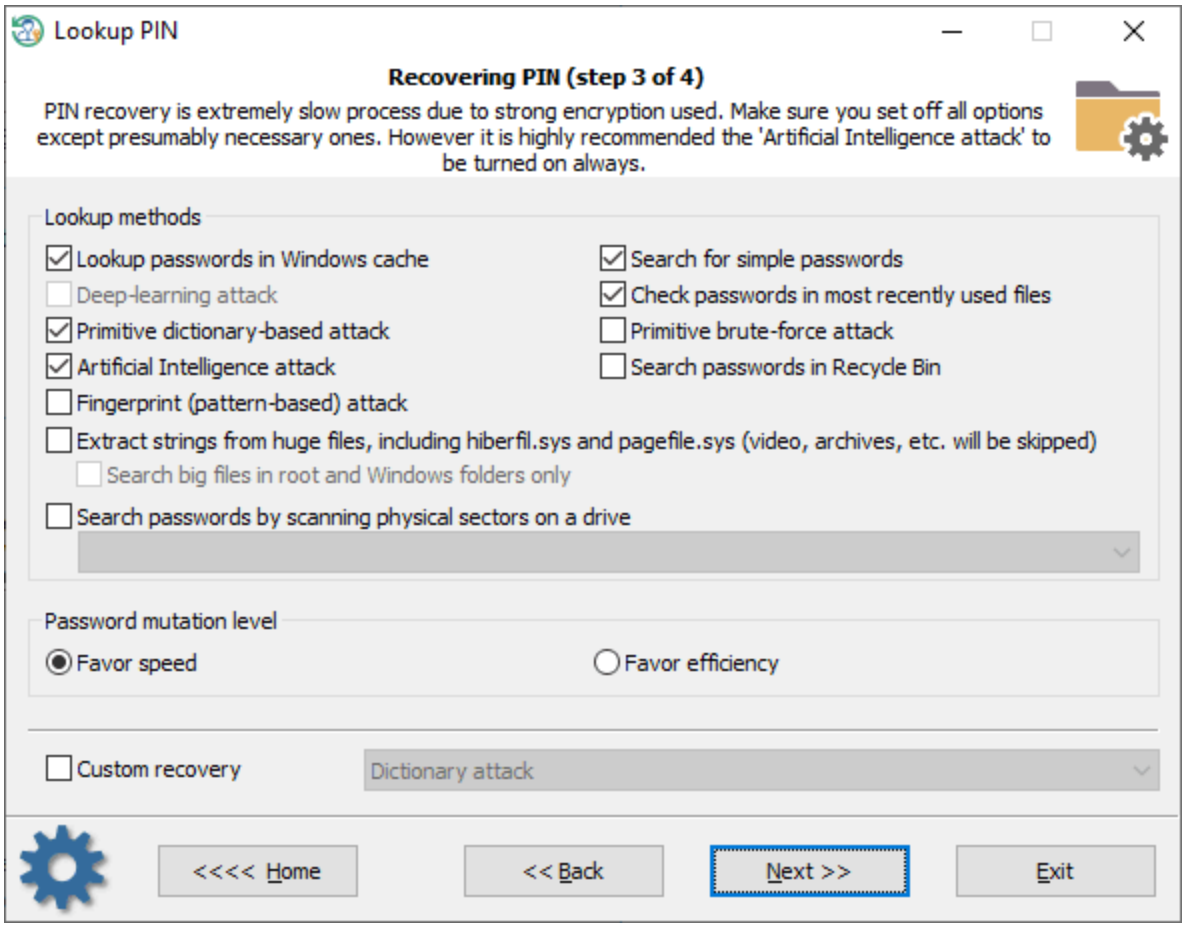
При настройке Windows Hello прежде всего требуется создание PIN-кода. PIN-код можно использовать как запасной вариант, когда биометрический датчик недоступен или не работает должным образом. В отличие от Windows 8, для защиты PIN-кода в операционной системе Windows 10 применяется очень сильное шифрование. Поэтому, особенно остро стоит вопрос восстановления забытого PIN.

Выбор каталога Windows



В первую очередь необходимо выбрать целевой каталог Windows или задать его самостоятельно.

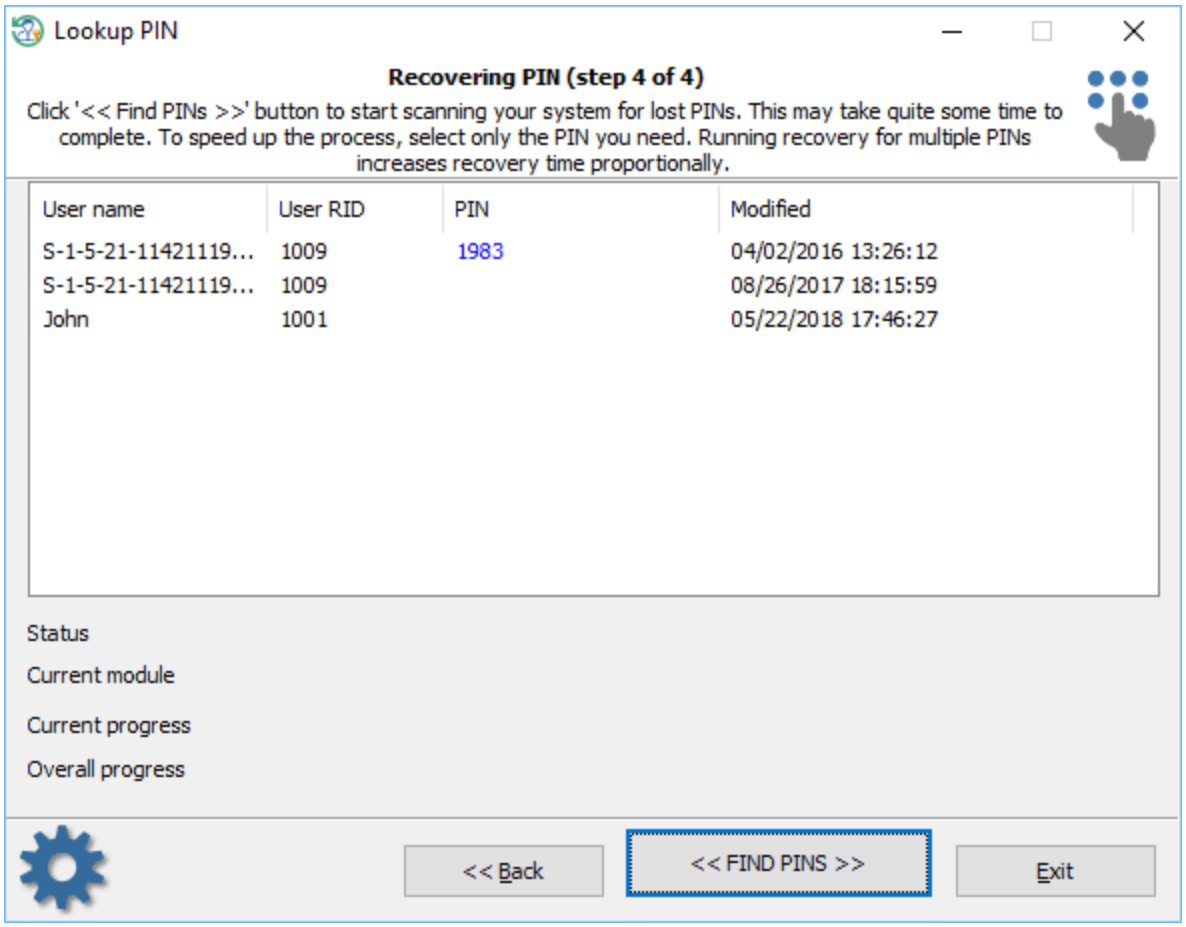
Установка опций поиска и методов восстановления



На следующем шаге мастер программы предложит доступные методы поиска PIN. Учтите, не смотря на то, что код программы оптимизирован, поиск PIN кода - процесс очень медленный. Поэтому рекомендуется отключить самые затратные методы поиска. Например, как показано на картинке выше.

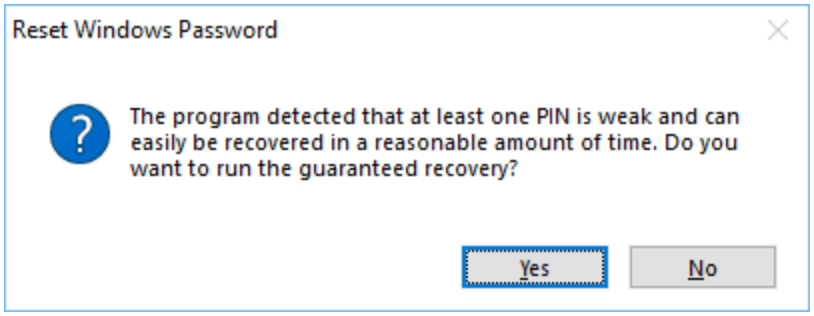
Чтобы запустить свое собственное восстановление, установите галочку напротив 'Настраиваемые атаки' и выберите тип атаки. На одном из следующих шагов вам будет предложено настроить опции выбранной атаки.

Поиск PIN-кодов



Скорость поиска обратно пропорциональна количеству искомых PIN. Т.е. чем больше PIN кодов ищется одновременно, тем меньше скорость поиска. Поэтому рекомендуется исключить из поиска все ненужные PIN, оставив только один необходимый. Сделать это можно просто: щелкните правой кнопкой по PIN-коду, который надо восстановить, и выберите пункт 'Исключить все записи, кроме выбранной'. Для запуска процесса поиска нажмите << ПОИСК PIN >>.

Имейте в виду, некоторые PIN-коды можно гарантированно восстановить за разумное время. Если программа обнаружит такой уязвимый код, то предложит запустить атаку с гарантированным восстановлением, как показано на скриншоте ниже.



В новых версиях программы встроен алгоритм так называемой "умной расшифровки". Каждый раз, когда пользователь нажимает кнопку << ПОИСК PIN >>, программа анализирует найденные ПИН-коды и

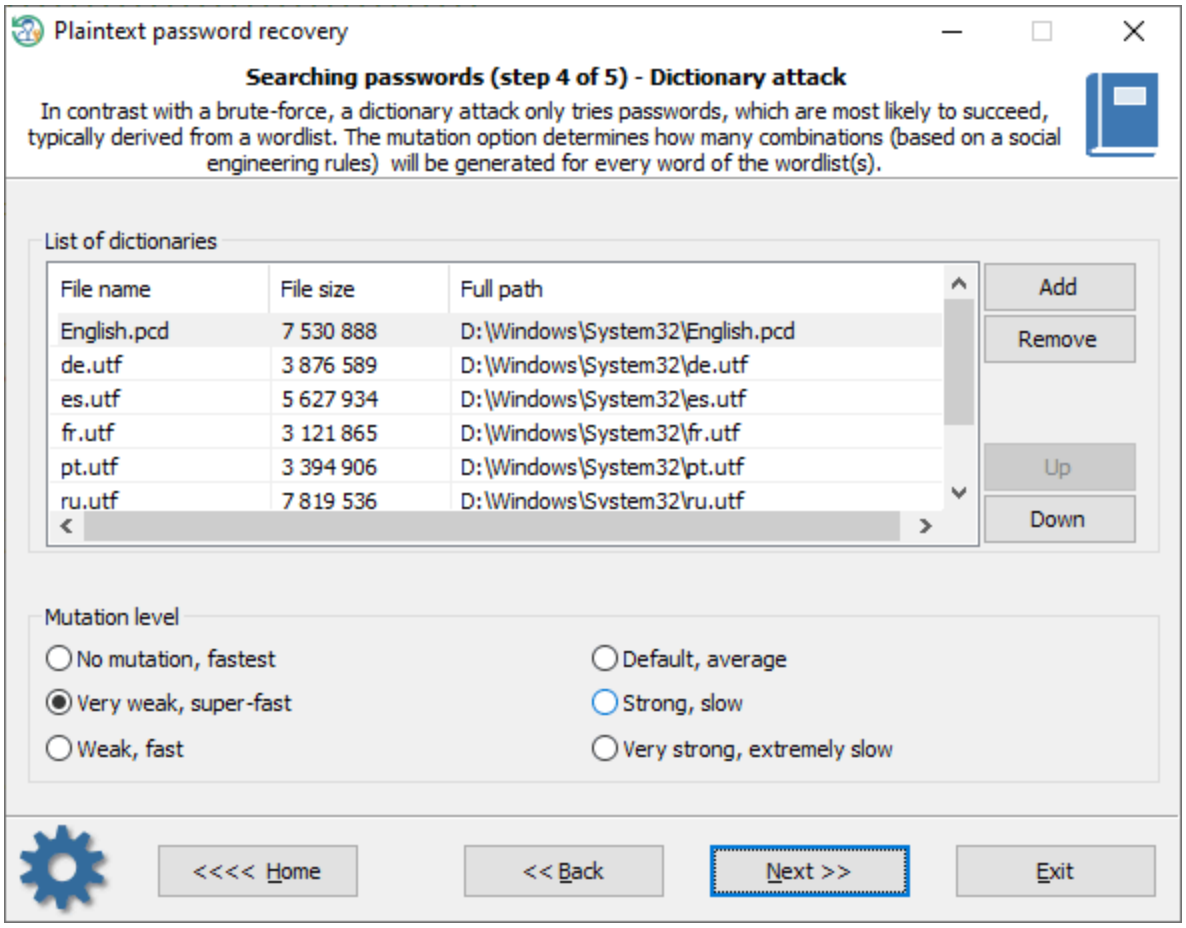
предлагает умное восстановление записей. Умное восстановление подразумевает либо гарантированную расшифровку за разумный промежуток времени, либо негарантированный поиск по шаблону (только тех записей которые могут потенциально содержать часто-употребляемые комбинации). Т.е. сначала производится гарантированный поиск ПИН-кодов, которые могут быть найдены за минимальное время, затем за более длинный промежуток времени и затем негарантированный поиск шаблонных ПИН.
Если программа не обнаружила ни тех, ни других типов ПИН, запускается атака, выбранная пользователем.

3.5.4.1 Настраиваемые атаки

Если выбрана опция 'Настраиваемая атака', то программа предлагает 3 дополнительных инструмента для угадывания паролей:

- Словарная атака
- Гибридная атака
- Атака по маске

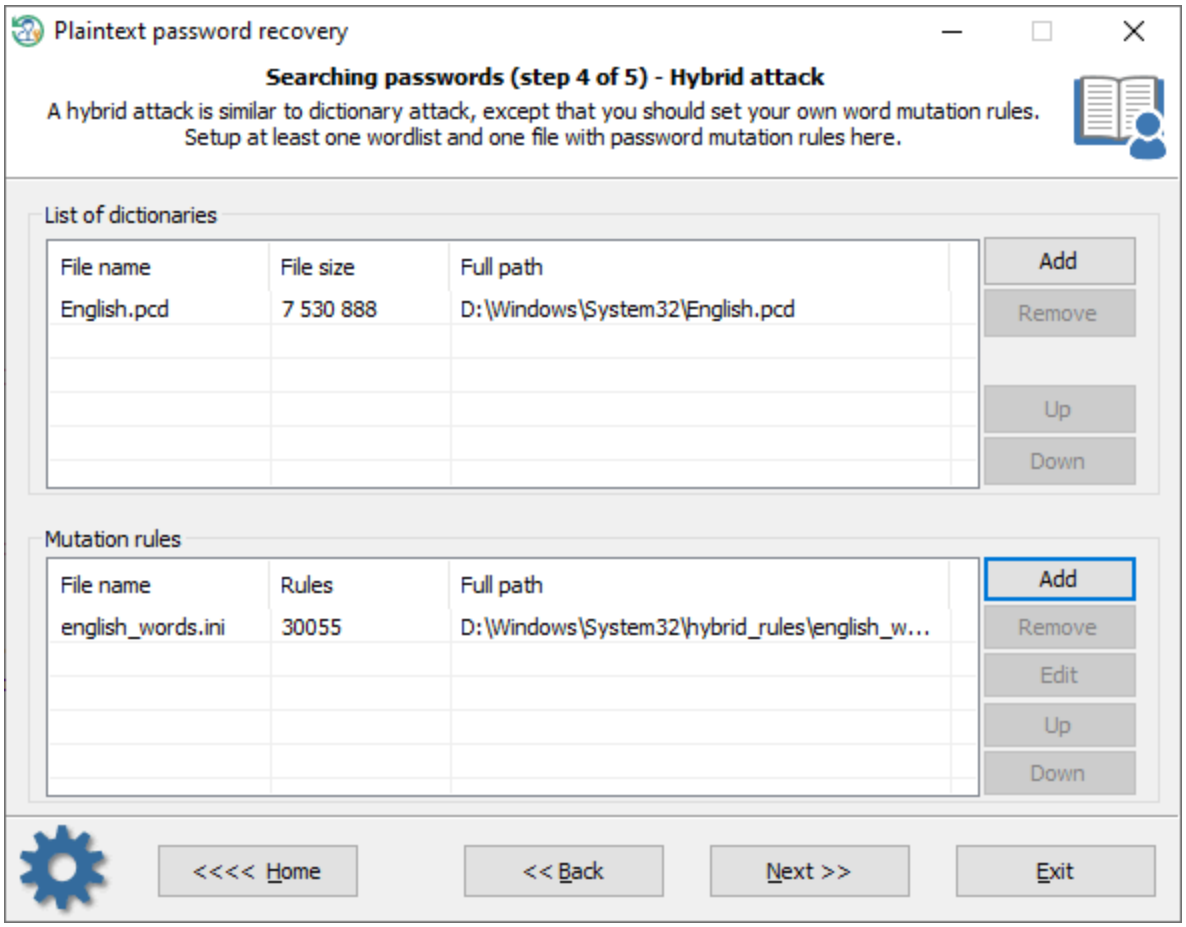
Словарная атака



Атака по словарю использует слова из заданного списка для подбора наиболее вероятных кандидатов в пароли. RWP поддерживает различные типы словарей: ASCII, UNICODE, UTF8, а также зашифрованные/сжатые словари в собственном формате PCD. Вы можете использовать как стандартные,

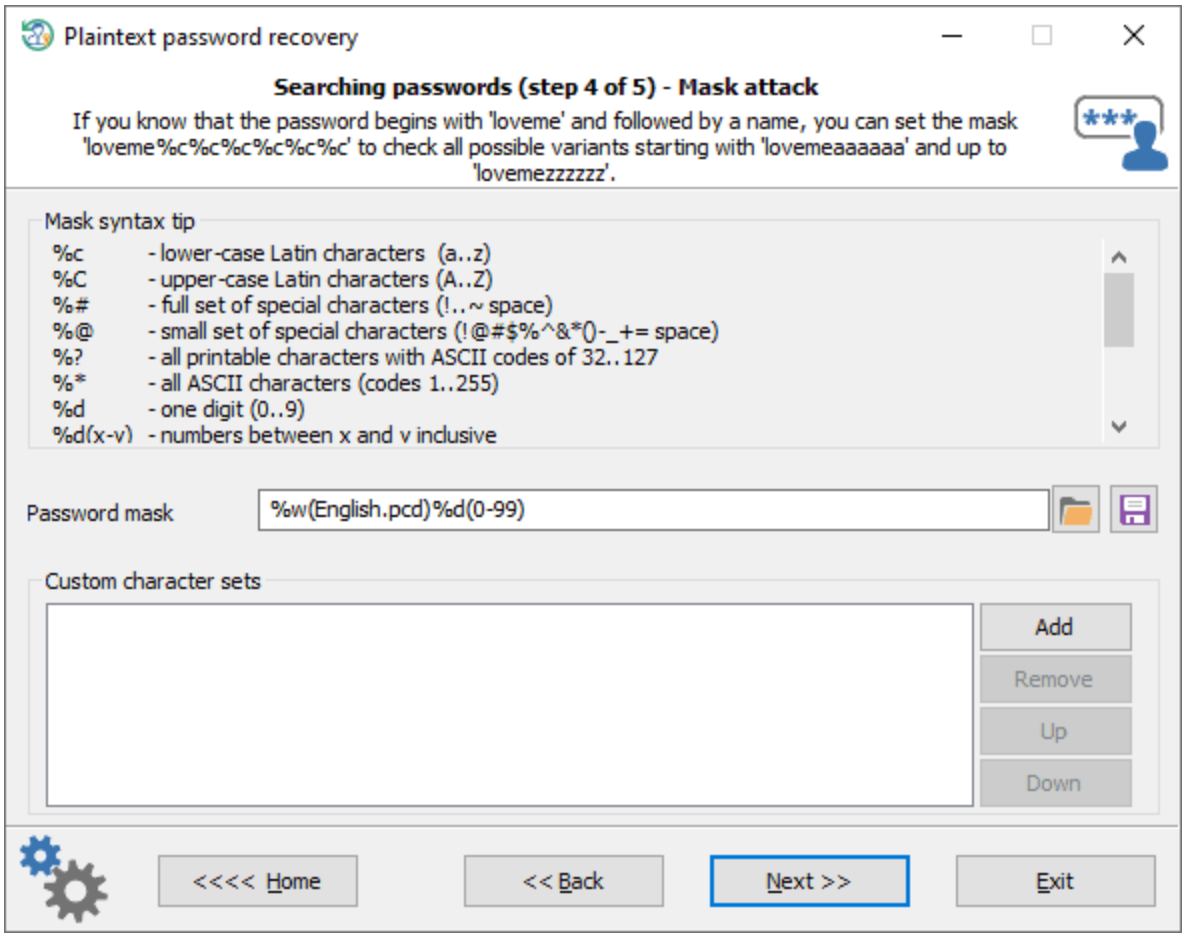
поставляемые вместе с программой, так и свои собственные словари. Чтобы использовать свой словарь, скопируйте его на USB-носитель и подключите его к целевому компьютеру. Уровень мутации определяет, сколько комбинаций на основе правил социальной инженерии будет создано для каждого слова из исходного словаря.

Гибридная атака



Гибридная атака похожа на словарную, за исключением того, что можно устанавливать свои собственные правила мутации слов. Программа поставляется с огромным набором файлов с правилами. Просто используйте тот, который лучше всего подходит для вашей задачи. Кроме того, гибридная атака позволяет дополнительно создавать, редактировать или изменять правила мутации в соответствии с вашими потребностями.

Атака по маске



Атака по маске является незаменимым инструментом, когда вы знаете часть пароля или имеете какую-либо информацию о нем. Например, если известно, что пароль состоит из 12 символов и начинается с 'loveme', то достаточно перебрать последние 6 символов пароля чтобы угадать весь пароль. Вот для чего нужна атака в маске. В нашем примере можно установить такую маску: loveme%c%c%c%c%c%c
Для получения более подробной информации о том, как работает маска, обратитесь к нашей онлайн-документации.

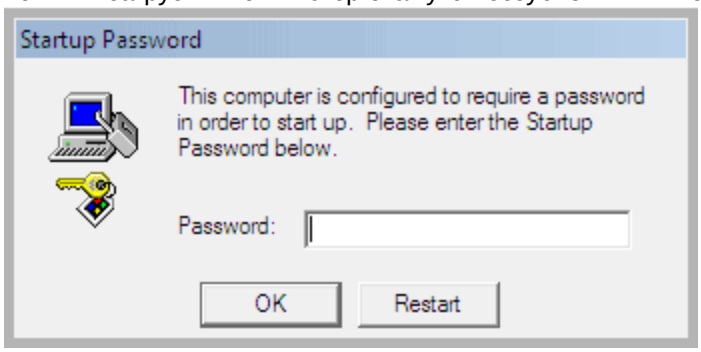
3.5.5 Поиск пароля SYSKEY

SYSKEY - это дополнительный уровень защиты операционной системы, который впервые был представлен в Windows 2000. SYSKEY по-умолчанию всегда включен и предлагает три типа защиты:

1. **По-умолчанию** - ключ шифрования SYSKEY хранится в реестре Windows.
2. **Загрузочный диск** - ключ шифрования хранится на дискете.
3. **Начальный пароль** - ключ шифрования создается на основе стартового пароля.

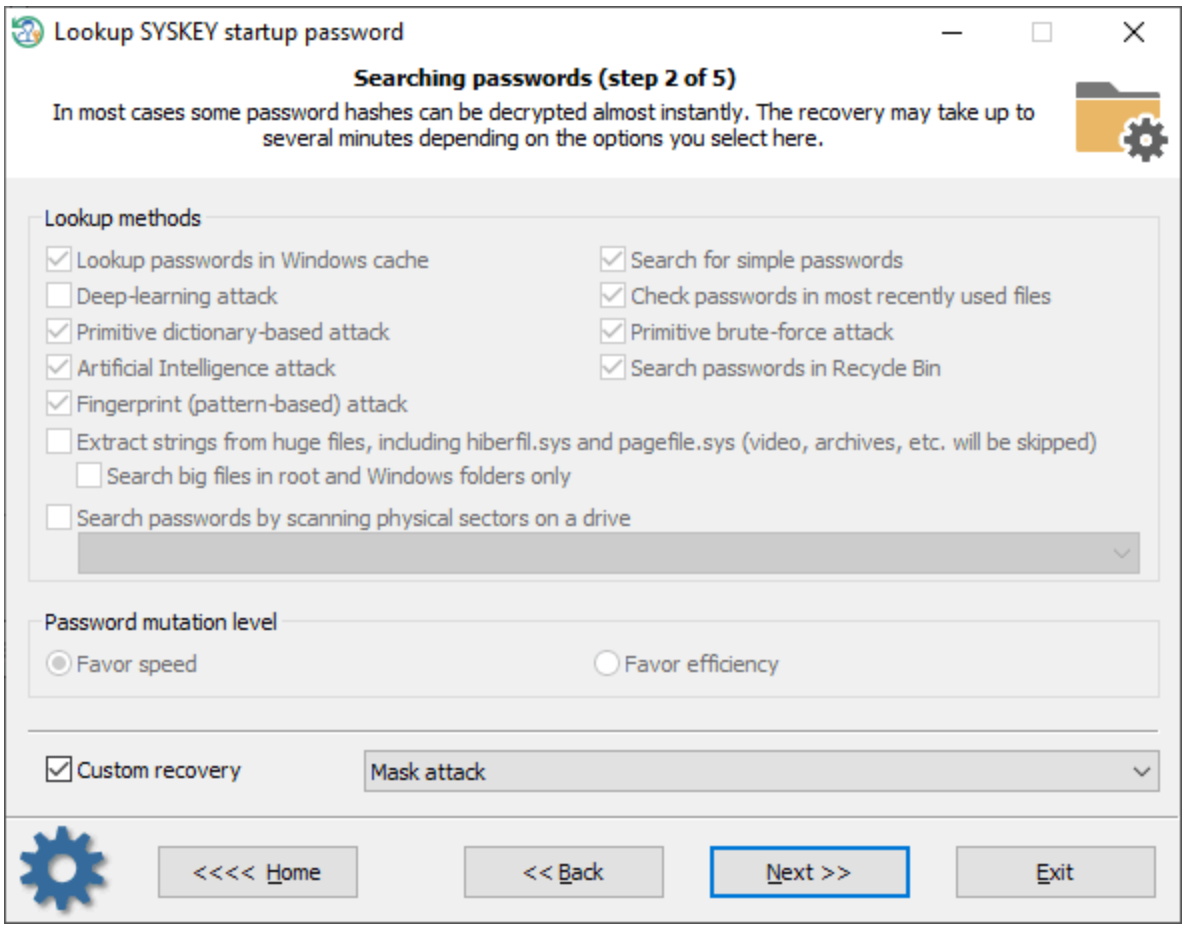
Очень часто мошенники используют SYSKEY для того, чтобы установить на компьютере жертвы начальный пароль и блокировать таким образом дальнейшую загрузку операционной системы. Обычно они связываются с вами, представившись сотрудниками службы поддержки Microsoft, и сильным Индийским акцентом постараются уверить, что ваш ПК имеет серьезные, критические проблемы с безопасностью, которые необходимо срочно исправить. Как правило, они пытаются убедить вас разрешить дам им удаленный доступ к вашему компьютеру, чтобы исправить эти 'проблемы'. Если вы совершите

неосторожность и разрешите сделать им это, они просто установят стартовый пароль SYSKEY. После перезагрузки вы получите запрос на ввод пароля, который, естественно, неизвестен и все дальнейшие попытки загрузить компьютер окажутся безуспешными пока вы не заплатите мошенникам за разблокировку.



К счастью, в большинстве случаев, но не всегда, устанавливаемые мошенниками пароли довольно простые и могут быть подобраны и расшифрованы при помощи инструмента для поиска пароля SYSKEY. Вам необходимо пройти через три простых шага, чтобы запустить поиск пароля:

Установка и настройка поиска пароля SYSKEY

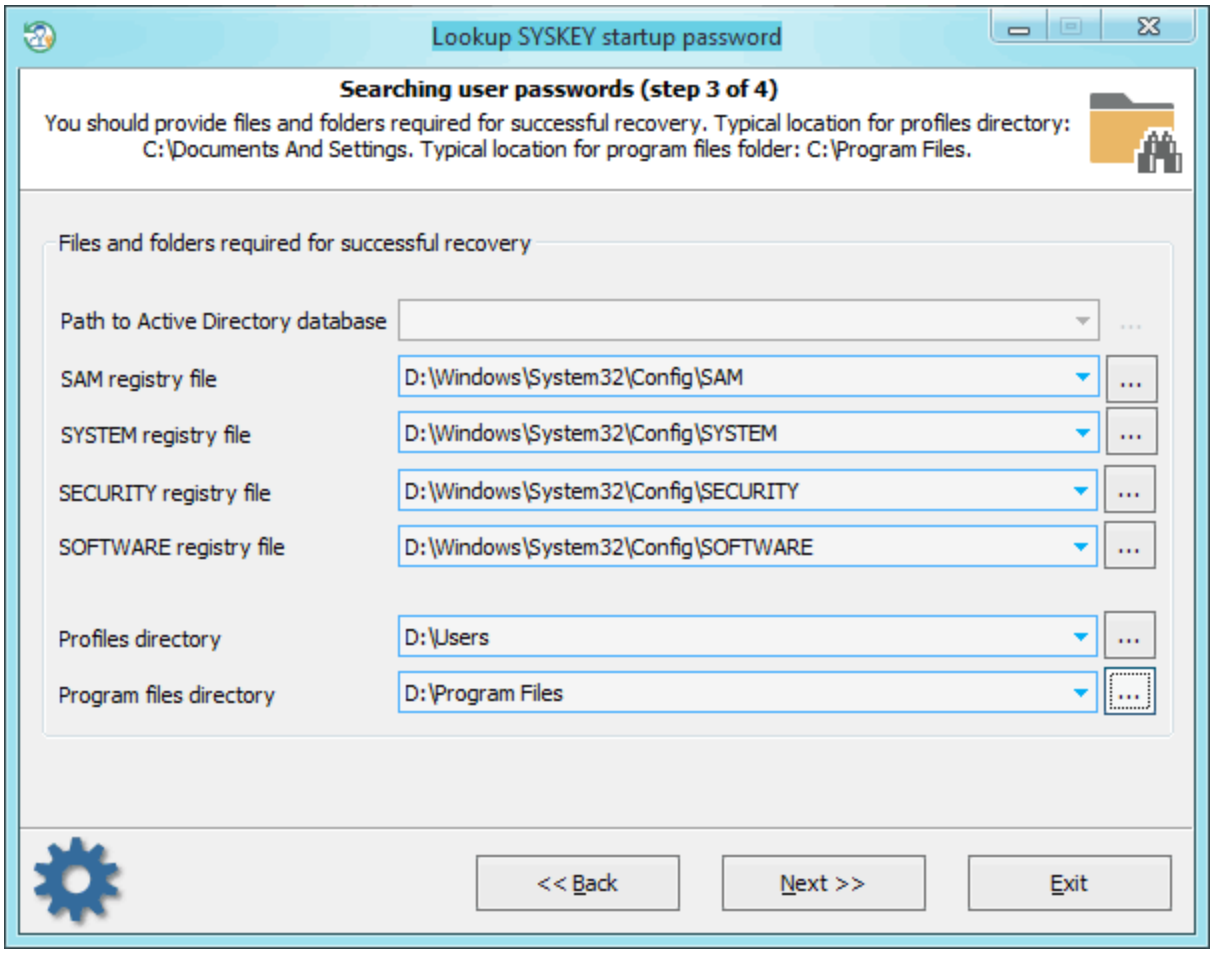


Поиск пароля SYSKEY может занять довольно много времени и состоит из несколько шагов:

1. Поиск слов и паролей в системном кэше Windows. Данный метод в свою очередь тоже состоит из более чем дюжины мини-атак в ходе которых происходит подбор и проверка всевозможных найденных паролей пользователей, от секретов LSA, до паролей DSL, VPN, FTP, IM, паролей браузеров, паролей почты, базы данных Windows Search и т.д.
2. Анализ простых, коротких паролей, клавиатурных комбинаций и т.д.
3. Сканирование, анализ и выборка слов из всех последних открываемых пользователем файлов целевой системы.
4. Простая атака по словарю. Проверяются все пароли из встроенного словаря для Light и Standard редакций или из нескольких словарей (Арабский, Китайский, Английский, Французский, Немецкий, Португальский, Русский, Испанский) для Advanced Edition. Если установлена опция глубокого поиска, то при проверке дополнительно используются простейшие мутации слов.
5. Простая атака методом перебора. Программа автоматически меняет настройки перебора в зависимости от установленных настроек мутации.
6. Интеллектуальная атака анализирует сетевую активность пользователя на компьютере. На основе анализа создаются предпочтения пользователя и производится создание семантического словаря атаки, который затем используется при подборе и угадывании пароля SYSKEY.
7. Поиск паролей в удаленных файлах, временных каталогах и т.д.
8. Примитивная Идентификационная атака на сложные Английские пароли.
9. Поиск слов и паролей в больших файлах: RAM дисках, hiberfil.sys, pagefile.sys и т.д.
10. Поиск паролей путем индексирования и анализа слов в физических секторов выбранного диска. Если опция 'Password mutation level' выставлена в 'Deep search', то программа дополнительно попытается выполнить мутацию найденных слов. Используйте эту настройку аккуратно, т.к. проход по всем секторам с дополнительной мутацией слов может занять очень много времени.

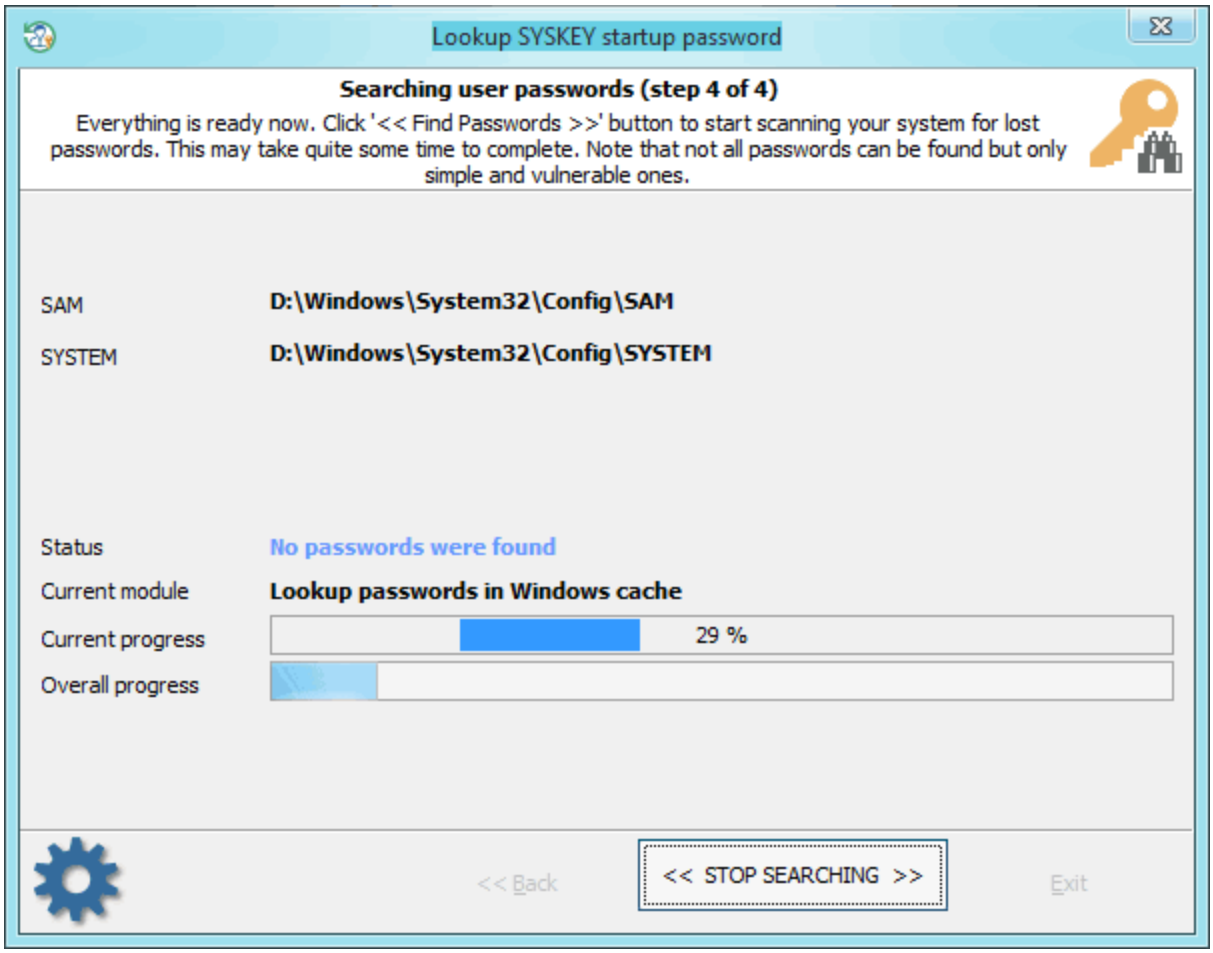
Чтобы запустить свое собственное восстановление, установите галочку напротив 'Настраиваемые атаки' и выберите тип атаки. На одном из следующих шагов вам будет предложено настроить опции выбранной атаки.

Выбор источника данных



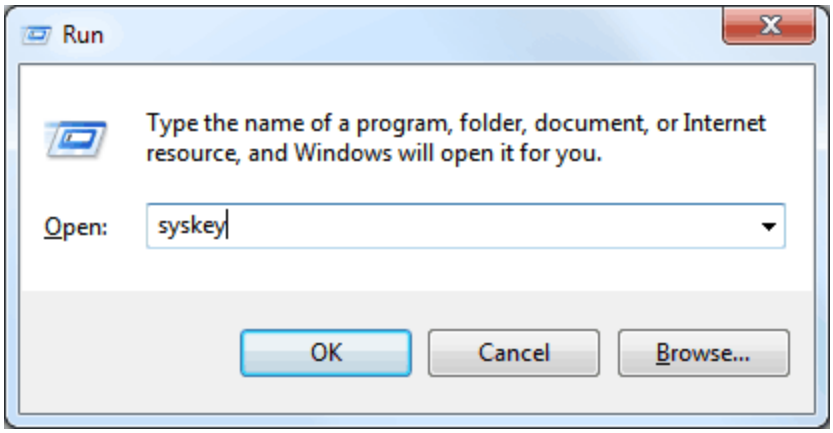
При поиске пароля SYSKEY особое внимание следует уделить правильному выбору всех необходимых в процессе анализа файлов и каталогов. Без них подбор паролей будет неэффективен или даже невозможен. Программа автоматически производит поиск файлов, но иногда, например, если на компьютере было установлено несколько операционных систем, требуется 'ручное управление'. Имейте в виду, что при наличии 2-х или более логических дисков, порядок букв для этих дисков может быть совершенно иной, нежели чем на оригинальной системе.

Поиск и расшифровка пароля SYSKEY

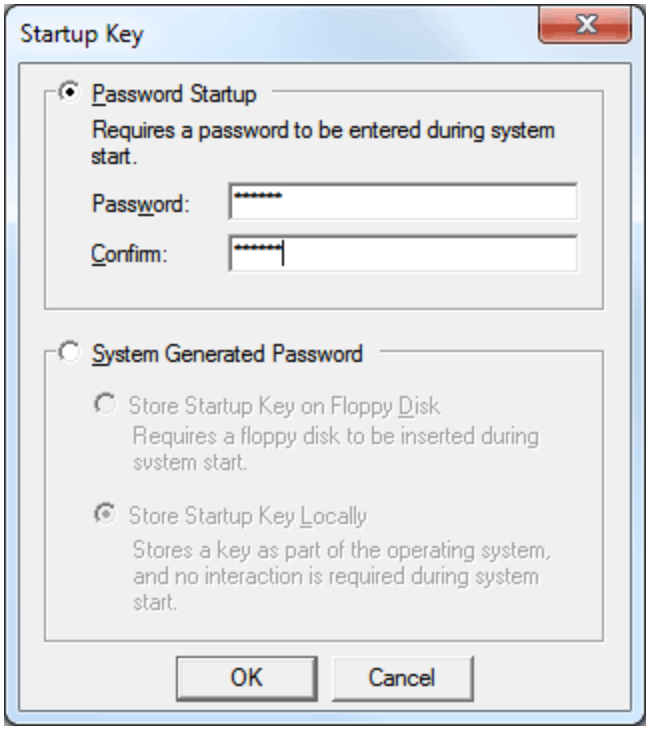


Поиск и угадывание пароля SYSKEY может занять некоторое время, которое зависит от настроек программы и особенностей вашего компьютера.
Учтите, из-за особенности шифрования SYSKEY, не все пароли могут быть расшифрованы и восстановлены, а только простые и уязвимые!

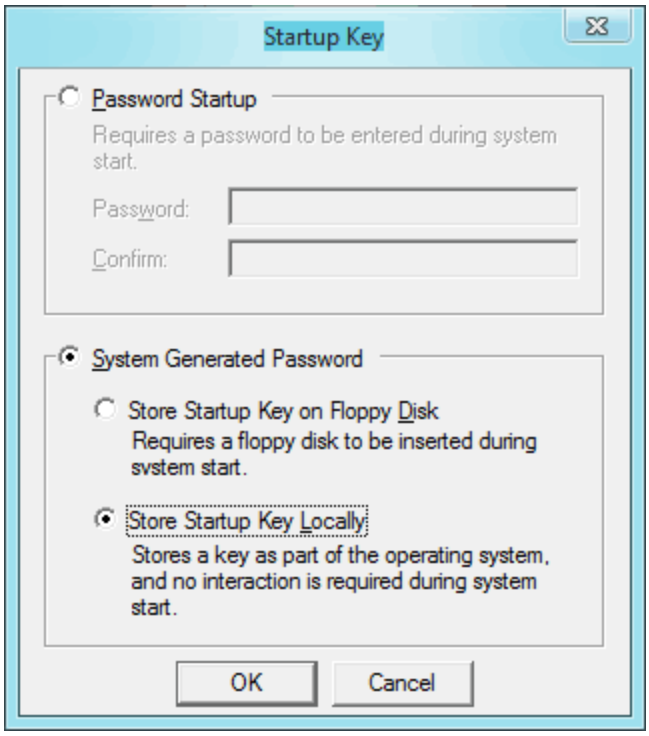
После того, как текстовый пароль SYSKEY был найден, необходимо отключить запрос на пароль, который появляется во время загрузки, вернув начальное состояние системы. Для этого, войдите в свою учетную запись Windows, нажмите сочетание клавиш '**Win+R**', введите 'SYSKEY' и щелкните кнопку 'OK', как показано на рисунке ниже.



Эта команда запустит диалог с настройками SYSKEY. Все, что необходимо сделать, это нажать конку *'Update*' и переключить опцию *'Password Startup*' обратно на '*System Generated Password*', указав найденный текстовый пароль.



После всех изменений, настройки SYSKEY должны выглядеть таким образом:

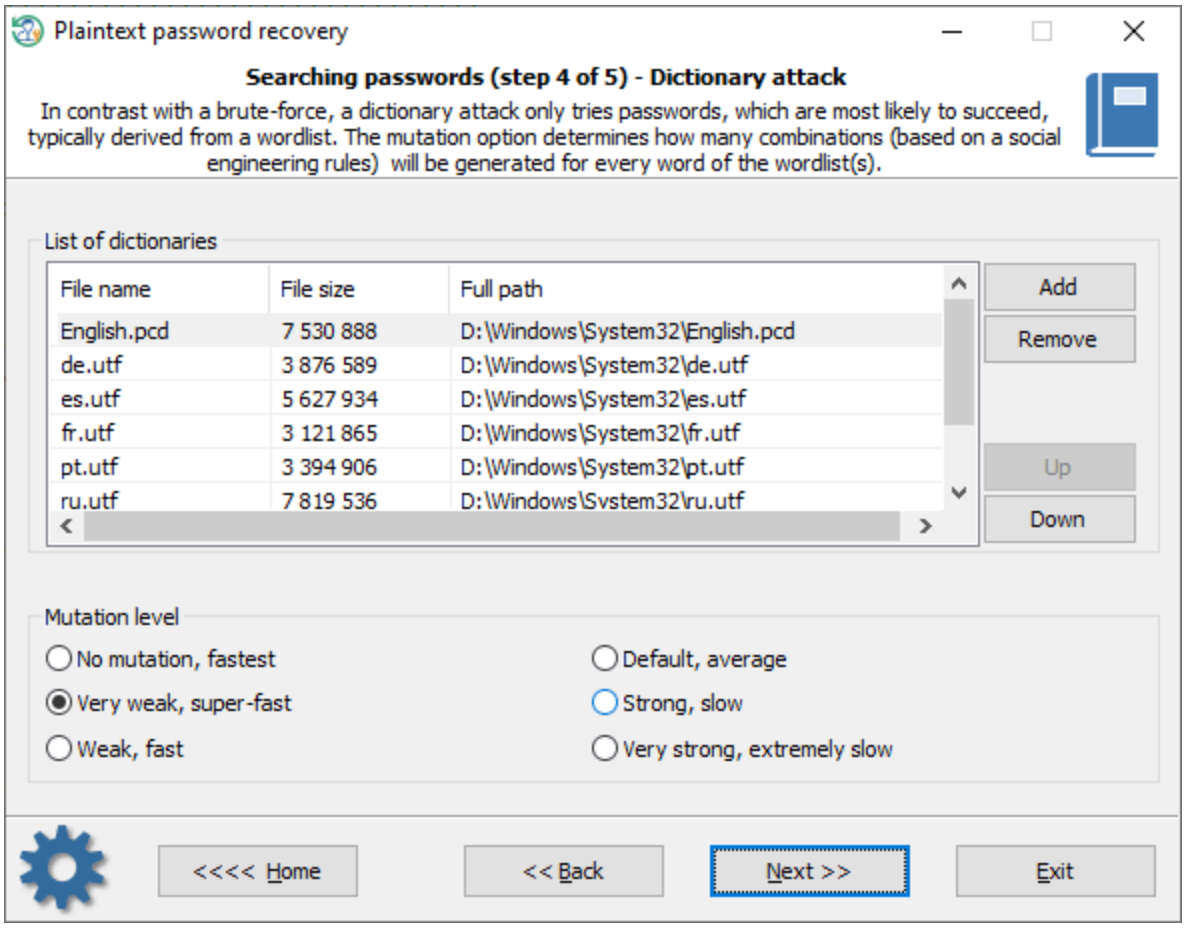


3.5.5.1 Настраиваемые атаки

Если выбрана опция 'Настраиваемая атака', то программа предлагает 3 дополнительных инструмента для угадывания паролей:

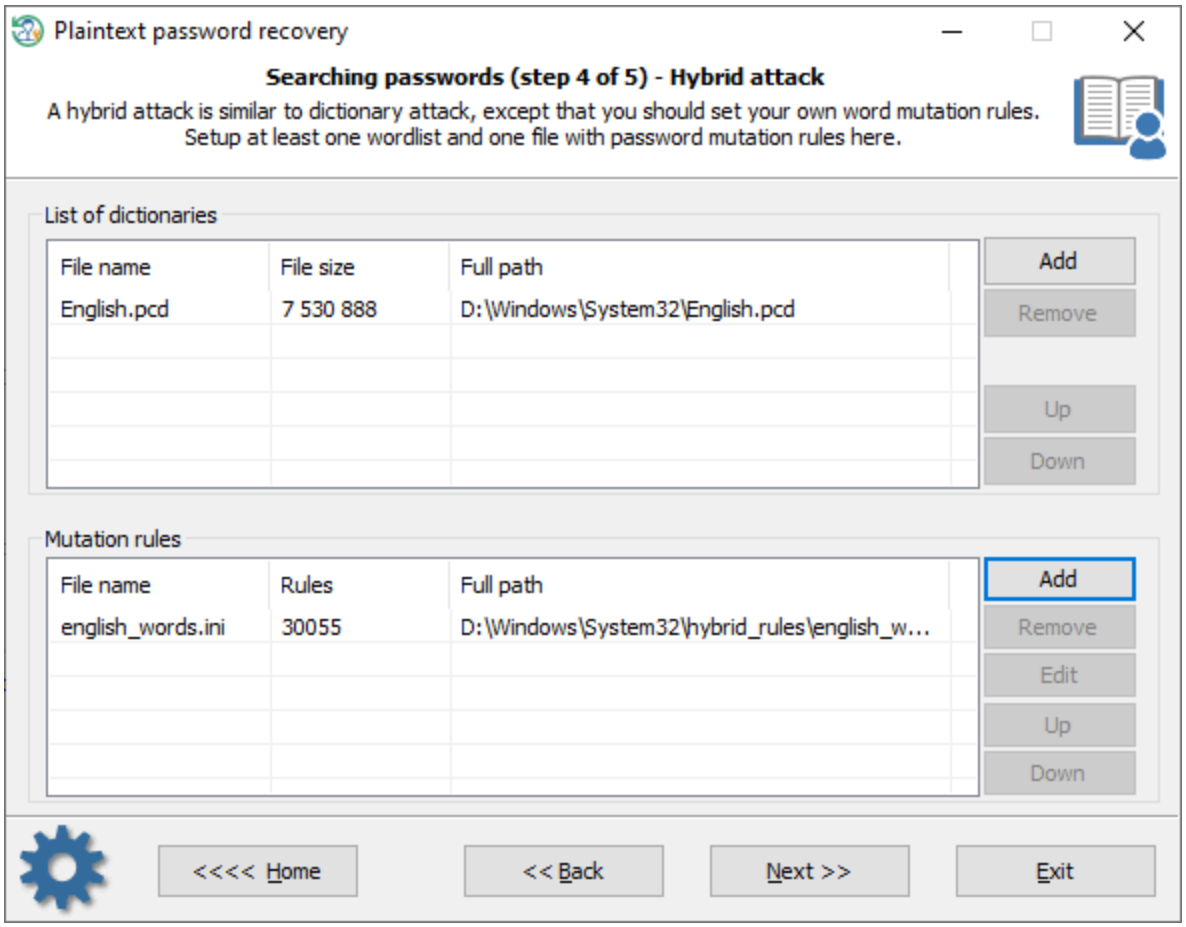
- Словарная атака
- Гибридная атака
- Атака по маске

Словарная атака



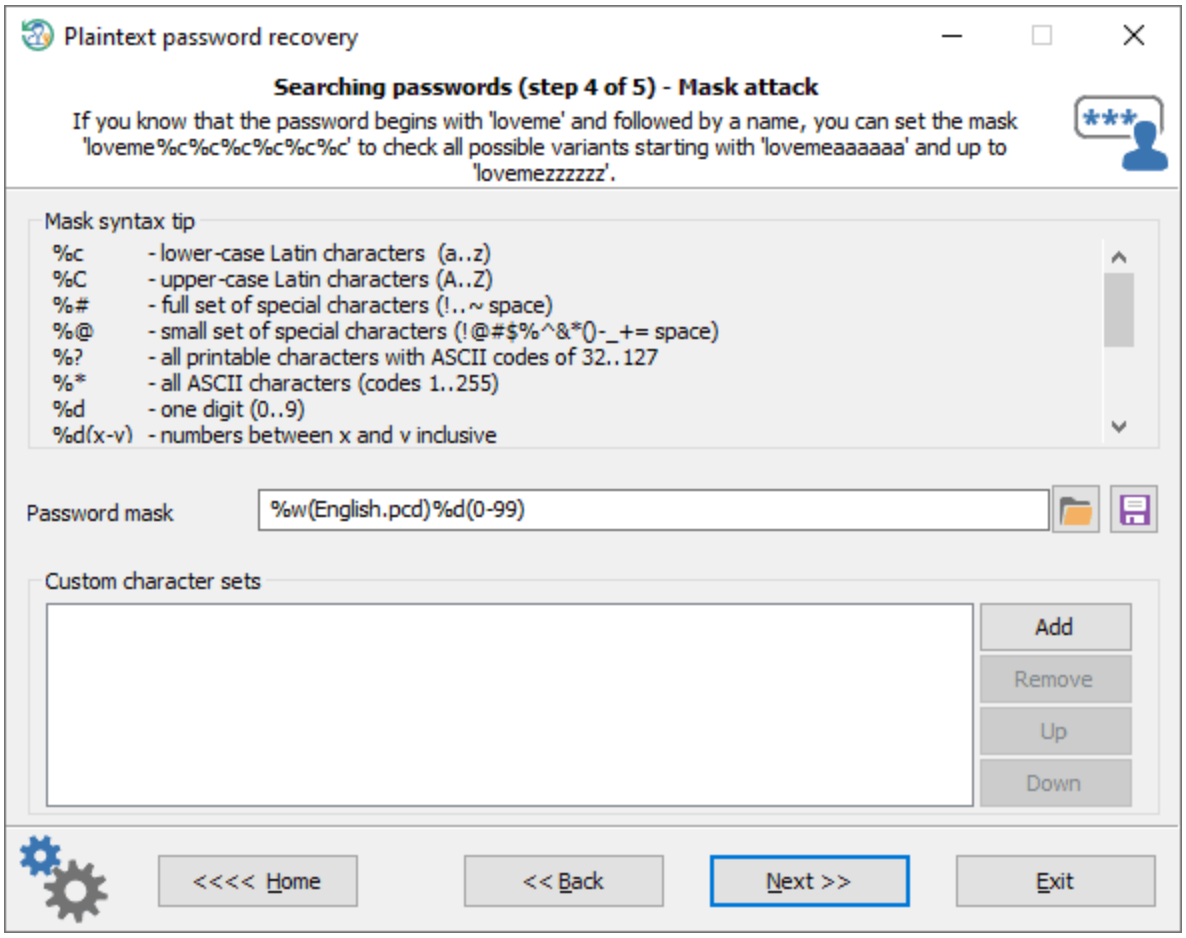
Атака по словарю использует слова из заданного списка для подбора наиболее вероятных кандидатов в пароли. RWP поддерживает различные типы словарей: ASCII, UNICODE, UTF8, а также зашифрованные/сжатые словари в собственном формате PCD. Вы можете использовать как стандартные, поставляемые вместе с программой, так и свои собственные словари. Чтобы использовать свой словарь, скопируйте его на USB-носитель и подключите его к целевому компьютеру. Уровень мутации определяет, сколько комбинаций на основе правил социальной инженерии будет создано для каждого слова из исходного словаря.

Гибридная атака



Гибридная атака похожа на словарную, за исключением того, что можно устанавливать свои собственные правила мутации слов. Программа поставляется с огромным набором файлов с правилами. Просто используйте тот, который лучше всего подходит для вашей задачи. Кроме того, гибридная атака позволяет дополнительно создавать, редактировать или изменять правила мутации в соответствии с вашими потребностями.

Атака по маске

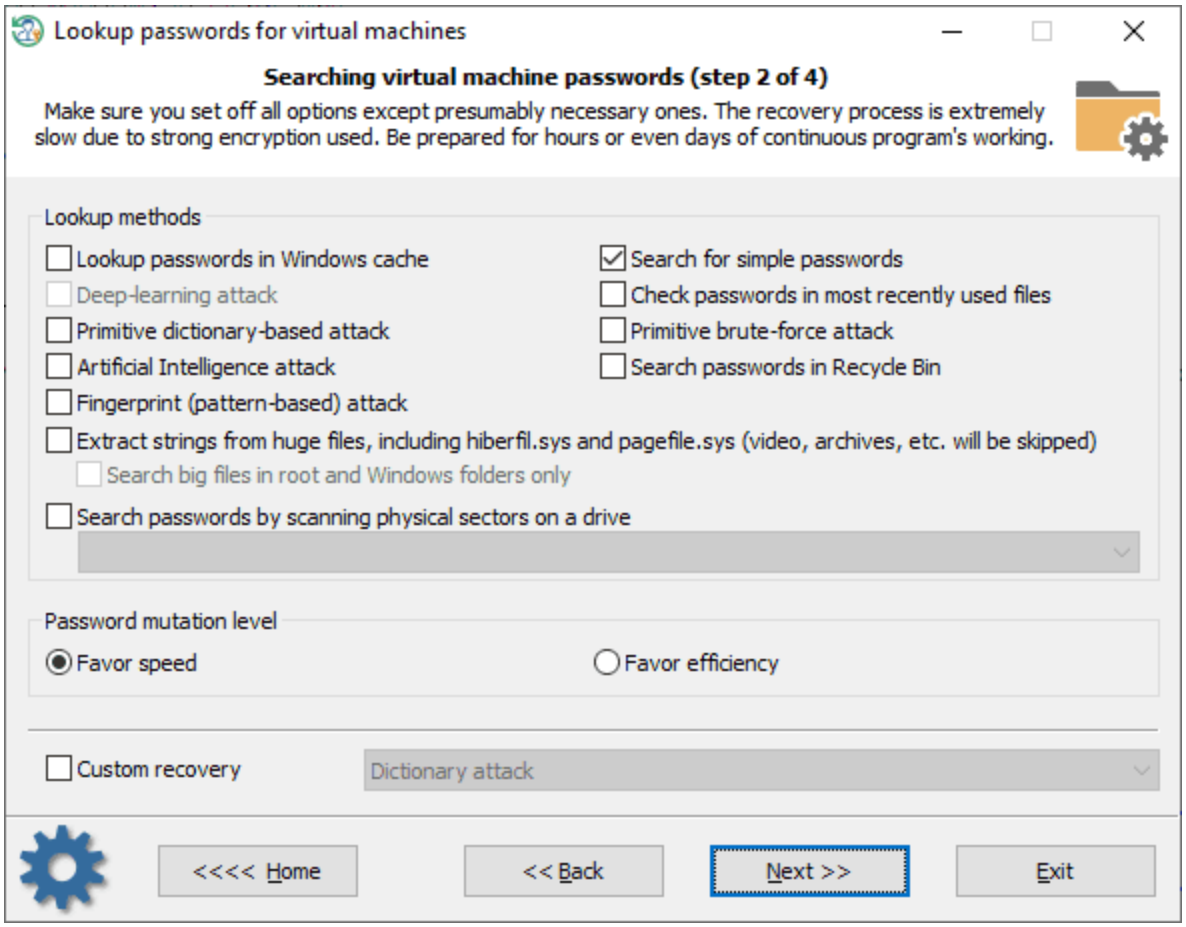


Атака по маске является незаменимым инструментом, когда вы знаете часть пароля или имеете какую-либо информацию о нем. Например, если известно, что пароль состоит из 12 символов и начинается с 'loveme', то достаточно перебрать последние 6 символов пароля чтобы угадать весь пароль. Вот для чего нужна атака в маске. В нашем примере можно установить такую маску: loveme%c%c%c%c%c%c
Для получения более подробной информации о том, как работает маска, обратитесь к нашей онлайн-документации.

3.5.6 Поиск паролей виртуальных машин

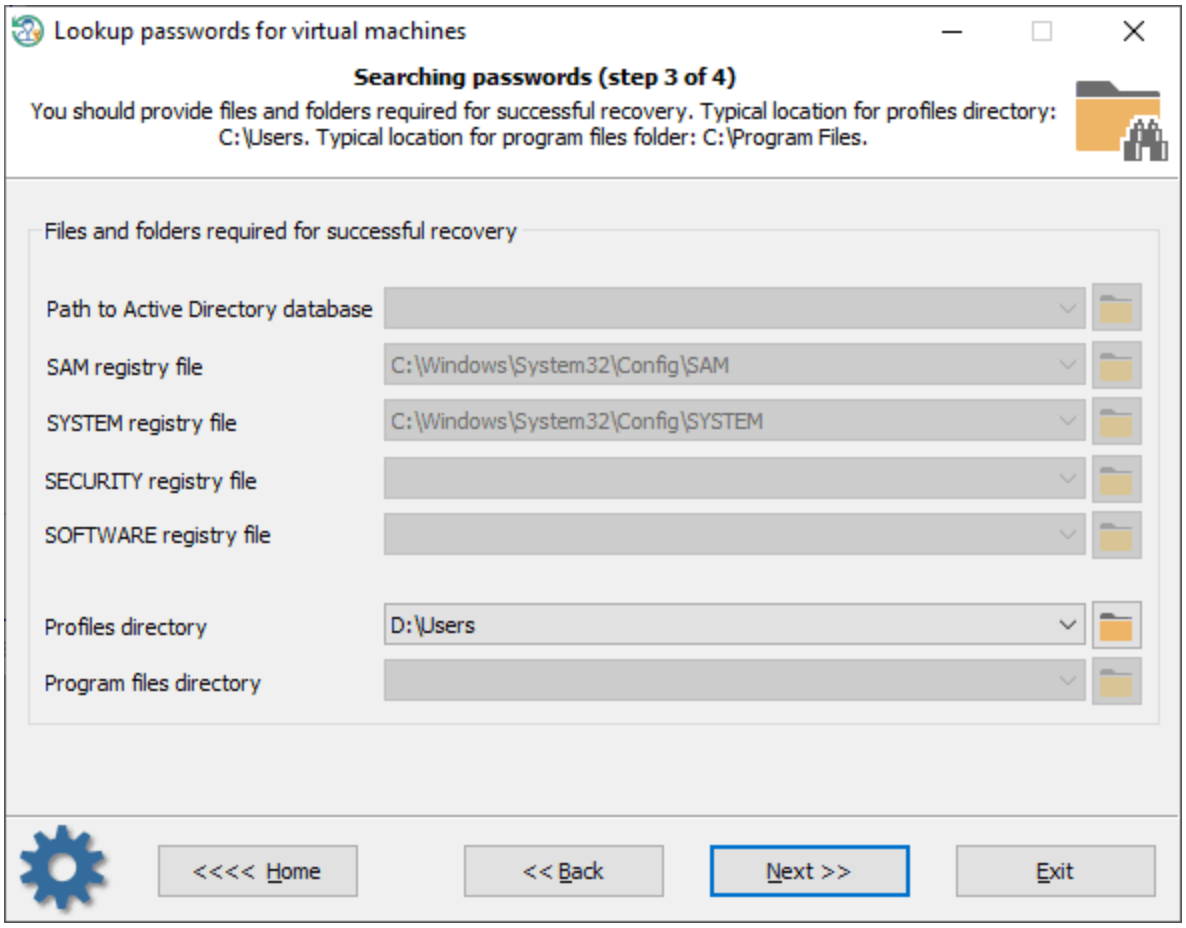
Если потерян или забыл пароль виртуальной машины, в RWP имеется необходимый инструмент для поиска паролей доступа к виртуальным машинам. Текущая версия программы поддерживает восстановление виртуальных машин VmWare и Oracle VirtualBox. Обе программы для виртуализации имеют очень сильную защиту, поэтому поиск паролей имеет ряд особенностей, о которых будет рассказано ниже.

Установка опций поиска и методов восстановления



В самом начале необходимо определиться с методами поиска. Восстановление паролей виртуальных машин - очень и очень медленный процесс, поэтому рекомендуется отключить наиболее затратные методы поиска. Можно также выбрать пользовательское восстановление. За это отвечает опция '*Настраиваемые атаки*', которая переключает между настраиваемыми и готовыми шаблонами атак. Если выбрать первое, то во время следующих шагов Мастера будет предложено настроить опции выбранной атаки. Настраиваемые атаки лучше подходят для случаев, когда известна к.л. информация о забытом пароле.

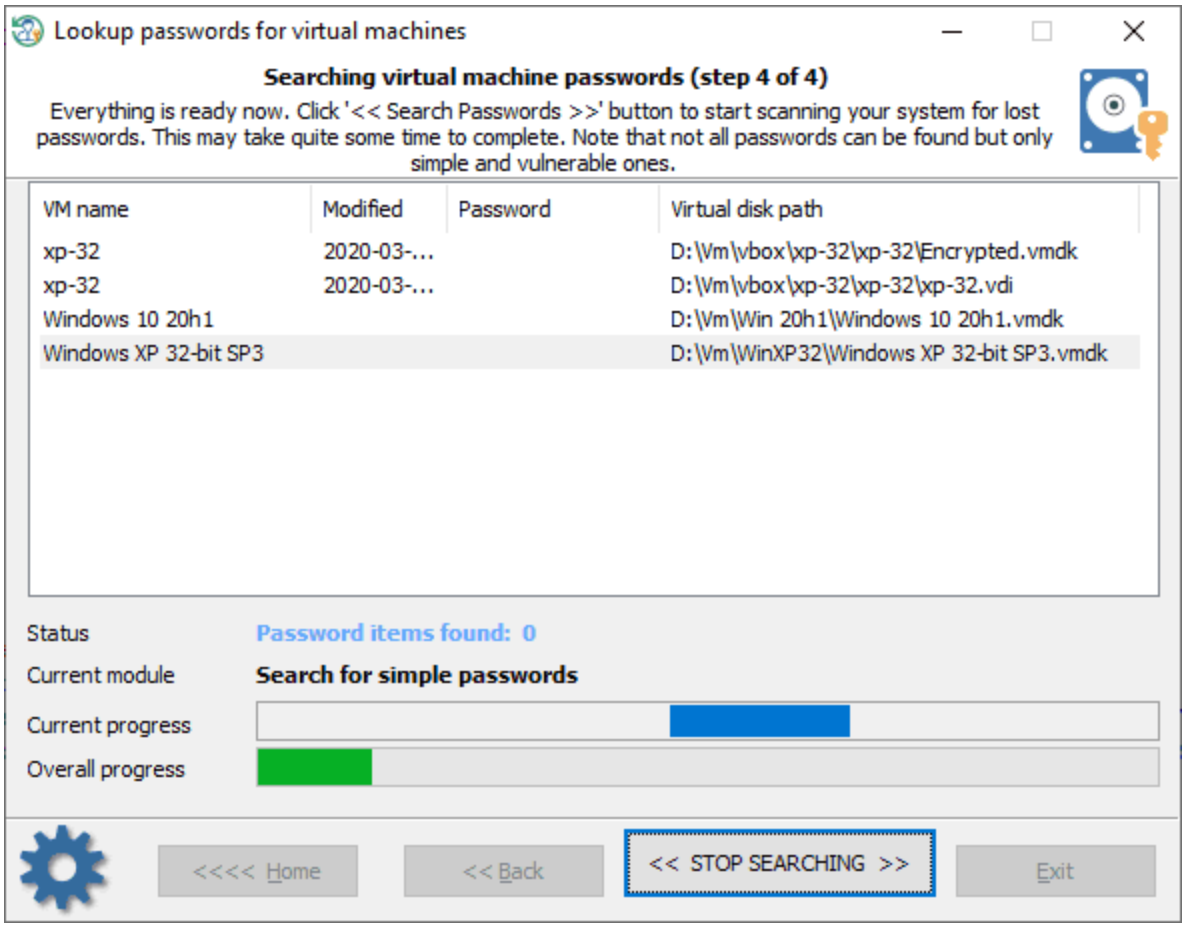
Настройка каталогов



При поиске паролей виртуальных машин следует уделить особое внимание выбору папок, необходимых для анализа файлов и поиска виртуальных машин. Без них подбор паролей будет неэффективен или программа будет не в состоянии обнаружить виртуальные машины. В большинстве случаев RWP автоматически производит поиск необходимых файлов.

Имейте в виду, порядок букв дисков может отличаться от оригинальной системы!

Поиск и расшифровка паролей виртуальных машин



Поиск паролей виртуальных машин может занять много времени. Все виртуальные машины имеют хорошую защиту. В некоторых случаях скорость перебора составляет всего несколько паролей в секунду. Поэтому для оптимизации и увеличения скорости, исключите из процесса поиска ненужные виртуальные машины, используя для этого контекстное меню.

3.5.7 Поиск паролей к зашифрованным документам

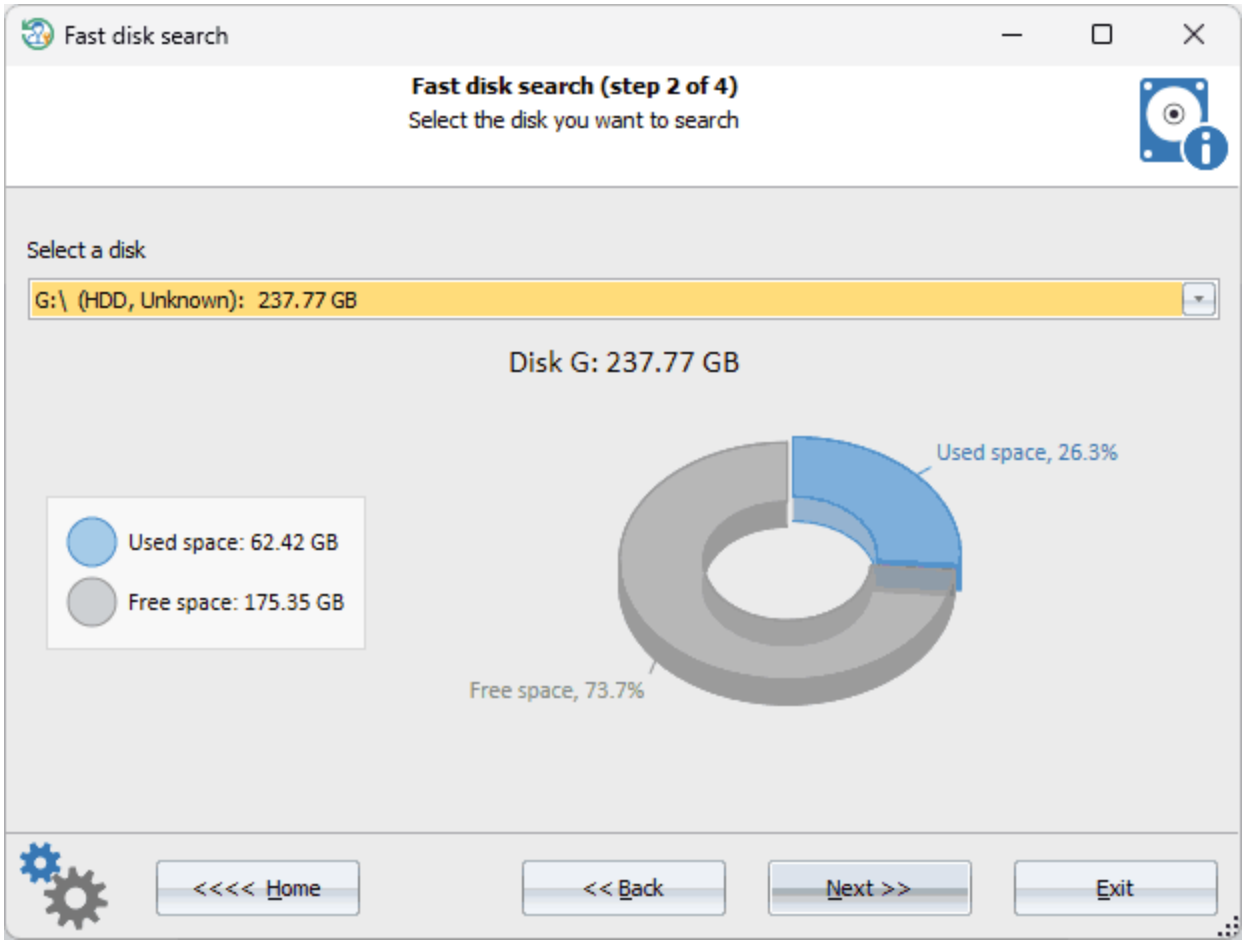
Почти все современные документы имеют очень сильную защиту шифрованием, и подобрать пароль, например, перебором, в большинстве случаев, не представляется возможным. Поэтому, если пароль шифрования для документа не подобран обычными средствами, то RWP - ваш последний шанс восстановить его.

Не секрет, что многие пользователи используют одни и те же (или немного модифицированные) пароли и при создании учетных записей Интернет, и для шифрования документов. В RWP для расшифровки документов можно задействовать всю мощь встроенного движка для поиска таких паролей. Если не вдаваться в подробности, то на первый взгляд все довольно тривиально: программа сканирует систему, отбирает найденные пароли, а также их кандидаты, составляет возможные мутации и модификации паролей, а на финальном этапе выполняет проверку всех полученных вариантов. Несмотря на кажущуюся простоту, алгоритмы программы довольно продвинутые. Например, только одна группа для поиска паролей состоит из

нескольких десятков модулей. А есть еще группы из модулей мутации, искусственно интеллекта и т.д. и т.п.

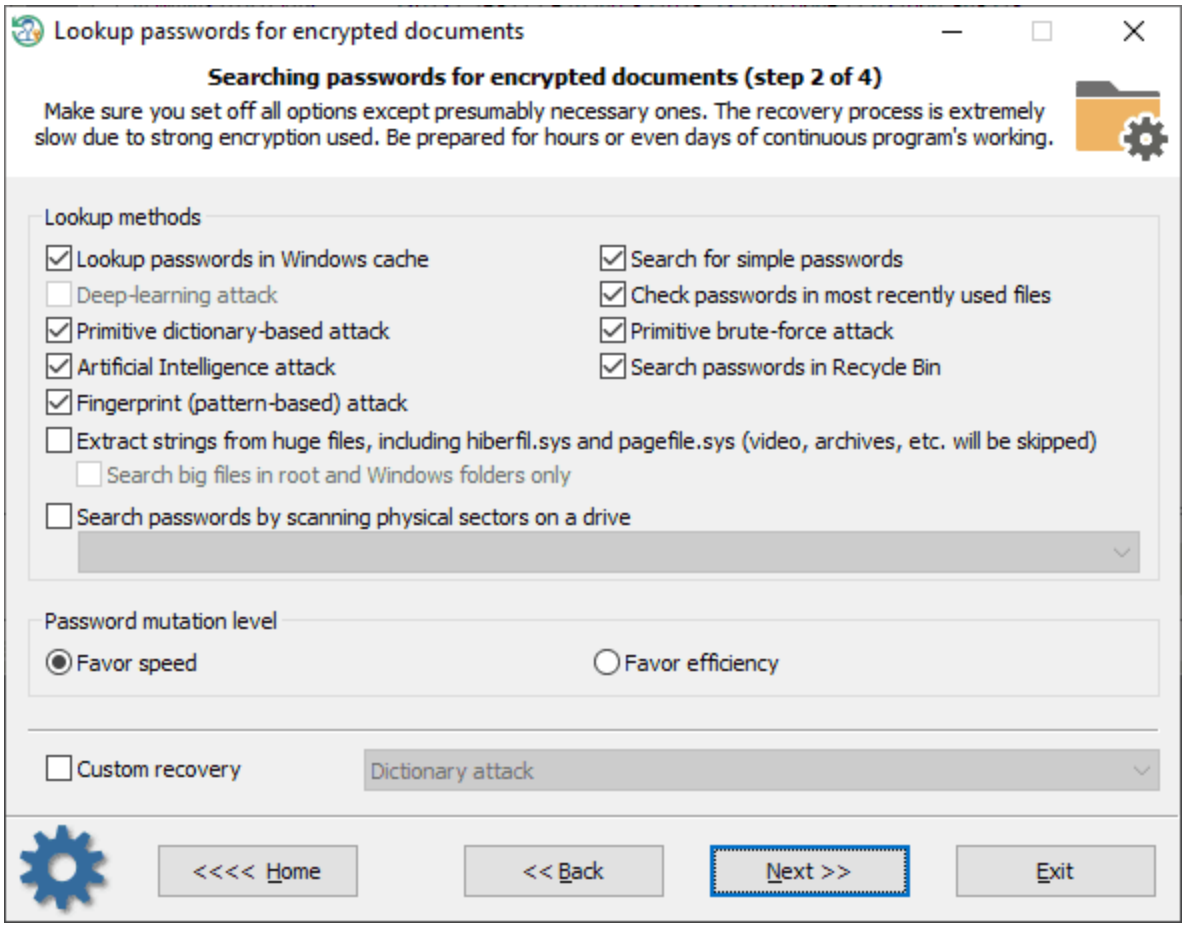
Текущая версия программы поддерживает следующие документы:
- Документы Microsoft Office 97 и новее
- Документы в формате OpenDocuments: OpenOffice, LibreOffice, MyOffice.
- Документы PDF (как пароль пользователя, так и владельца).

Выбор диска для поиска



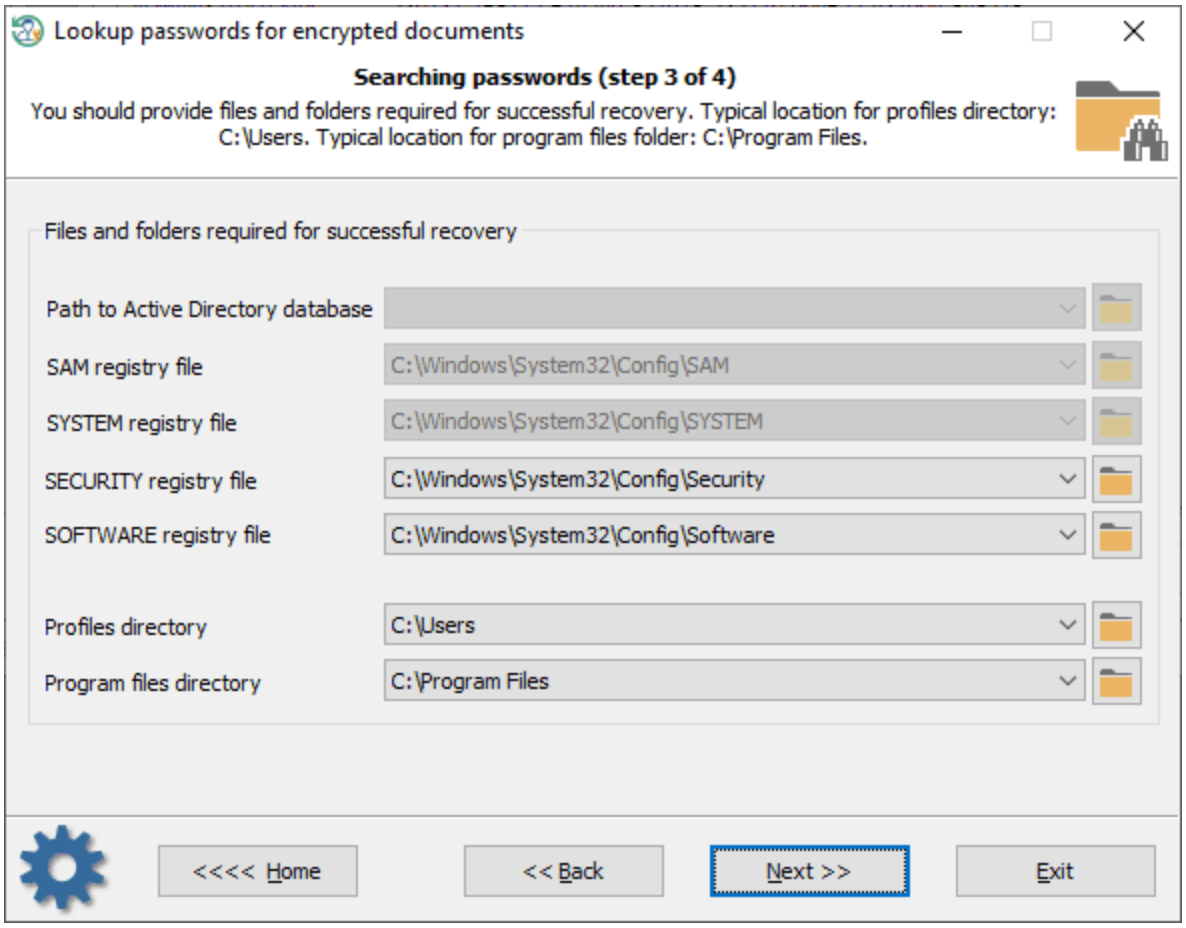
Выберите диск, на котором необходимо выполнить поиск документов.
Учтите, как только вы выберете диск и нажмете кнопку Далее, программа сразу начнет сканировать диск в фоновом режиме. Таким образом, к финальному диалогу, как правило, вы уже получите список всех найденных зашифрованных документов на всем диске.

Установка опций поиска и методов восстановления



В самом начале необходимо определиться с методами поиска. Восстановление паролей документов чрезвычайно медленный процесс. Особенно, если их несколько. Поэтому, рекомендуется отключить наиболее затратные методы поиска. Если что-то известно о пароле, то не лишенным разумности будет выглядеть выбор пользовательского восстановления. За это отвечает опция '*Настраиваемые атаки*', которая переключает между настраиваемыми и готовыми шаблонами атак. Если выбрать первое, то во время следующих шагов Мастера программа предложит настроить опции выбранной атаки. Настраиваемые атаки лучше подходят для случаев, когда известна какая-либо информация о забытом пароле.

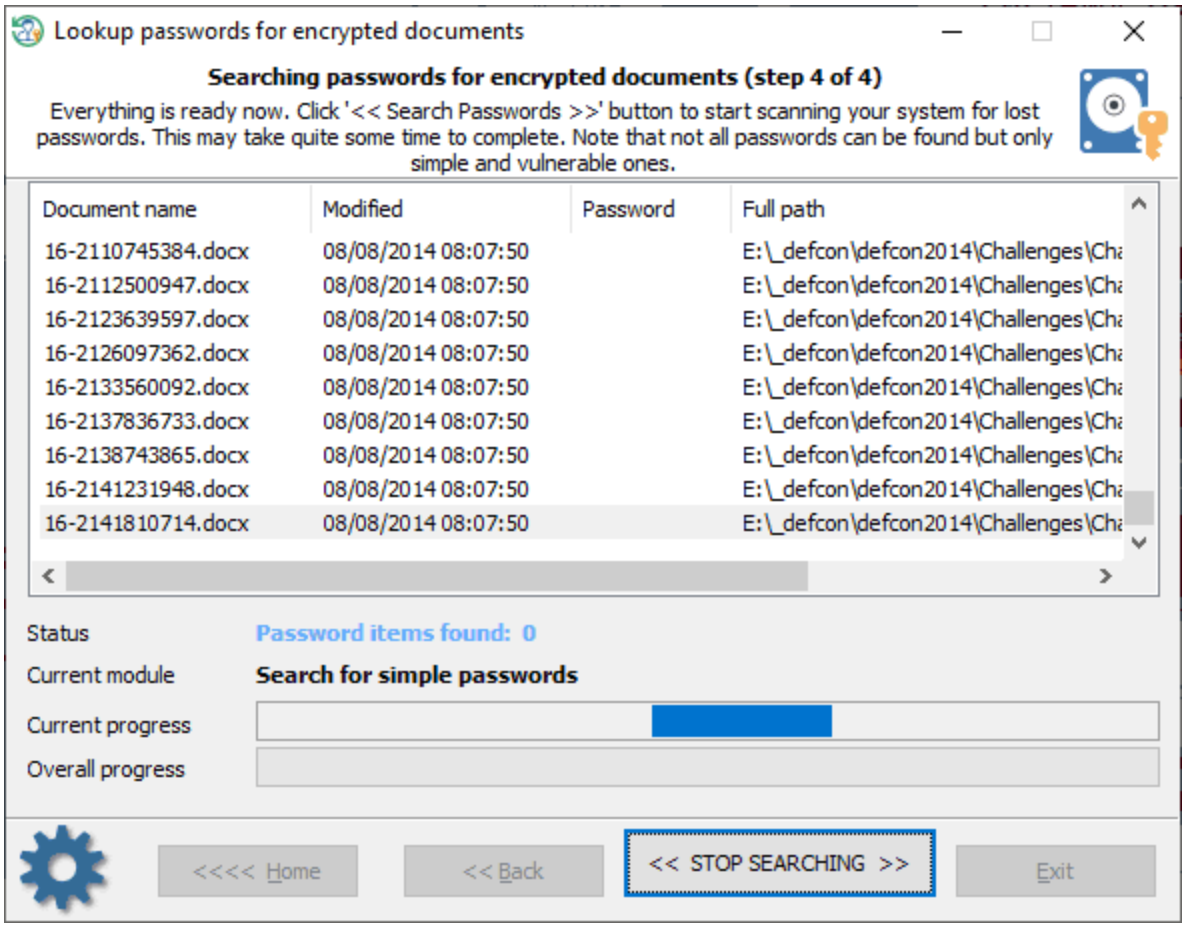
Настройка каталогов



При поиске паролей для зашифрованных документов ни в коем случае не стоит пренебрегать выбором папок. Иногда они жизненно необходимы для анализа файлов и кандидатов на пароли. Без них подбор может быть малоэффективен. В большинстве случаев RWP автоматически производит поиск необходимых файлов.

Имейте в виду, порядок букв дисков может отличаться от оригинальной системы!

Поиск и расшифровка паролей зашифрованных документов



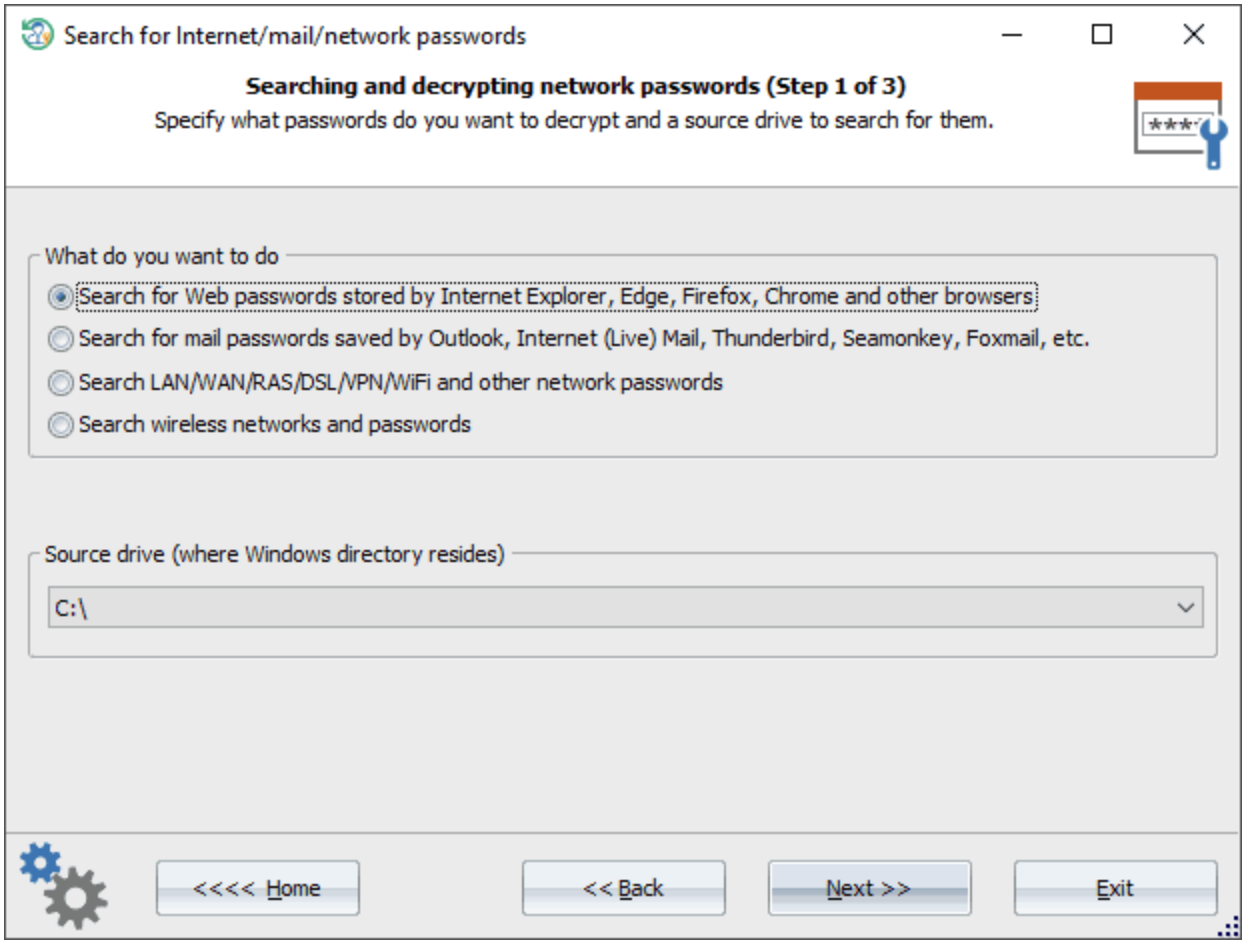
Поиск паролей документов может занять очень много времени. Например, поиск паролей к документам Microsoft Office 2013 или новее может составлять 1-2 пароля в секунду для одного документа! Поэтому, для оптимизации и увеличения скорости перебора, по-возможности исключите из процесса поиска ненужные документы, в идеале оставив только один необходимый документ. Для этого можно использовать контекстное меню. В противном случае, программа будет производить поиск паролей для всех найденных документов одновременно!

Если надо добавить новый документ, щелкните правой кнопкой мыши на списке и выберите '*Добавить новый документ*'.

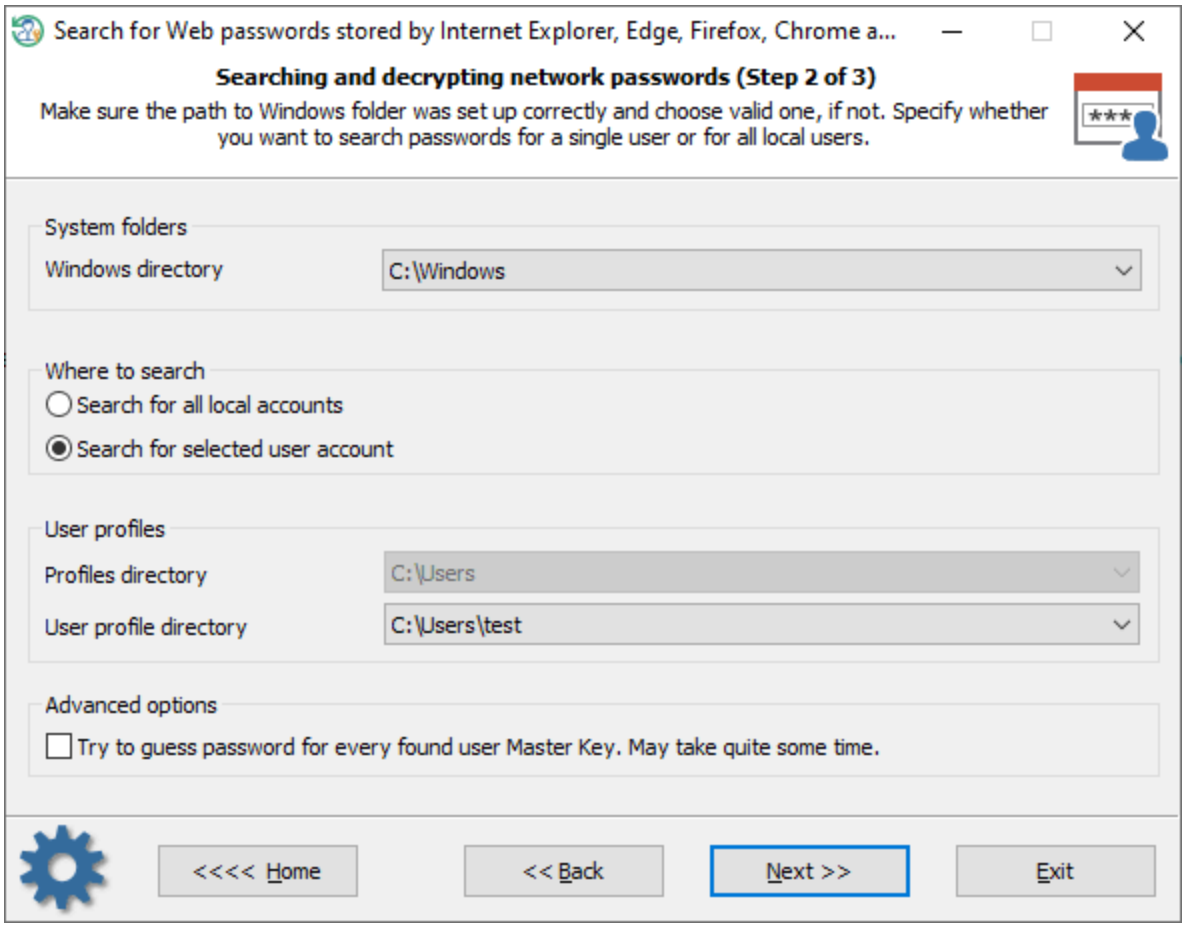
В новых версиях программы появилась возможность расшифровывать пароли Aadhaar и e-pan (электронные документы жителей Индии). Электронный документ Aadhaar представляет собой PDF файл, содержащий уникальный персональный номер, который присваивается каждому жителю Индии. Aadhaar считается крупнейшей в мире системой био-идентификации. Документ e-pan - это цифровой идентификатор, выданный налоговым департаментом Индии. Reset Windows Password имеет встроенную поддержку документов обоих типов. Для расшифровки документа Aadhaar/e-pan, щелкните правой кнопкой мыши на списке найденных файлов, удалите из списка все остальные документы (это значительно ускорит процесс поиска пароля) и запустите соответствующую атаку. Расшифровка PDF файлов Aadhaar/e-pan автоматически задействует 7 различных видов атак, что позволяет достичь практически 100% успеха.

3.5.8 Поиск сетевых и почтовых паролей

Одна из замечательных возможностей программы - поиск и расшифровка сетевых паролей пользователей ПК. Reset Windows Password поддерживает основные популярные браузеры и почтовые клиенты. Интерфейс разбит на три этапа для максимального упрощения процесса, оставив специфичные детали на откуп программе.



На первом шаге Мастера программа предлагает выбрать тип паролей для поиска и исходный диск с каталогом Windows. По умолчанию, предлагается первый жесткий диск с установленной системой.



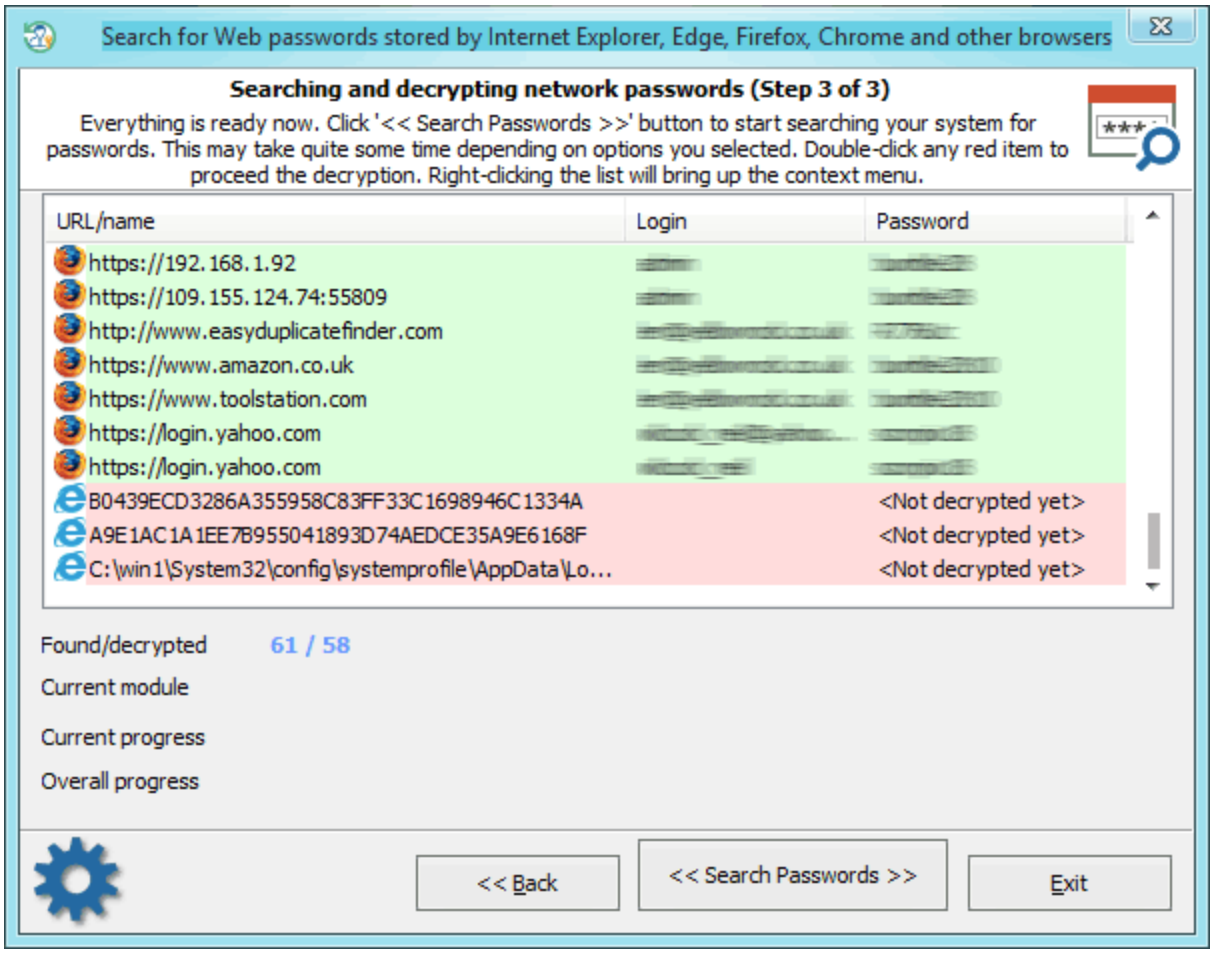
На следующем шаге следует уточнить расположение папки Windows, а также в каких каталогах будет производиться поиск паролей: во всех профилях пользователей или только в выбранном. В последнем случае, необходимо выбрать соответствующий каталог.

По умолчанию программа автоматически сканирует систему на наличие любой информации (например, TBAL или доменных секретов), которая может быть использована для расшифровки данных DPAPI без пароля пользователя. Однако, установив расширенный параметр, можно также заставить программу угадывать пароли Мастер-ключей DPAPI, используя некоторые найденные элементы. Например, найденные кэшированные учетные данные, LSA секреты, пароли браузеров, беспроводного/удаленного доступа/DSL/RAS/LAN и другие. Как только пароль Мастер-ключа DPAPI угадан, нет никакой необходимости предоставлять пароль пользователя. Программа использует расшифрованный Мастер-ключ для декодирования любых данных, защищенных этим ключом.
Однако, этот процесс может занять довольно значительное время, в зависимости от количества найденных Мастер-ключей и паролей для подбора.

В финальном диалоге нажатие кнопки **<< Поиск паролей >>** запускает процесс сбора, анализа и расшифровки данных. Будьте терпеливы, в зависимости от выбранных опций и количества пользователей целевой системы, этот процесс может занять довольно много времени.

3.5.8.1 Поиск веб паролей, хранящихся в браузерах

При выборе режима поиска Интернет паролей, вы должны увидеть примерно такую картинку:



Программа поддерживает расшифровку паролей основных популярных Интернет-обозревателей:

- Internet Explorer
- Edge
- Firefox
- Opera
- Chrome
- Safari
- Большинство браузеров на базе исходного кода Mozilla (Flock, Seamonkey, Pale Moon, Waterfox и т.д.)
- Основные браузеры на базе исходников Chromium: 360 Safe Browser, 7Star, Amigo, Brave, Centbrowser, Chedot, Canary, Coccoc, Comodo Dragon, Elements, Kometa, Orbitum, QQ Browser, Sputnik, Torch, UC Browser, Uran, Vivaldi.

Обозреватели интернет используют разные алгоритмы защиты персональных данных. Пароли следующих браузеров расшифровываются мгновенно:

- Internet Explorer 4-6
- Firefox и остальные браузеры на основе Mozilla (если не установлен Мастер Пароль)
- Старые версии Opera (если не установлен Мастер Пароль)

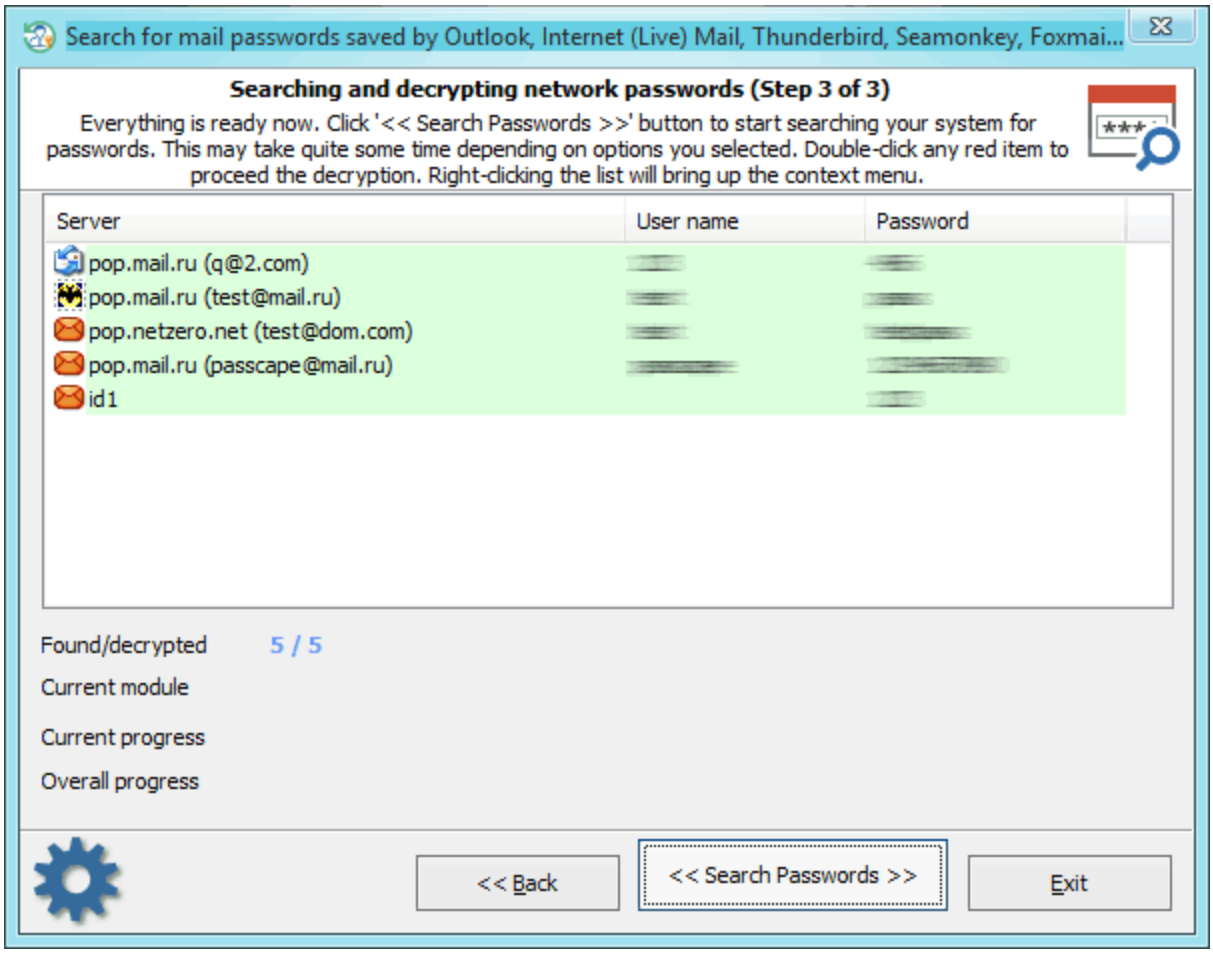
Расшифровка других данных требует ввода дополнительной информации. Как правило, Мастер Пароля или пароля пользователя учетной записи:

- Internet Explorer 10
- Edge
- Firefox (если установлен Мастер Пароль)
- Opera (если установлен Мастер Пароль)
- Chrome
- Safari

Чтобы активировать второй этап расшифровки, просто дважды щелкните мышкой по записи, выделенной красным цветом.

Браузер Internet Explorer 7-9 требует трехэтапной расшифровки. Сначала необходимо ввести URL адрес, где был сохранен пароль, затем ввести пароль учетной записи. Детали этой интересной защиты, которая применяется в Internet Explorer 7-9, можно узнать в нашей статье.

3.5.8.2 Поиск почтовых паролей популярных e-mail клиентов



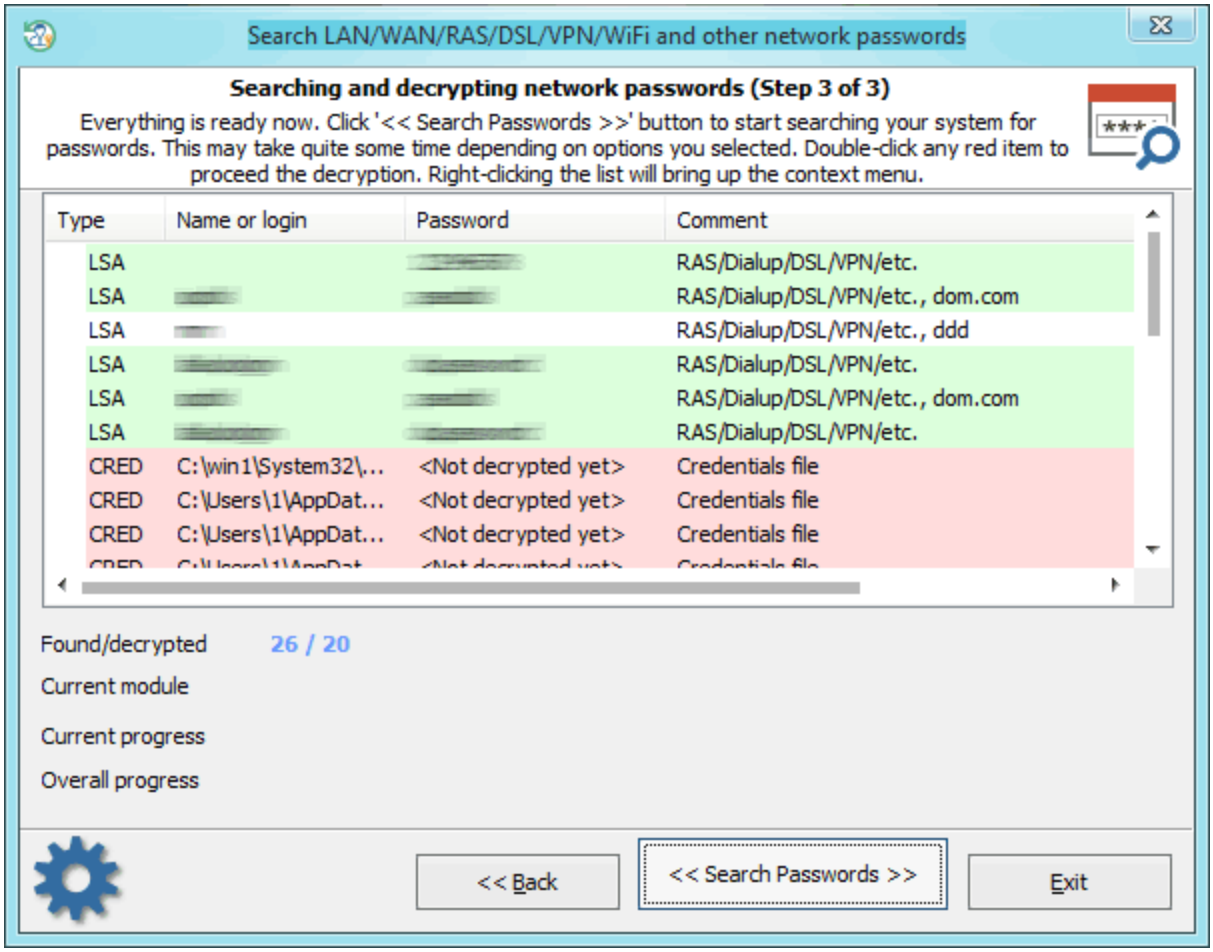
Поддерживаются следующие почтовые клиенты:

- Outlook Express
- Microsoft Office Outlook

- Internet Mail
- Internet Live Mail
- Windows Mail
- TheBat!
- Incredimail
- Eudora

Учтите, некоторые почтовые пароли могут хранится в браузерах. Это зависит от того, работал пользователь в почтовом клиенте или читал почту из Интернет-обозревателя. Пароли Outlook Express, TheBat!, Incredimail, Eudora и некоторых версий MS Office Outlook расшифровываются мгновенно. Для расшифровки остальных данных требуется пароль учетной записи. Просто дважды щелкните мышкой по выделенной красным цветом записи. Это активирует второй этап анализа найденных данных. Если введенный пароль пользователя подходит к остальным записям, они будут декодированы автоматически.

3.5.8.3 Поиск сетевых паролей LAN/WAN/RAS/DSL/VPN/WiFi и т.д.



Для сбора сетевых паролей программа имеет несколько модулей чтения и расшифровки секретов LSA, защищенного хранилища, менеджера паролей, Windows Vault и т.д.

Расшифровка данных, хранящихся в секретах LSA и защищенном хранилище происходит мгновенно и не требует ввода дополнительных параметров. Это распространяется на следующие данным:

- Кэшированные пароли пользователей
- Пароли некоторых системных учетных записей, SQL сервера, помощника удаленного рабочего стола и др.
- Пароли сервисов и служб запускаемых с задаваемыми учетными данными
- Некоторые сетевые пароли, хранимые на серверных ОС
- Пароли проводных соединений: RAS, DSL, VPN и т.д.
- Пароли старых версий IE/Outlook/OE/FTP и др.
- Пароли беспроводных соединений WPA/WPA2
- Пароли групповых политик домена
- Пароли VNC
- Пароли учетных записей Tortoise SVN
- Пароли учетных записей Open VPN
- другой

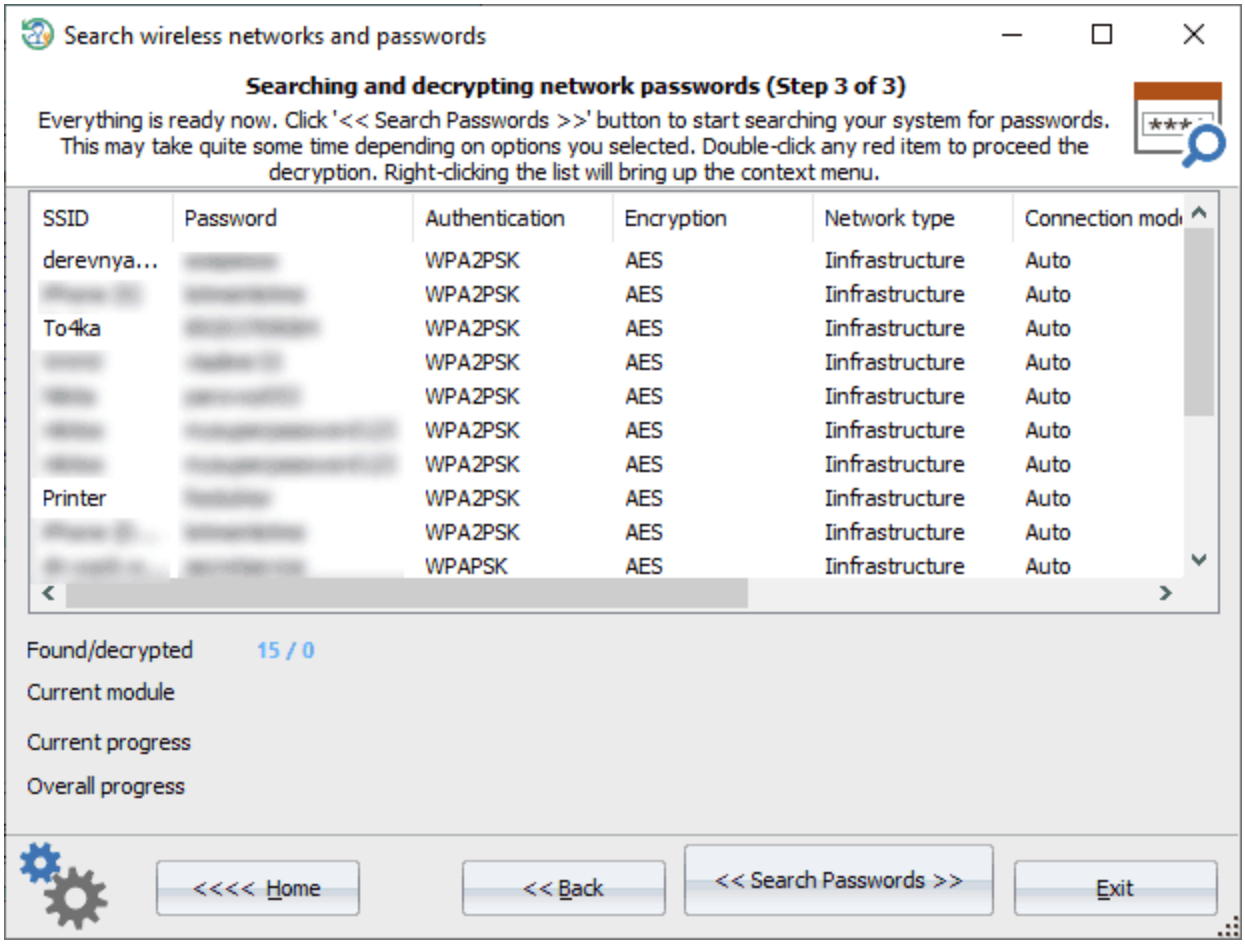
Другим паролям, защищенным при помощи DPAPI, для успешного декодирования дополнительно необходимо предоставить пароль учетной записи пользователя:

- Пароли, хранящиеся в Диспетчер учетных данных: 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.
- Записи Windows Vault: пароли некоторых версий IE/Outlook/Windows Mail, пароли учетных записей при использовании пароля PIN/Picture или биометрической аутентификации (только для ОС Windows 8).

Подробнее о шифровании DPAPI можно почитать в нашей детальной статье, посвященной этой защите.

В некоторых серверных операционных системах программа может успешно эксплуатировать найденную нами уязвимость, позволяющую расшифровывать пароли DPAPI без ввода пароля учетной записи владельца данных! Дополнительная информация содержится в нашей статье, посвященной уязвимости серверных ОС.

3.5.8.4 Поиск беспроводных паролей



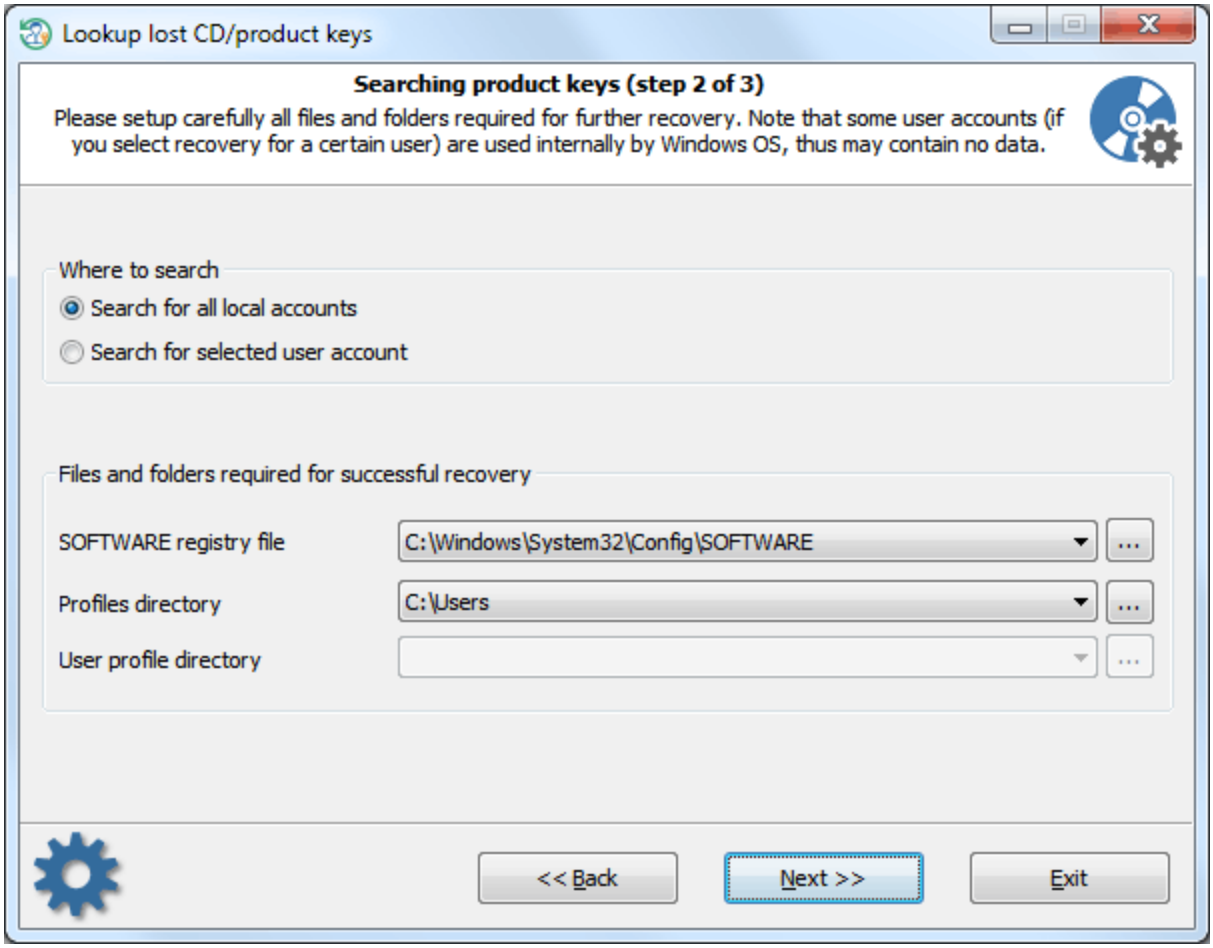
Пароли беспроводных сетей (всех пользователей) расшифровываются мгновенно.

3.5.9 Поиск серийных номеров и регистрационных ключей

С помощью этой функции вы можете легко восстановить забытый лицензионный ключ или серийный номер, даже если операционная система не загружается или если вы не имеете доступ к вашей учетной записи на этом ПК.

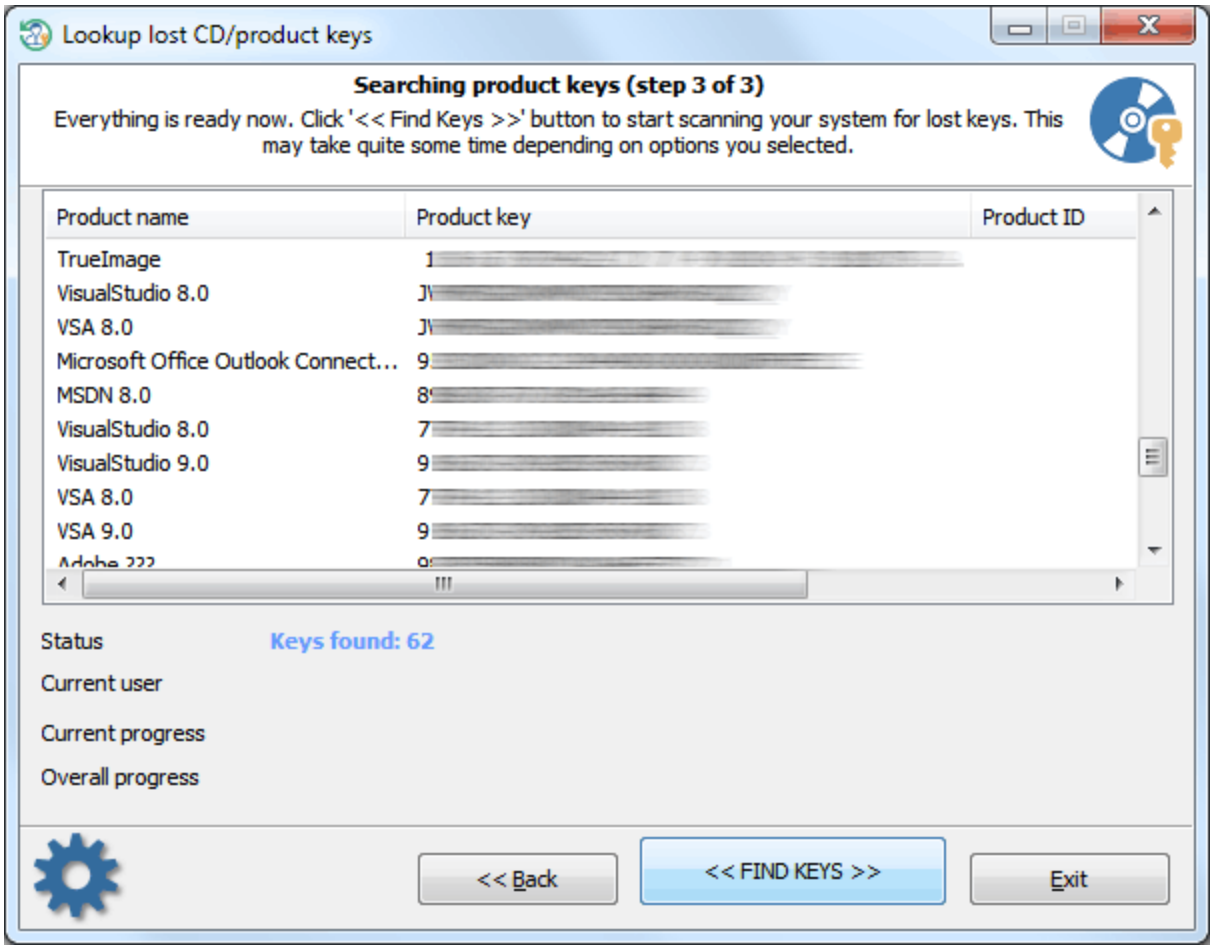
Почти все коммерческое ПО поставляется с серийным кодом (лицензионным ключом), который привязывает программу к компьютеру и делает программного обеспечение полнофункциональным. Потеряв лицензионный ключ после переустановки программного обеспечения, вы не получите доступ ко всем функциям программы до тех пор, пока не введете этот ключ снова. Представьте, что в один прекрасный день вам потребовалось выполнить переустановку операционной системы. Этому может предшествовать множество причин, от обновления системы до удаления вирусов, исправления проблем в работе ОС и т.д. После переустановки ОС может потребоваться и переустановка остального программного обеспечения и регистрация его заново. Однако без регистрационного ключа вы не сможете это сделать.

К счастью, большинство программ хранят свои серийные номера в реестре Windows, и поэтому они легко могут быть извлечены. Для это и предназначена данная функция программы. При помощи встроенного скриптового языка, Reset Windows Password может восстановить забытые лицензионные ключи к более чем 1000 программным продуктам. Кроме того, это очень просто даже для неподготовленного пользователя.



Сначала необходимо указать, хотите ли вы выполнить поиск ключей для всех локальных пользователей системы или только для одной выбранной учетной записи. Расшифровка ключей всех учетных записей потребует правильного указания двух обязательных параметров:
1. Файл реестра SOFTWARE, который расположен в каталоге 'C:\Windows\System32\Config'. Учтите, буква целевого диска, а также Windows каталог могут быть другими. Например, 'D:\Windows', 'E:\Win' и т.д.
2. Папка с профилями пользователей. Это каталог, в котором физически расположены профили локальных учетных записей. Для операционных систем Windows Vista и выше, она обычно называется 'C:\Users'. Тогда как Windows XP использует каталог 'C:\Documents and Settings'. Как правило, папка с профилями находится на том же диске, что и каталог Windows, хотя и необязательно.

Программа постарается определить указанные каталоги самостоятельно. Все что вам потребуется, это выбрать предложенный каталог из списка или, в противном случае, указать его самостоятельно. Если требуется осуществить поиск серийных номеров определенного пользователя, просто установите соответствующую опцию и дополнительно выберите имя учетной записи из предложенного списка.



После того, как заданы все необходимые настройки, перейдите к финальному диалогу в котором нажмите кнопку '<< Искать Ключи >>' для запуска процесса поиска ключей.

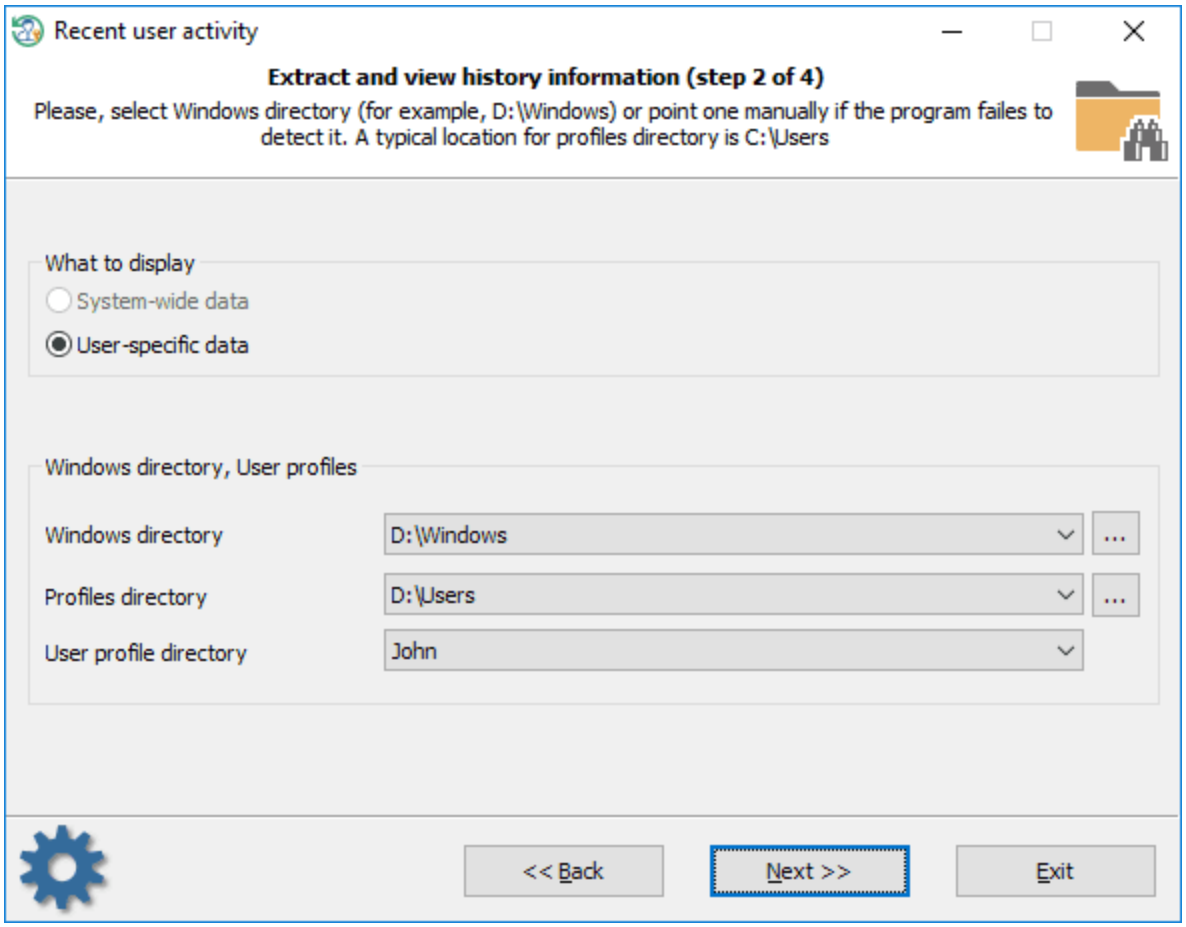
Поиск и восстановление серийных номеров может занять некоторое время в зависимости от выбранных настроек.

3.6 Активность пользователя

3.6.1 Последняя активность пользователя

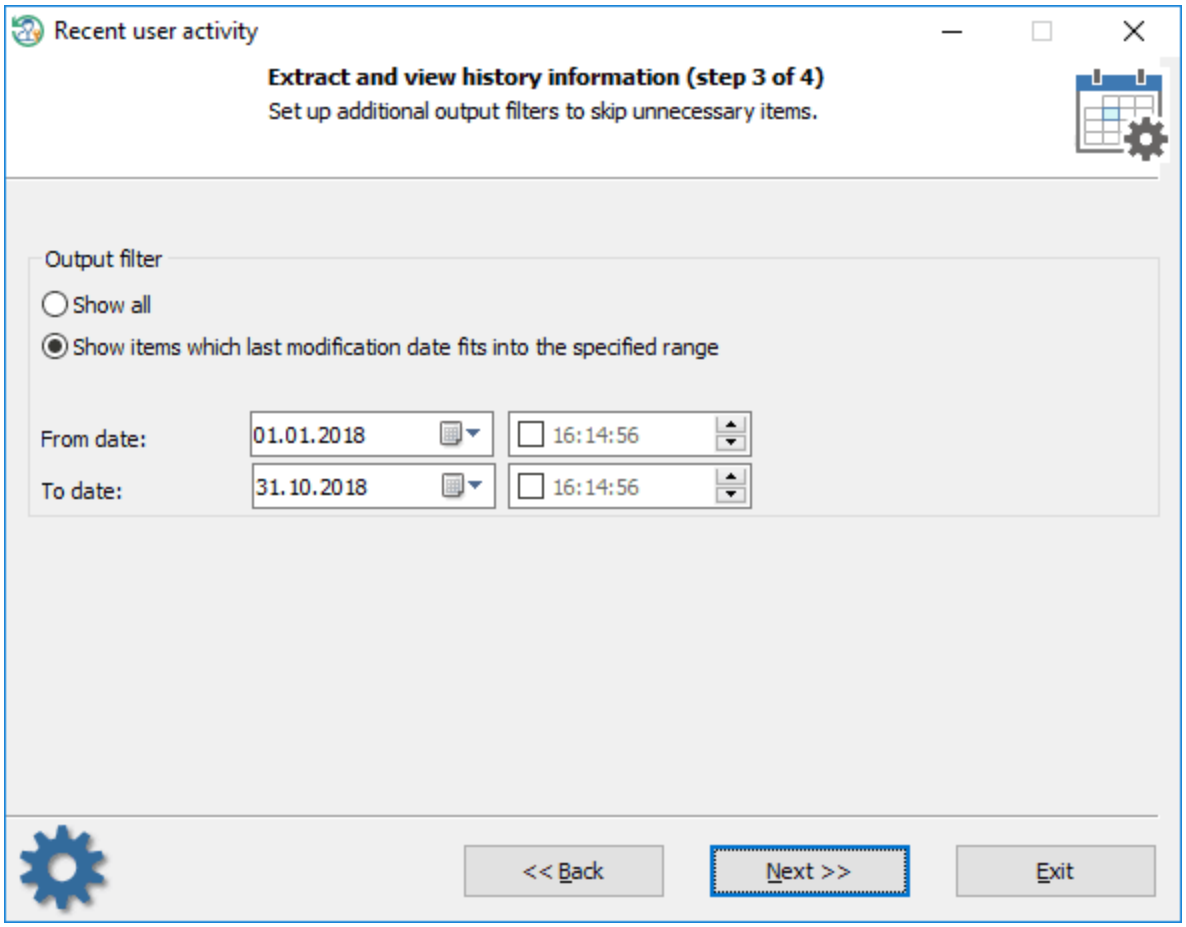
Эта утилита собирает всю доступную информацию о последних действиях пользователя на этом компьютере.

Выбор типа информации



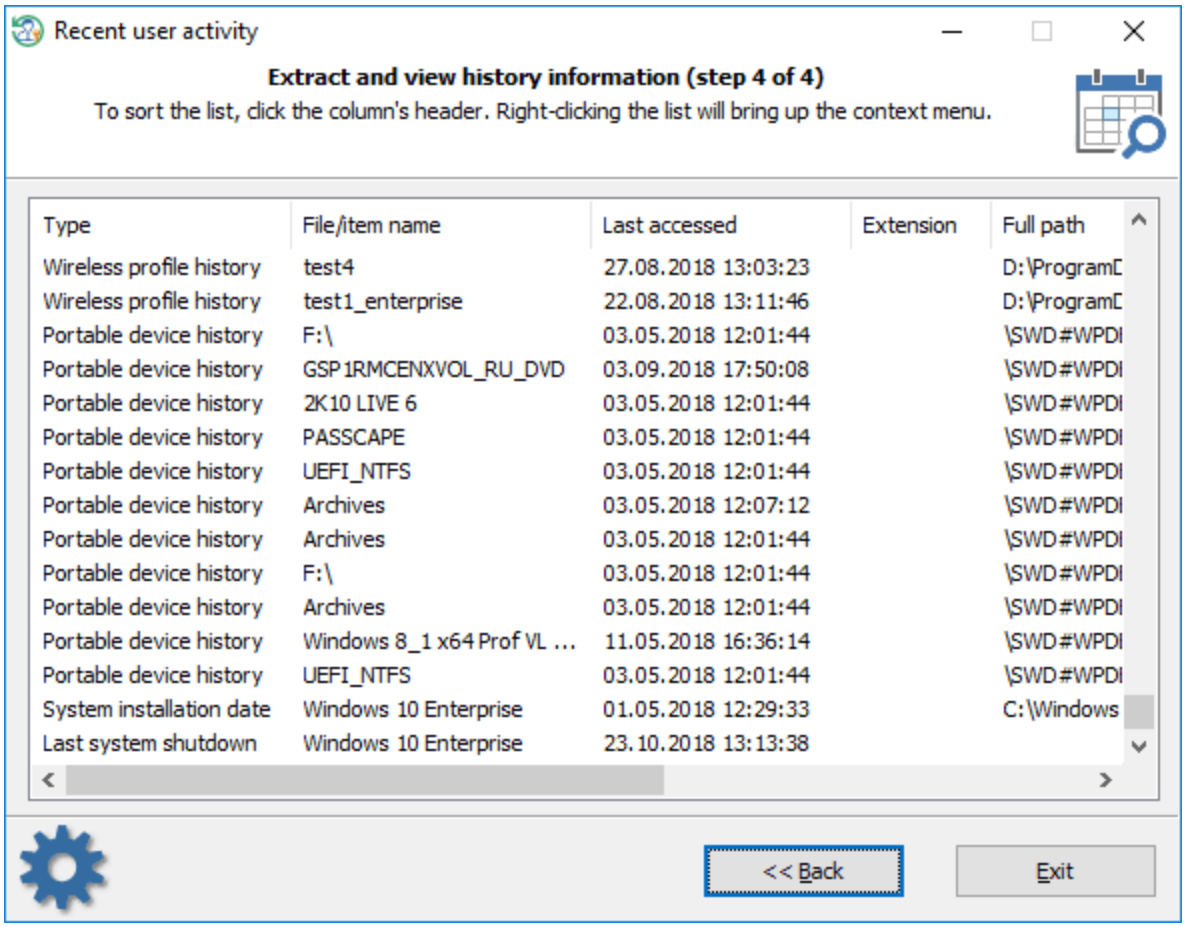
Прежде всего, выберите, хотите ли вы просматривать общесистемные или пользовательские данные.

Установка фильтров отображения



Затем укажите, должны ли отображаться все записи или только те, которые вписываются в определенные временные рамки.

Последняя активность пользователя



Будьте терпеливы, сбор статистики может занять некоторое время.
Чтобы скрыть ненужные записи, щелкните правой кнопкой мыши на списке и выберите соответствующий пункт меню.

Текущая версия программы поддерживает следующую информацию (некоторые элементы недоступны в старых ОС):

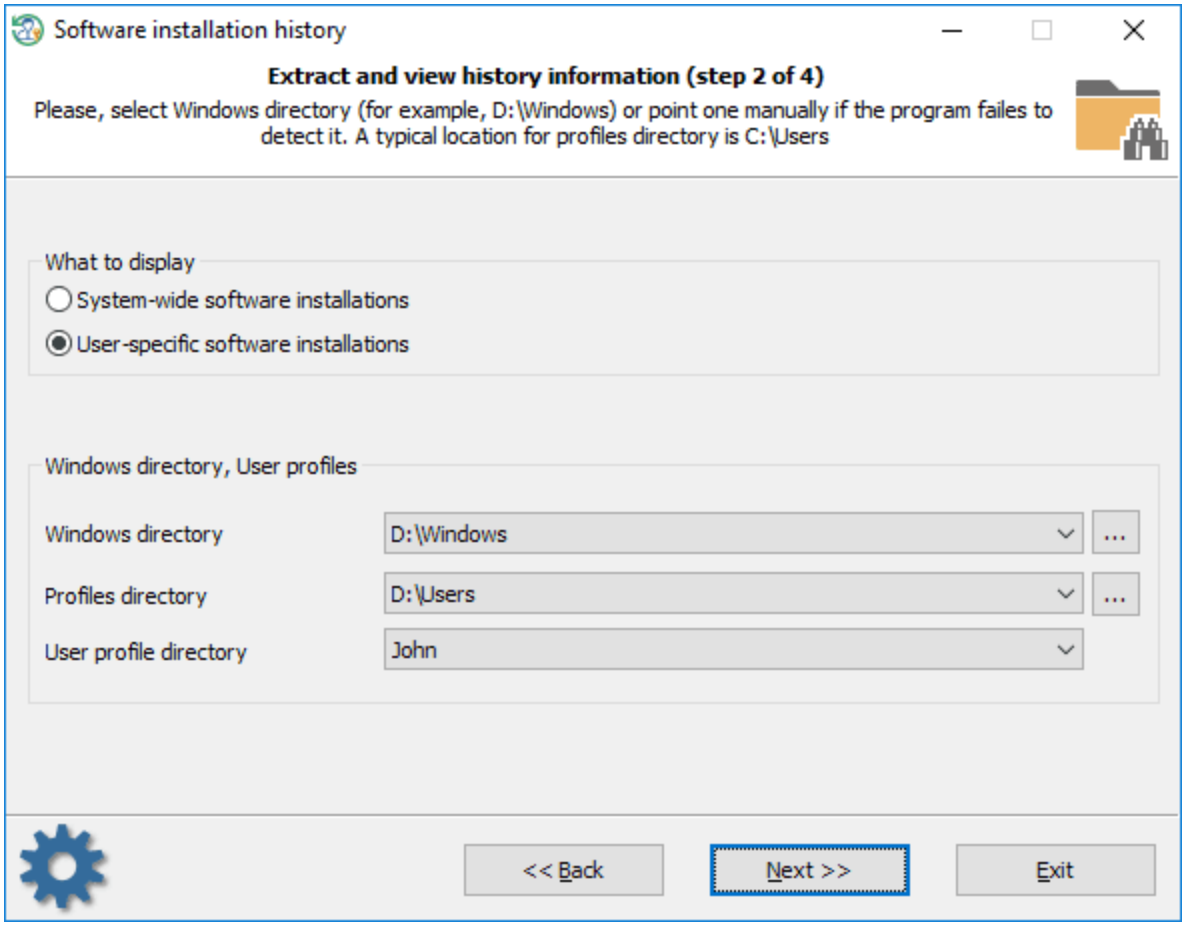
- Последние файлы в диалогах открытия/сохранения
- История запуска задач
- История подключений сетевых дисков
- Последние сетевые элементы поиска
- Недавние элементы поиска файлов и папок
- Последние редактируемые документы апплетов Windows
- Последний открываемый ключ Regedit
- Последние открываемые документы
- Последние открываемые документы MS Office
- Последние учетные записи и соединения Outlook
- Недавно запущенные приложения
- Последние элементы запущенных приложений
- Последние соединения удаленного рабочего стола
- Введенные адреса Internet Explorer
- Введенные пути в Explorer
- История поиска Explorer
- Элементы помощника Explorer
- Последние элементы фоновой активности

- Последние элементы активности рабочего стола
- Беспроводные соединения
- Активность устройств Bluetooth
- История портативных устройств
- Дата установки Windows
- Дата последнего выключения системы

3.6.2 Статистика учетных записей

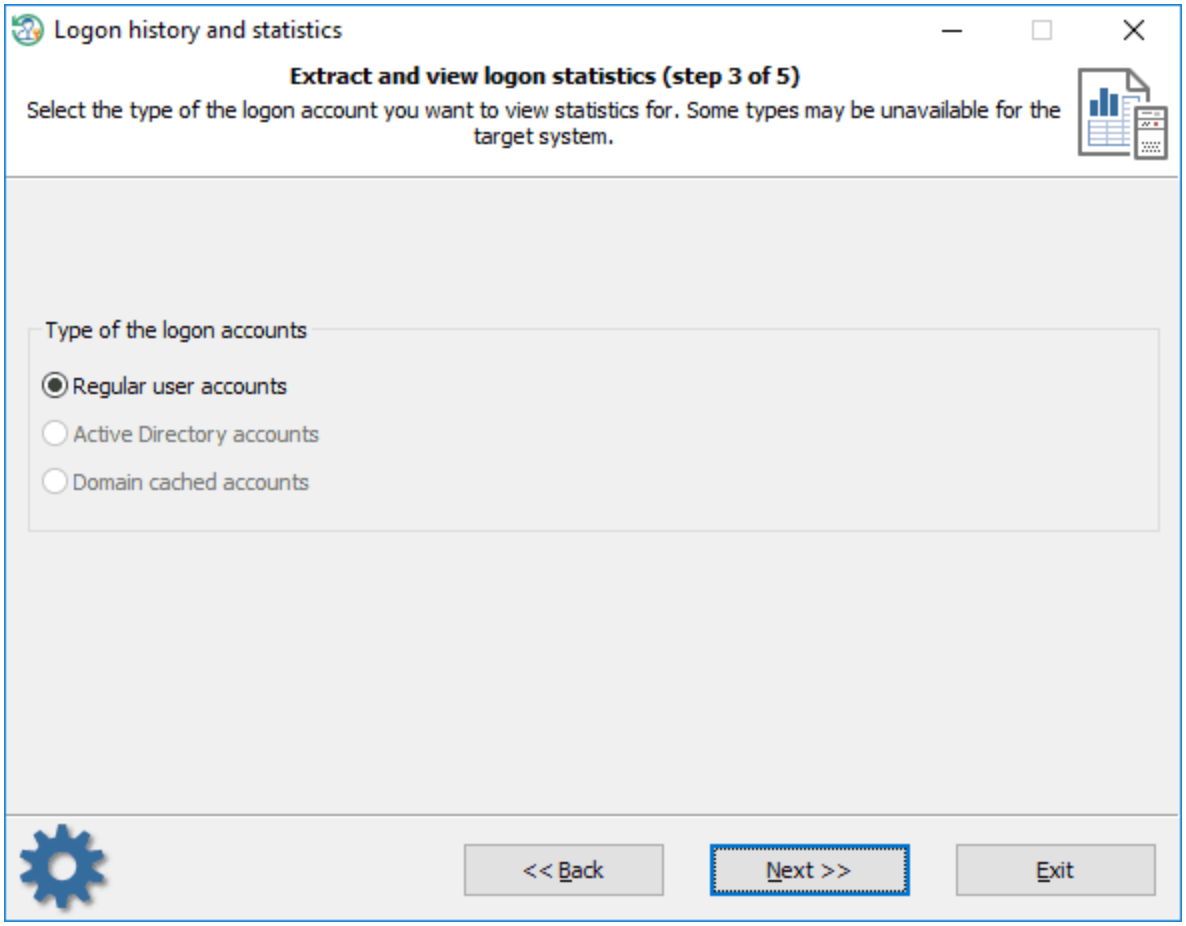
Этот инструмент предназначен для просмотра различной статистики как обычных, так и доменных пользователей.

Выбор типа установки



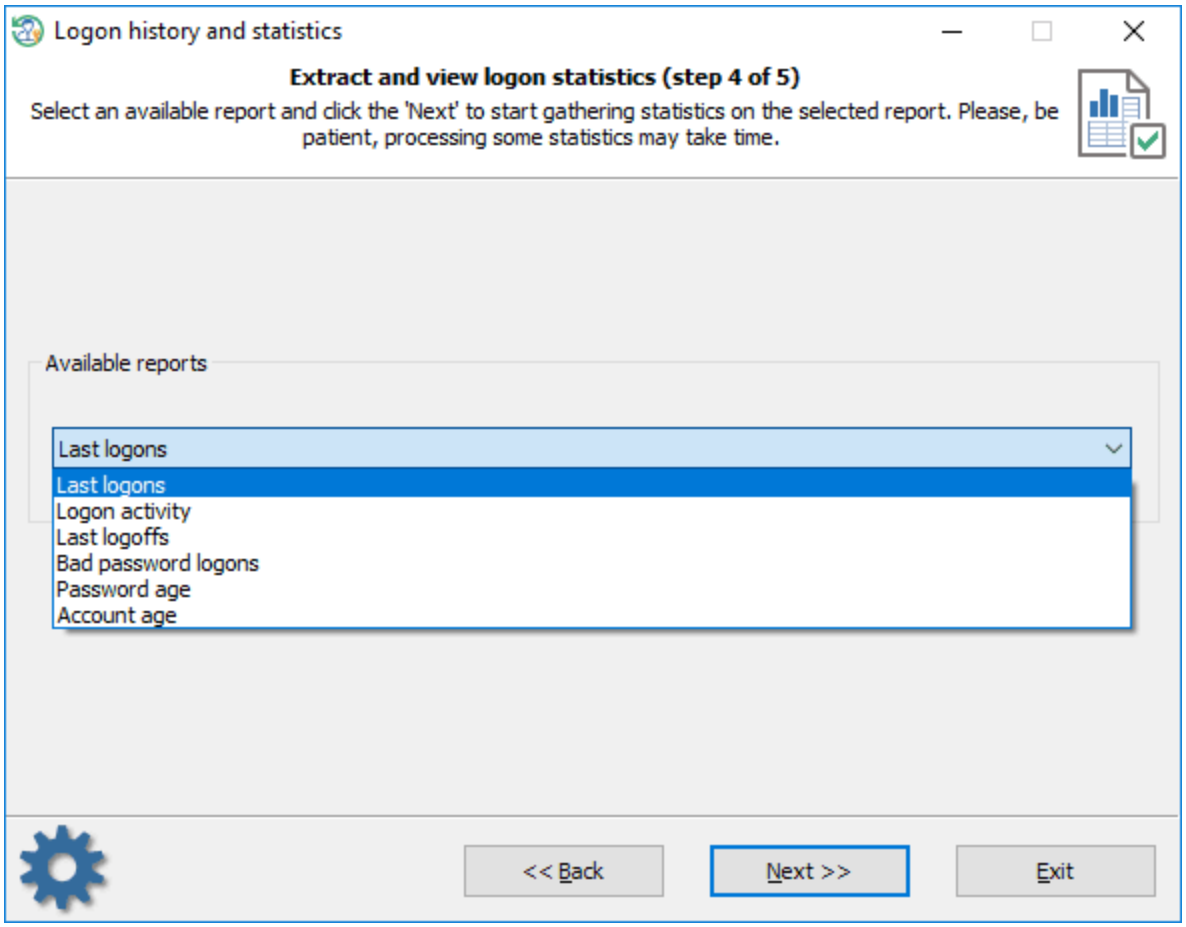
Выберите тип установки ПО для просмотра. Это может быть либо установки пользователя (программы, установленные для определенной учетной записи), либо системные установки (программы, доступные всем пользователям).

Тип учетных записей



После того, как каталог Windows выбран, программа попытается определить, содержит ли система какие-либо учетные записи домена (в дополнение к обычным). Выберите тип учетных записей, который вас интересует, и перейдите к следующему шагу.

Выбор отчета

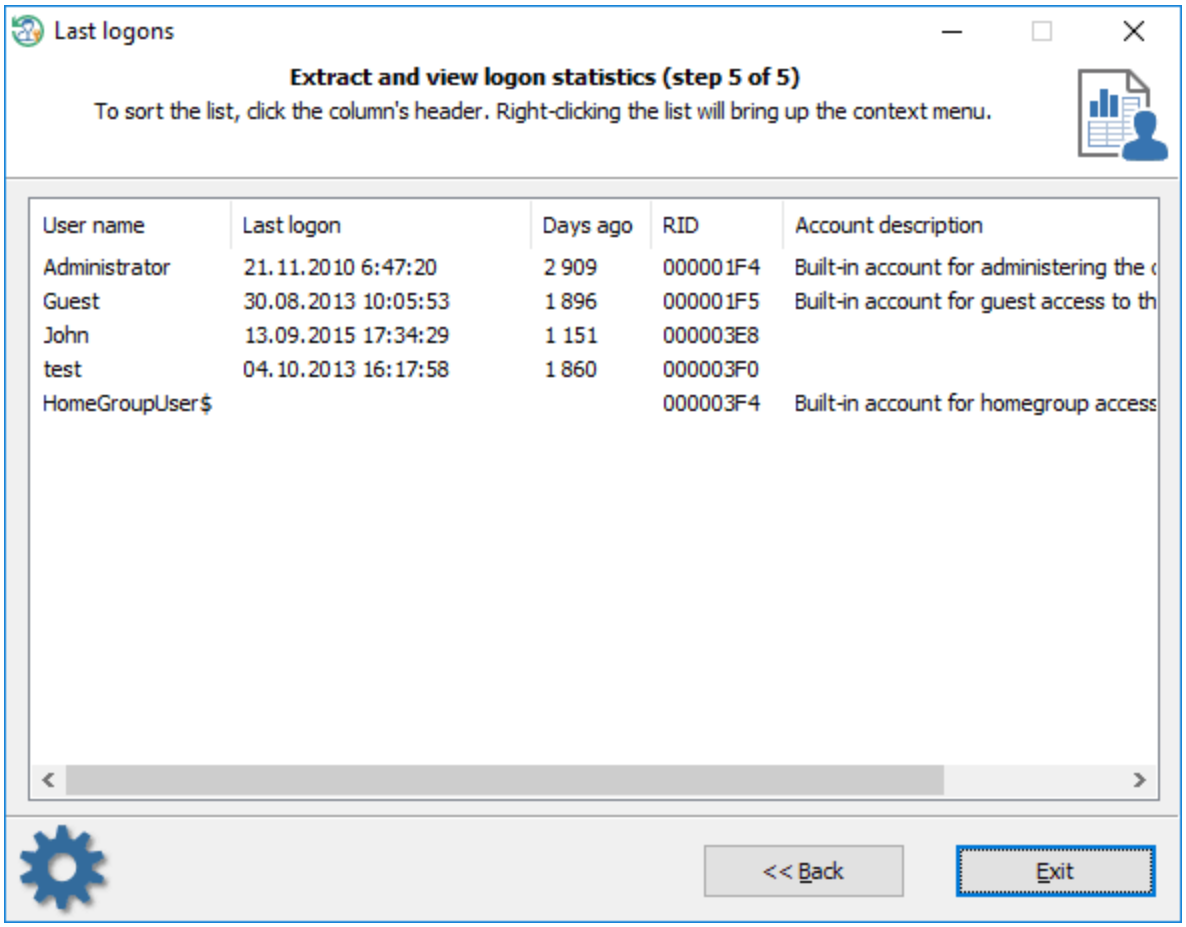


На этом этапе необходимо выбрать один из доступных отчетов:

- Last logons - отображает дату последнего входа пользователей
- Logon activity - показывает наиболее активных пользователей
- Last logoffs - к сожалению, большинство версий Windows перестало сохранять журнал даты выхода. Однако некоторые связанные сведения можно найти в разделе 'Последняя активность пользователя'.
- Bad password logons - последний раз, когда пользователь пытался войти в свой аккаунт с неверным паролем.
- Password age - последний раз, когда пользователь менял свой пароль.
- Account age - когда была создана учетная запись.

Некоторые отчеты недоступны для кэшированных учетных записей домена.

Статистика учетных записей

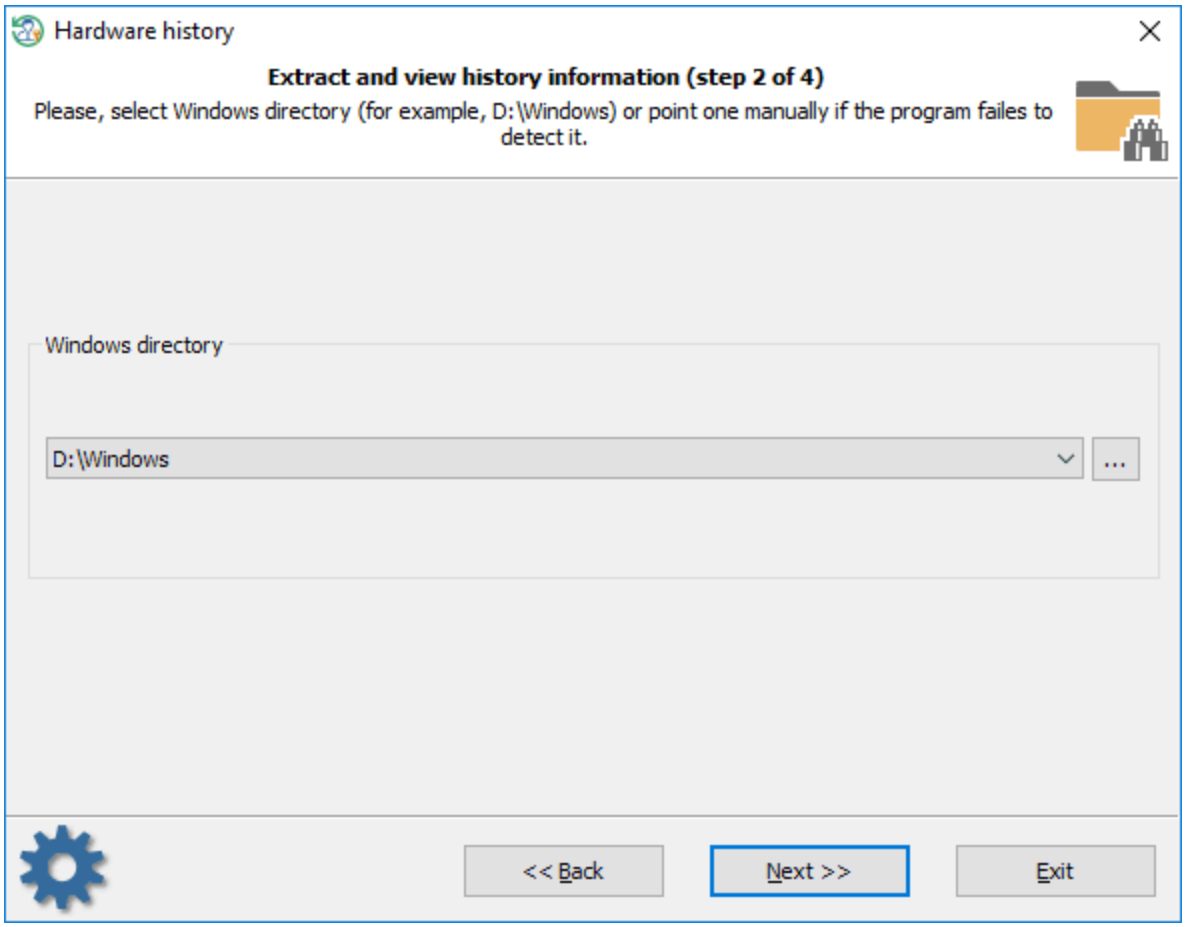


Статистику можно скопировать в буфер обмена или сохранить в файл.

3.6.3 История оборудования

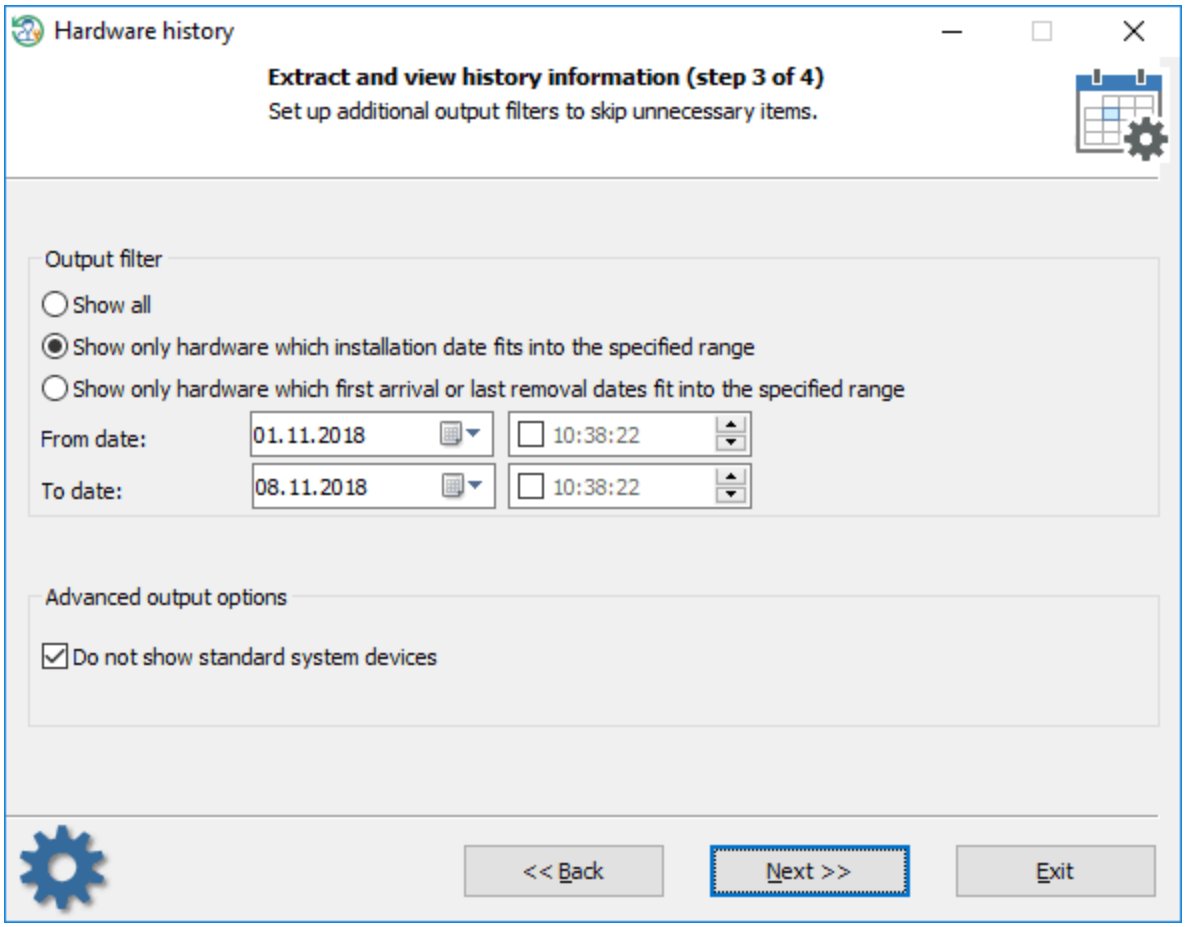
Статистика оборудования производит поиск установленного железа на целевой ОС и сортирует его по дате установки или последнего использования.

Выбор каталога Windows



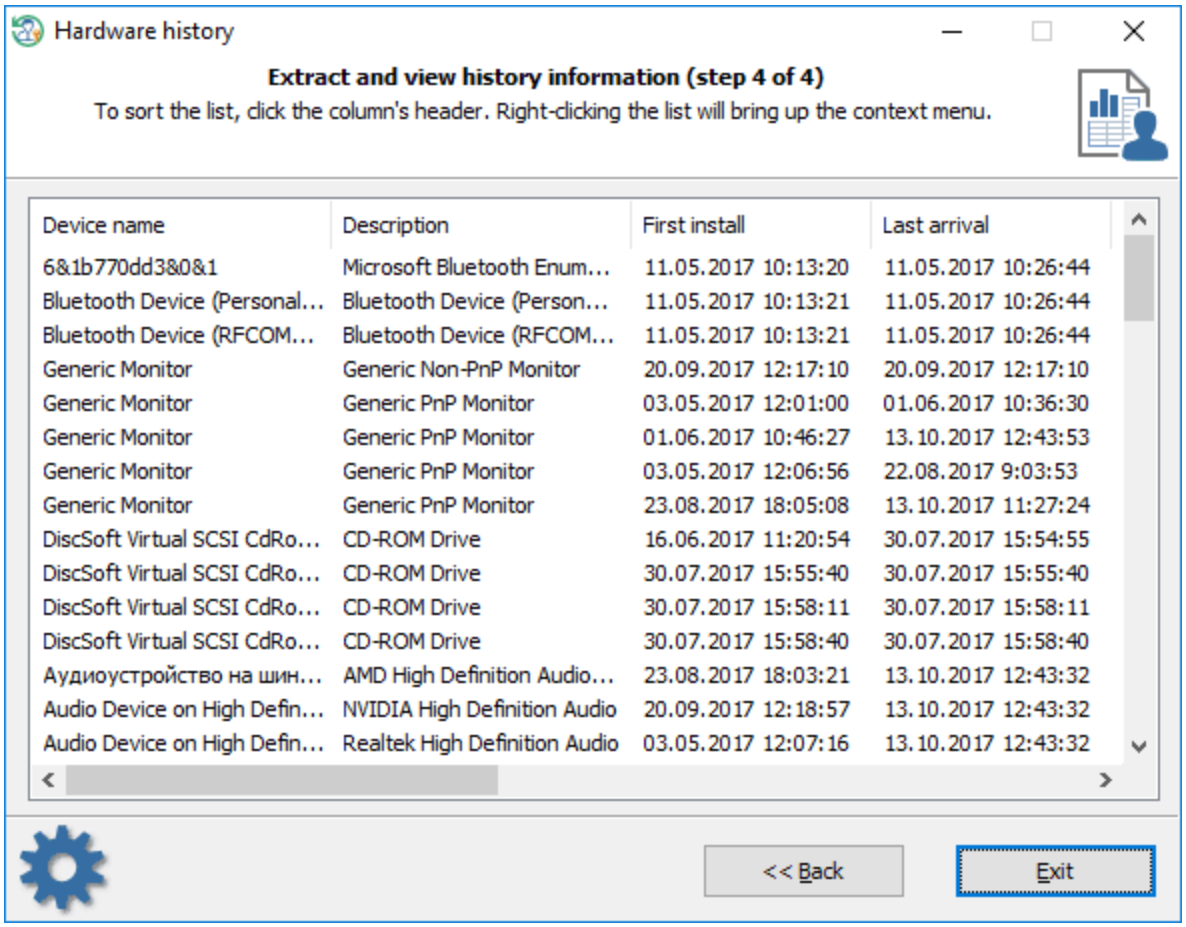
Сначала выберите целевую папку Windows. Программа обычно делает это автоматически.

Установка фильтров отображения



Настройте дополнительные фильтры вывода, чтобы пропустить ненужные элементы. Можно настроить программу так, чтобы отображалось только оборудование, которое было установлено или было видимо последний раз за указанную дату.

История железа

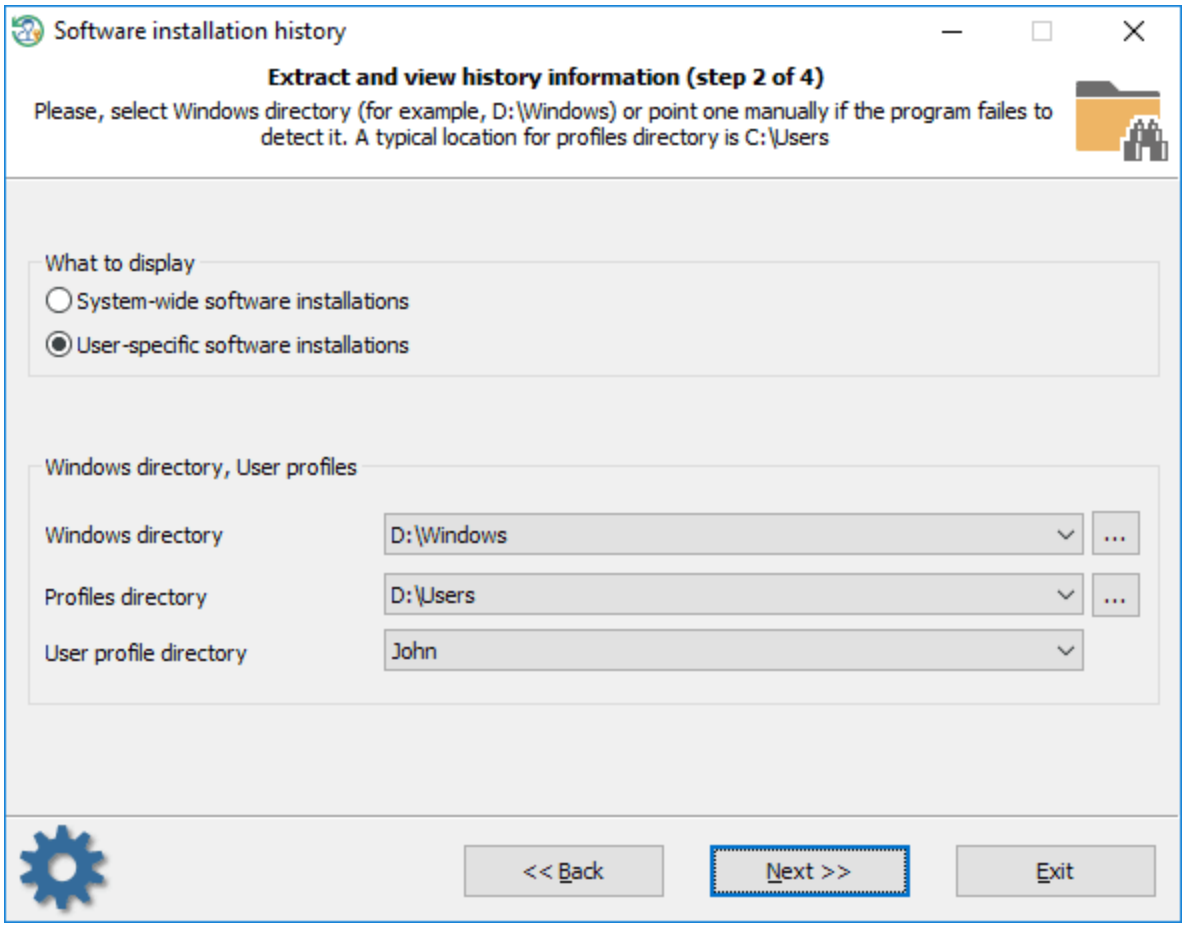


Чтобы отсортировать список, щелкните один из столбцов.

3.6.4 История установок ПО

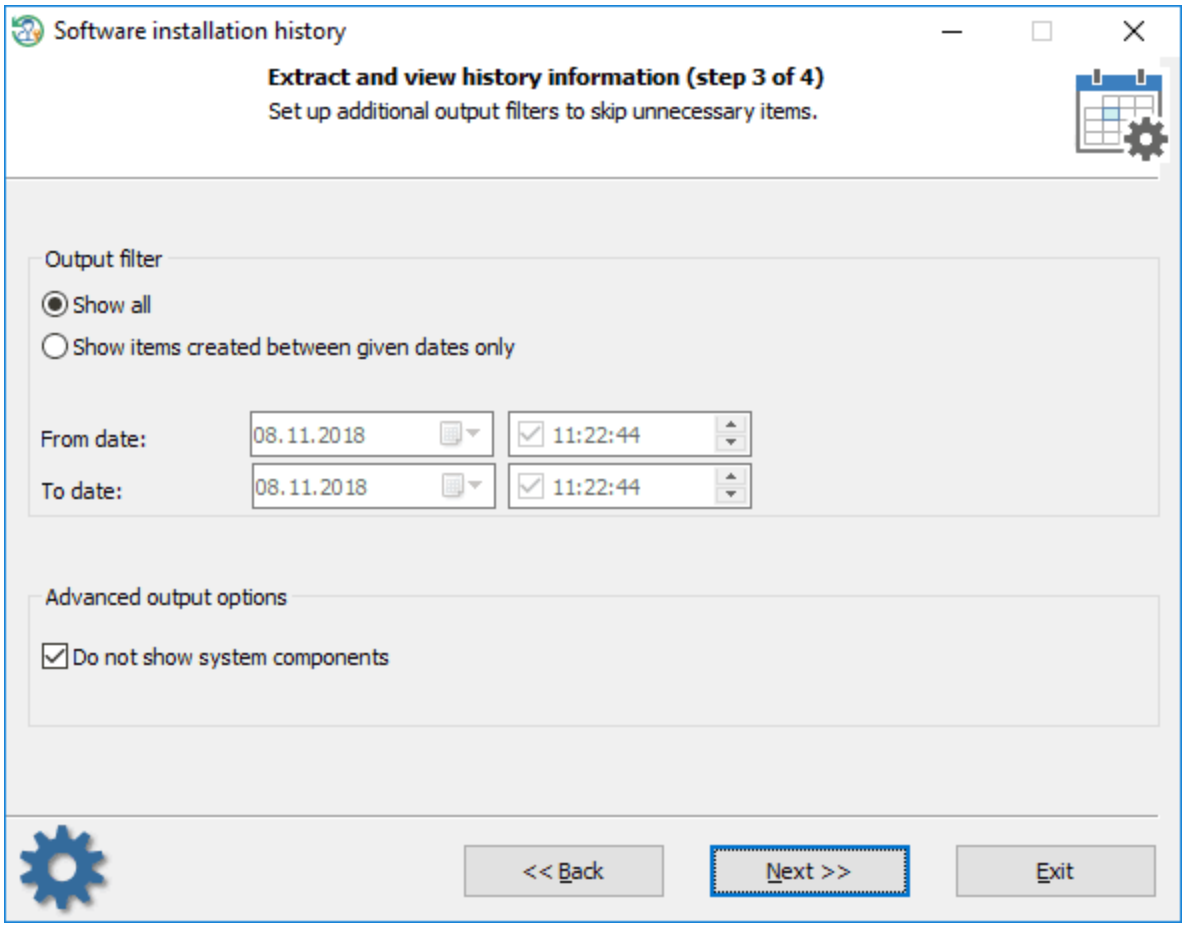
История установков ПО отображает программы, которые были установленные на целевой системе.

Выбор типа установки



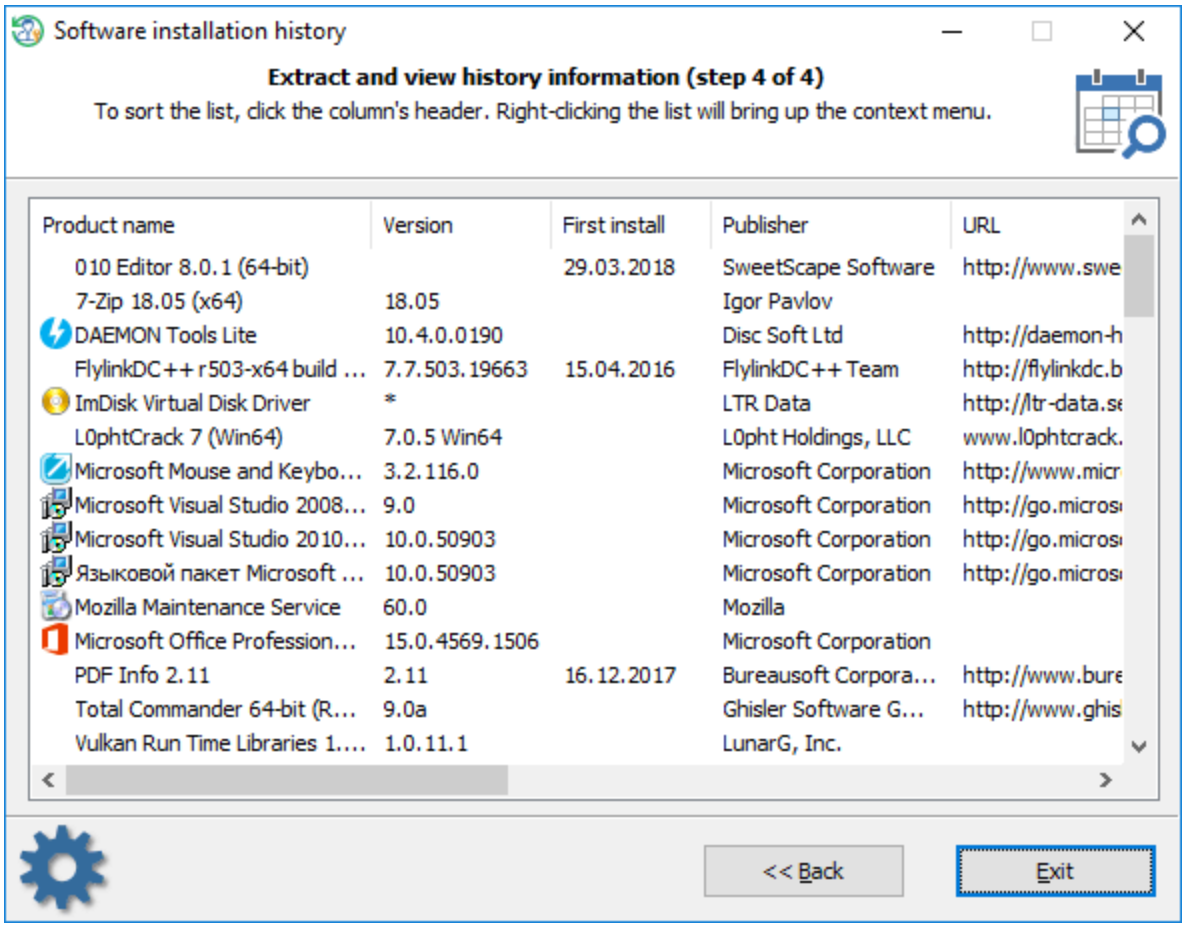
Выберите тип установки ПО для просмотра. Это может быть либо установки пользователя (программы, установленные для определенной учетной записи), либо системные установки (программы, доступные всем пользователям).

Установка фильтров отображения



Можно указать программе отображать все элементы или элементы, созданные только в определенныый промежуток времени. Дополнительная опция призвана скрыть некоторые системные компоненты, такие как обновления ОС и т. д.

История установок ПО

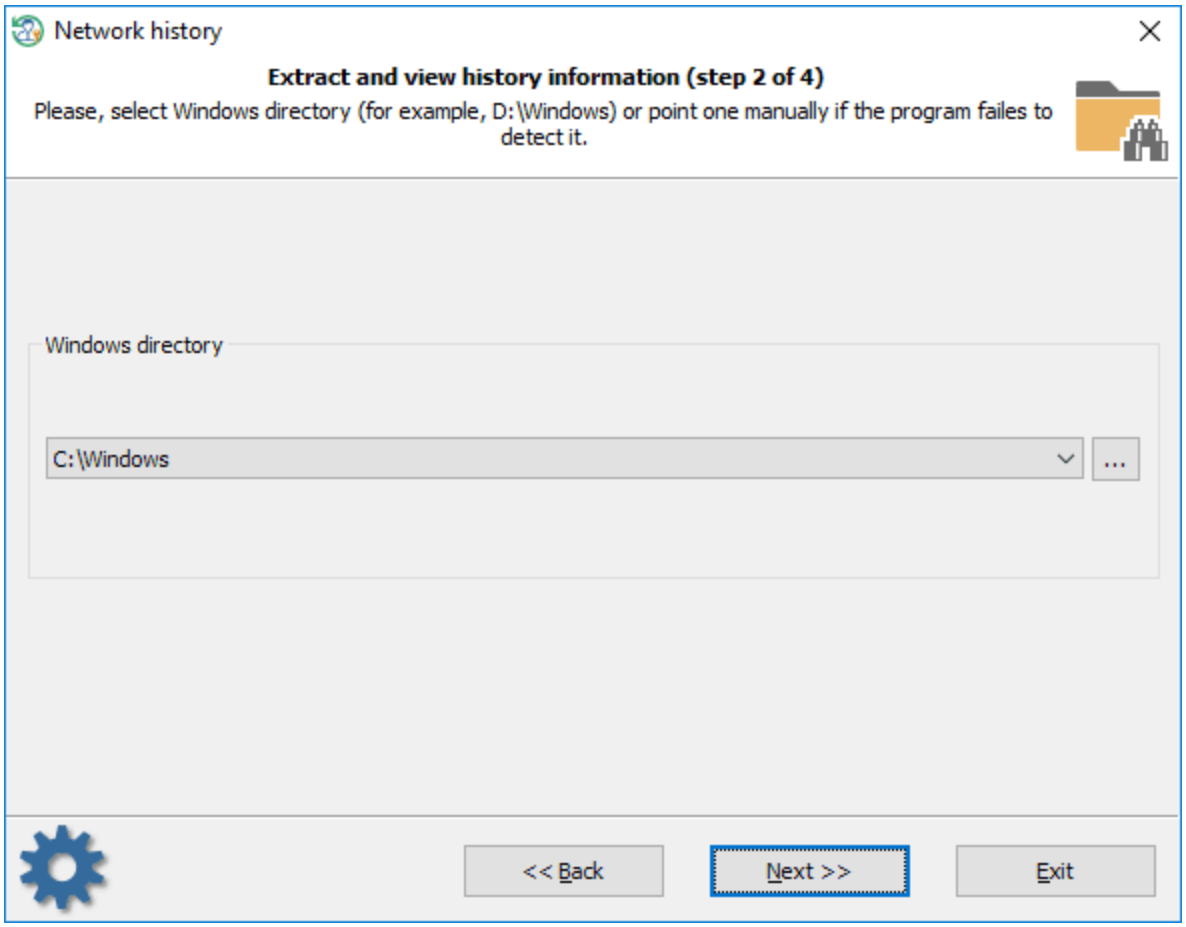


Чтобы отсортировать список, щелкните один из столбцов.

3.6.5 История сетевых соединений

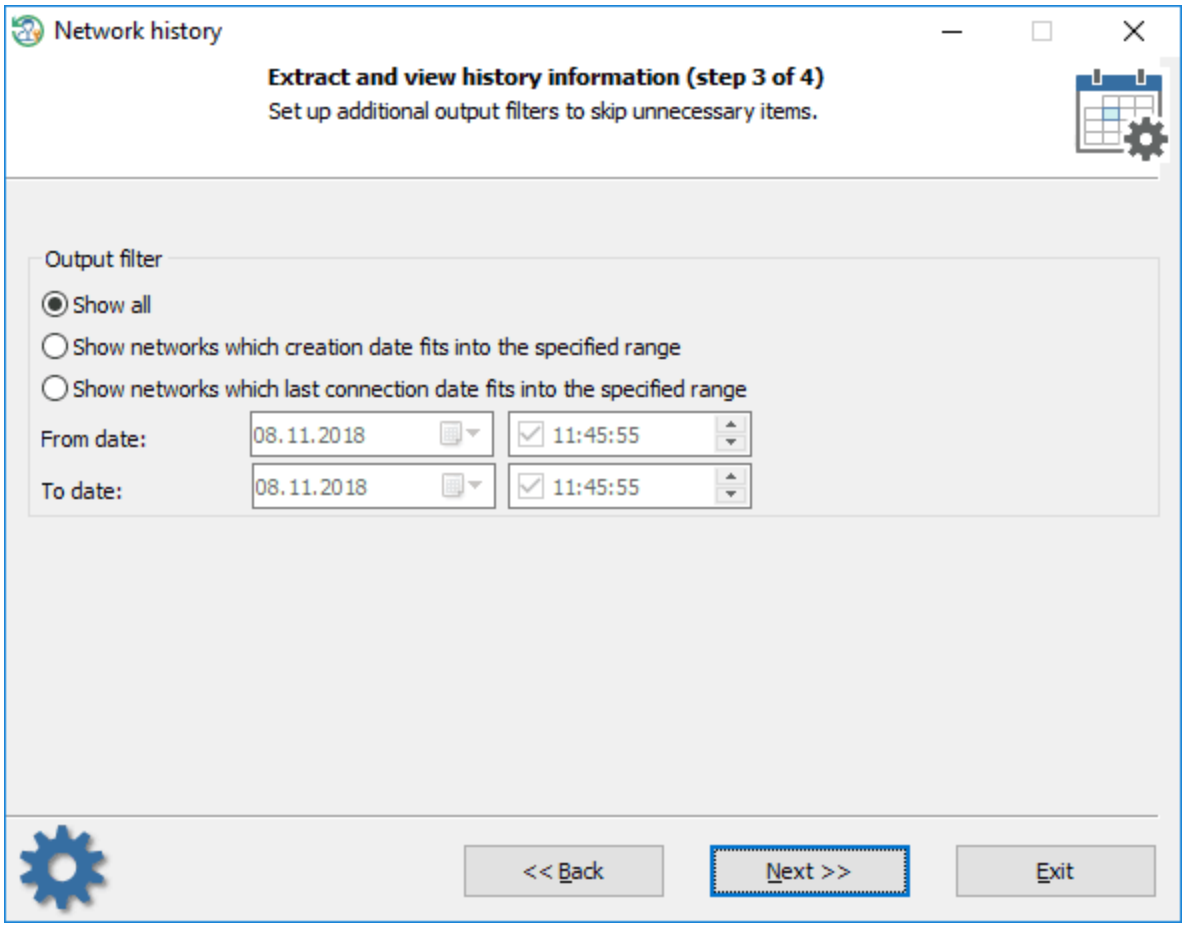
История сетевых соединений показывает все доступные сети, а также дату их установки и последнего подключения к ним.

Выбор каталога Windows



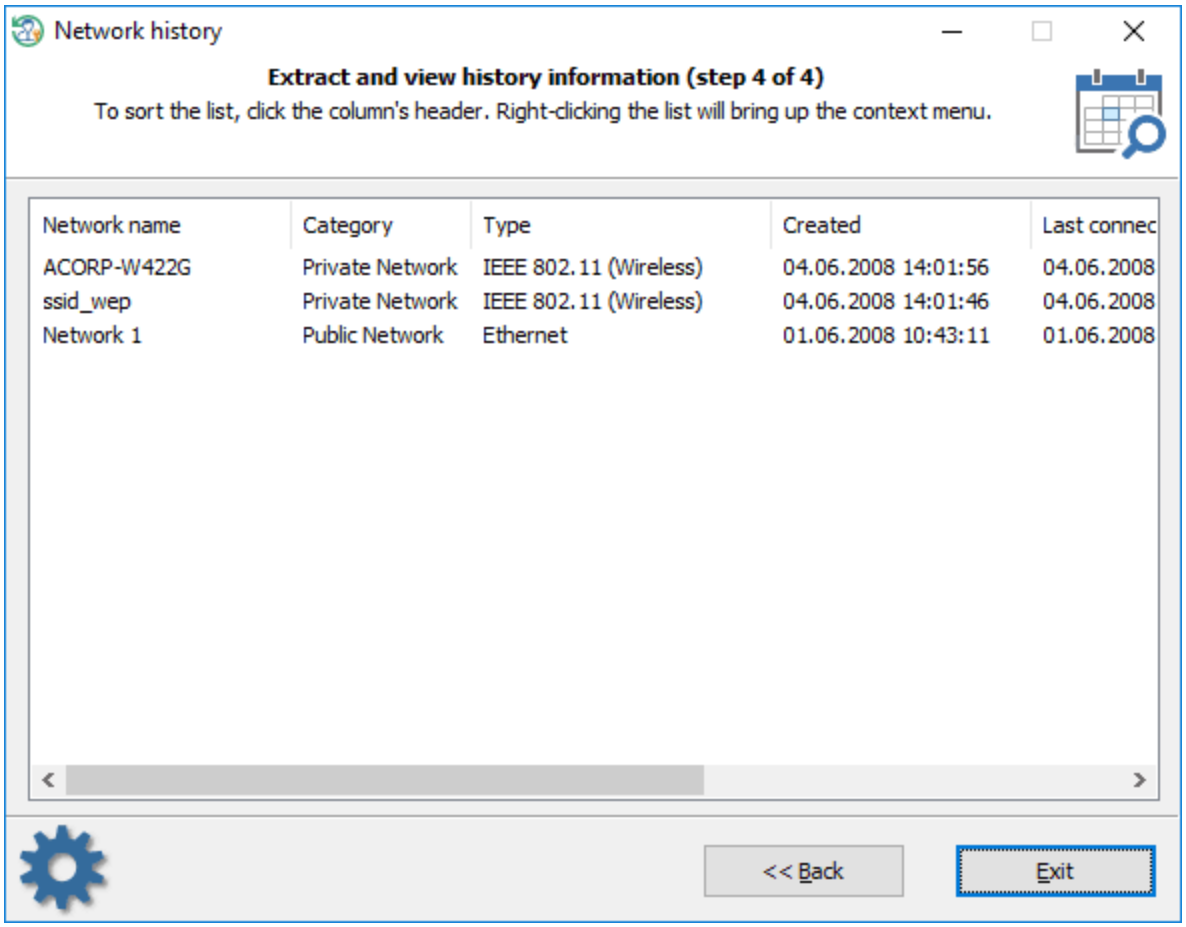
Сначала выберите целевую папку Windows. Программа обычно делает это за вас.

Установка фильтров отображения



Настройте дополнительные фильтры вывода для отображения только интересующих вас сетей.

История сетевых соединений



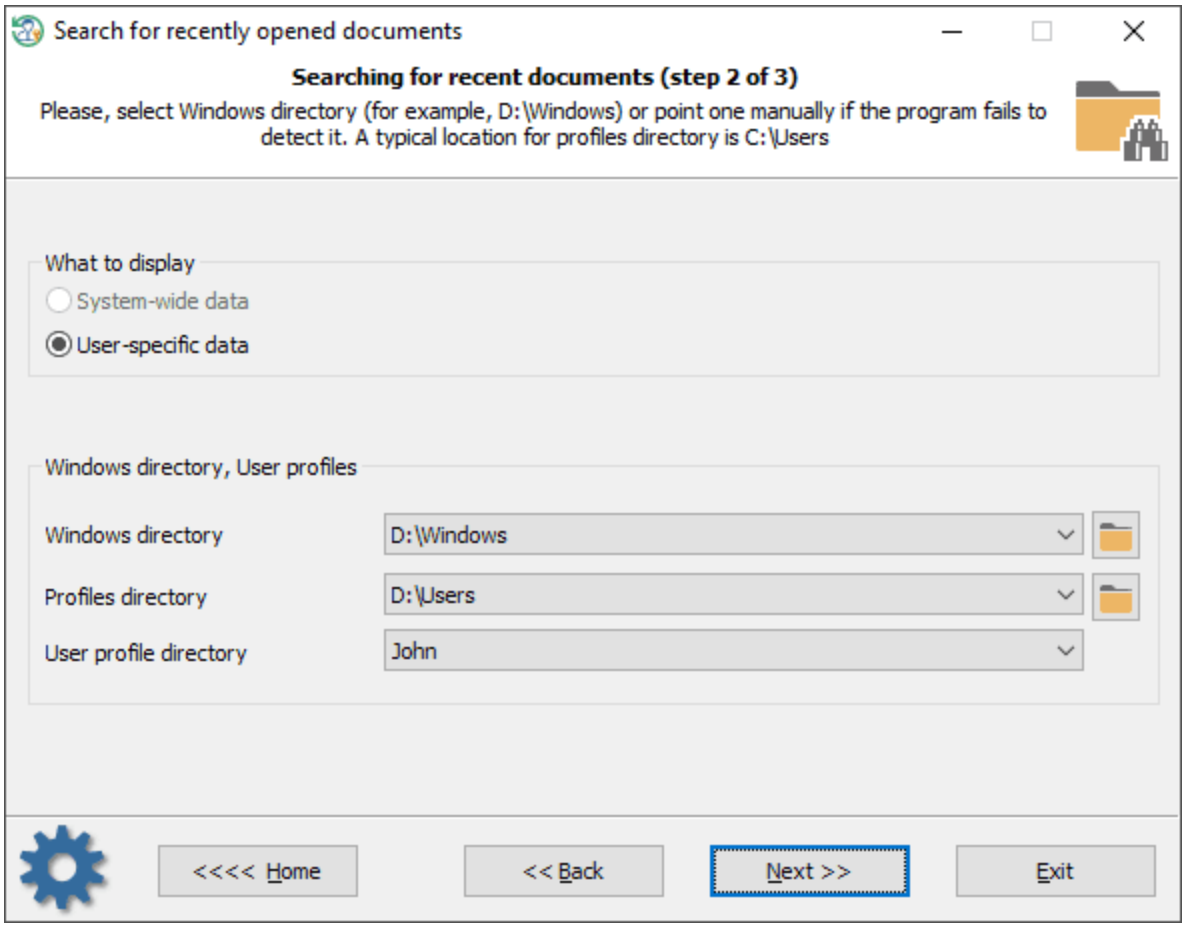
Сети обычно содержат дату их создания и дату последнего подключения. Для сортировки списка по датам, щелкните один из соответствующих столбцов.

3.6.6 Поиск последних открываемых документов

ОС Windows отслеживает все открытываемые пользователем документы, сохраняя ссылки на них в специальную папку Microsoft, которая находится в профиле пользователя и называется 'Recent'.
'C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent' - это специальная папка, в которой Windows хранит ссылки на недавно использованные документы.
Вы можете управлять поведением Windows из меню Пуск > Настройки > Персонализация > Пуск, переключив опцию '*Сохранять и показать последние открытые программы*'.

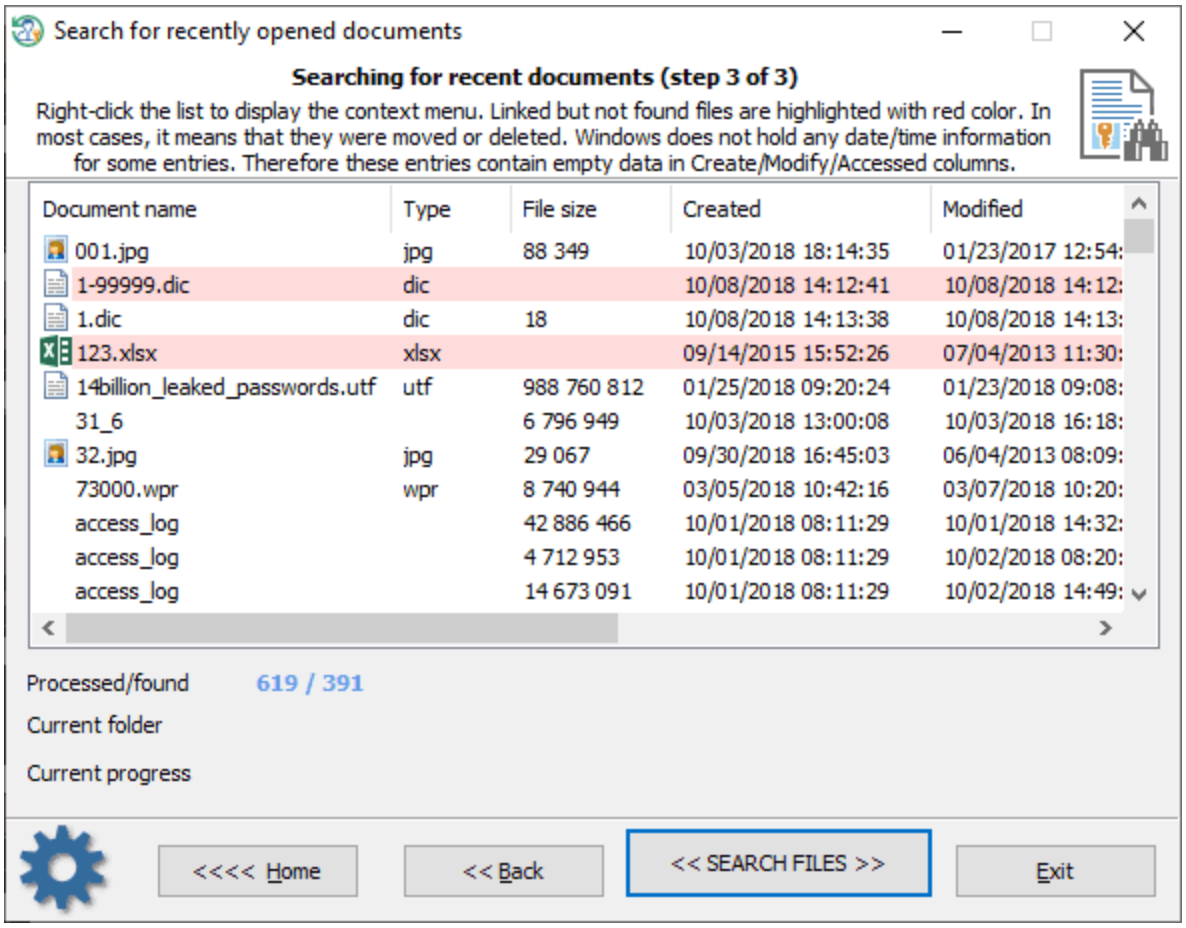
Эта функция программы предназначена для просмотра списка документов и файлов, которые были недавно открыты и сохранены в Windows папке 'Recent'.

Выбор пользователя



Выбираем профиль пользователя, список последних документов которого надо открыть.

Список последних открываемых пользователем документов



Нажимаем кнопку << *ПОИСК ФАЙЛОВ* >> и терпеливо ждем пока программа не найдет последние открываемые файлы и не заполнит ими таблицу.

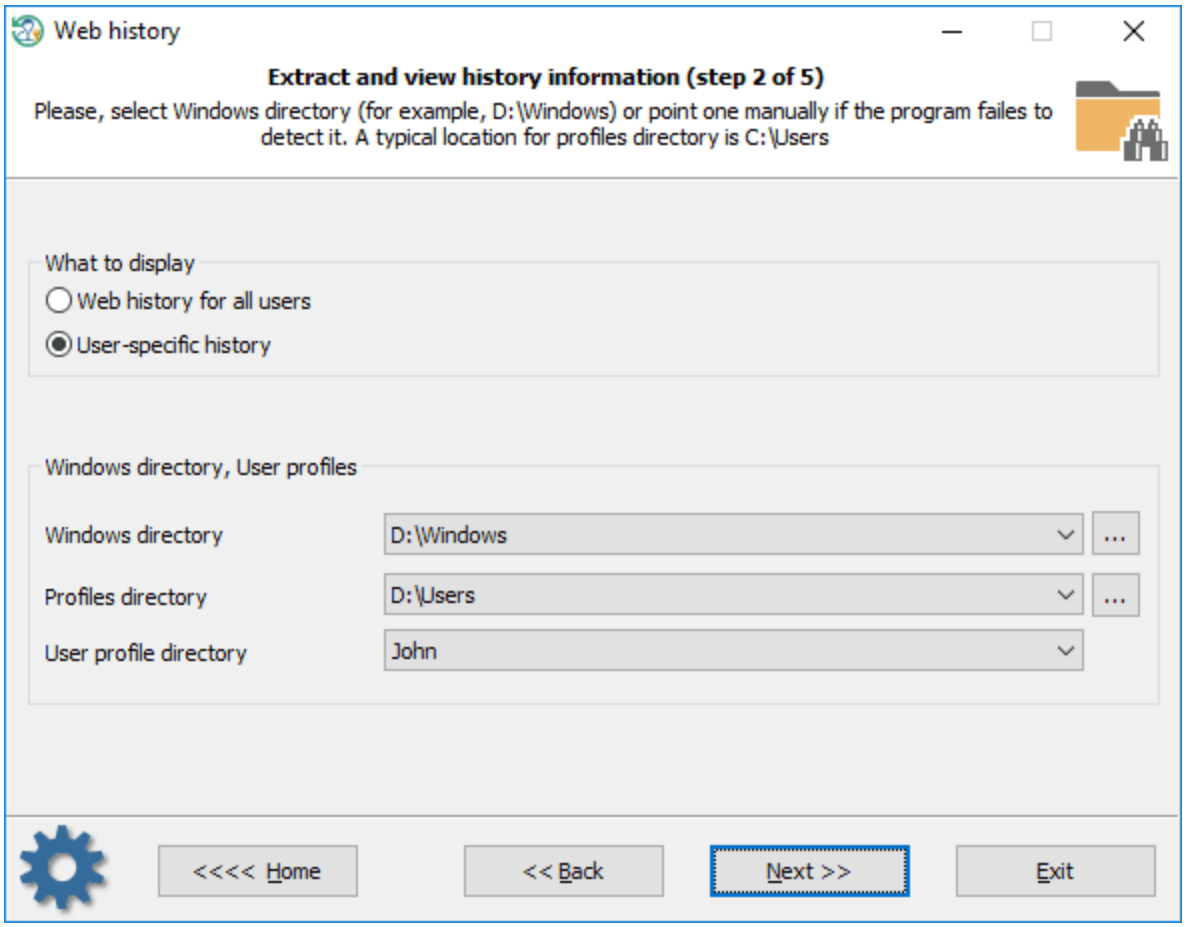
Для того чтобы скрыть ненужные записи, щелкните правой кнопкой мыши на списке и выберите соответствующий пункт меню.

Красным цветом выделены файлы, ссылки на которые остались, но сами они были удалены или перемещены.

3.6.7 Интернет активность пользователя

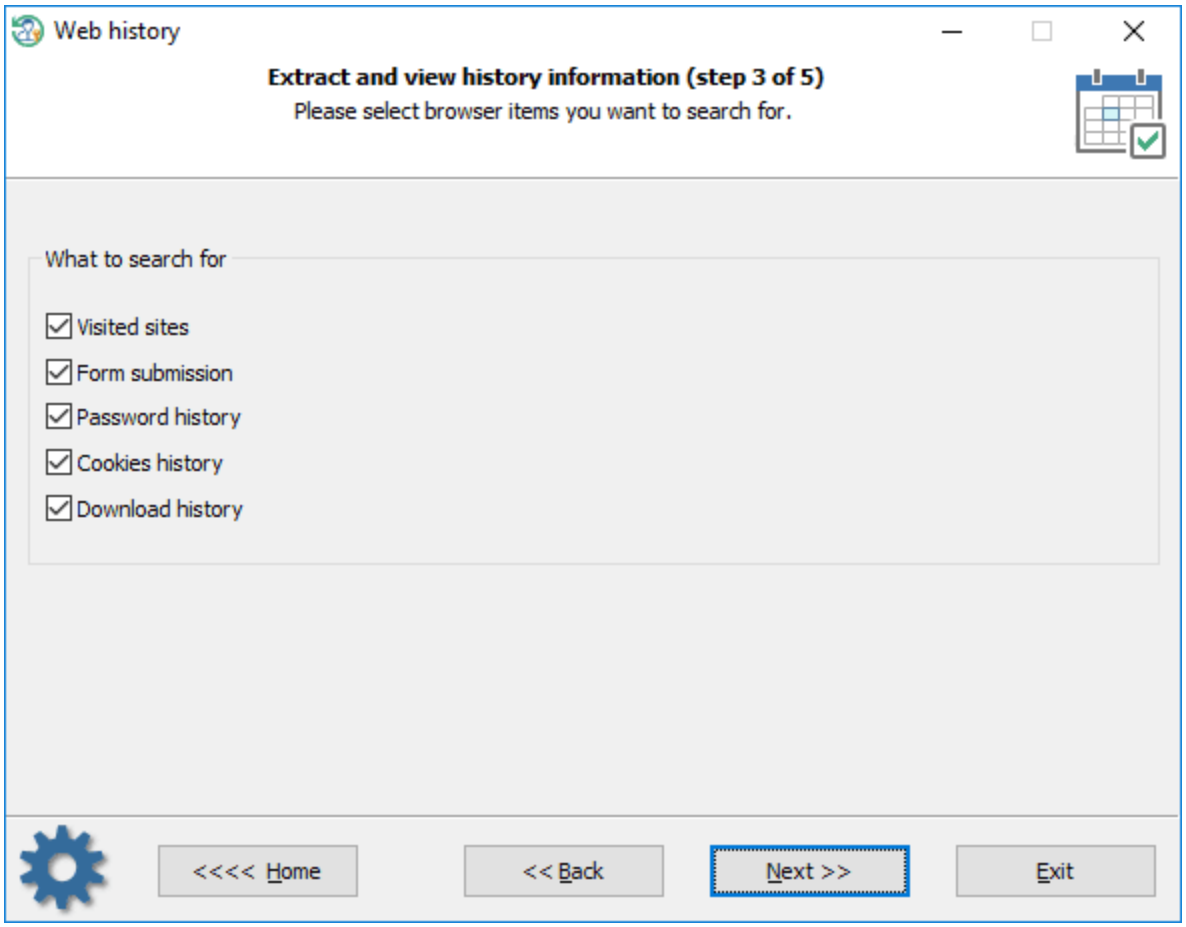
История Интернет обозревателей позволяет собирать статистику посещенных Web страниц, сохраненных кукисов, сохраненных полей автозаполения и паролей. Поддерживаются браузеры Internet Explorer 4-11, Edge, Opera, браузеры на базе Mozilla (Firefox, SeaMonkey и т.д.), Chromium (Google Chrome, YandexBrowser, 360 Extreme Explorer и т.д.)

Выбор источника информации



На начальном этапе программа предлагает выбрать источник инормации для поиска: профиль конкретного пользователя или профили всех пользователей системы.

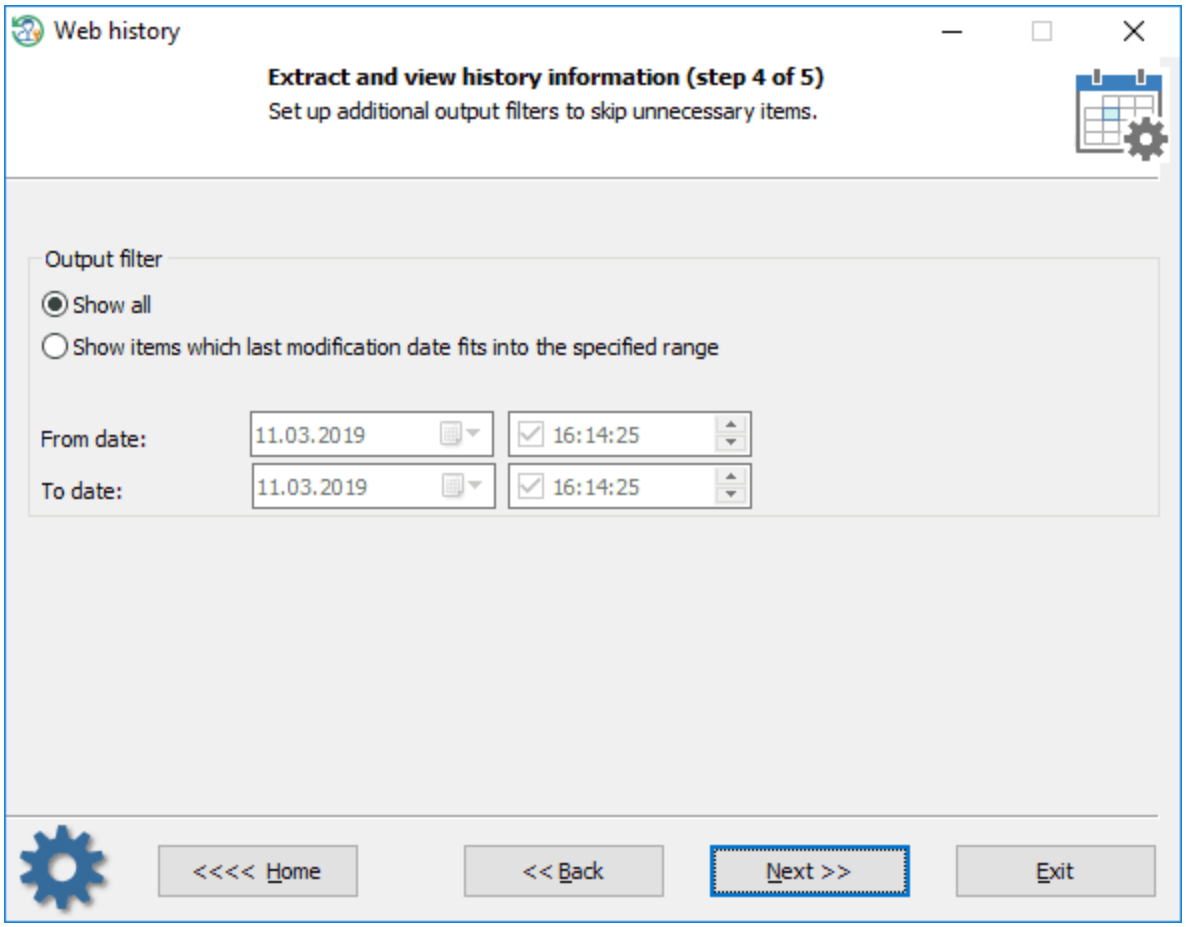
Тип информации



По умолчанию, программа осуществляет поиск следующих элементов:

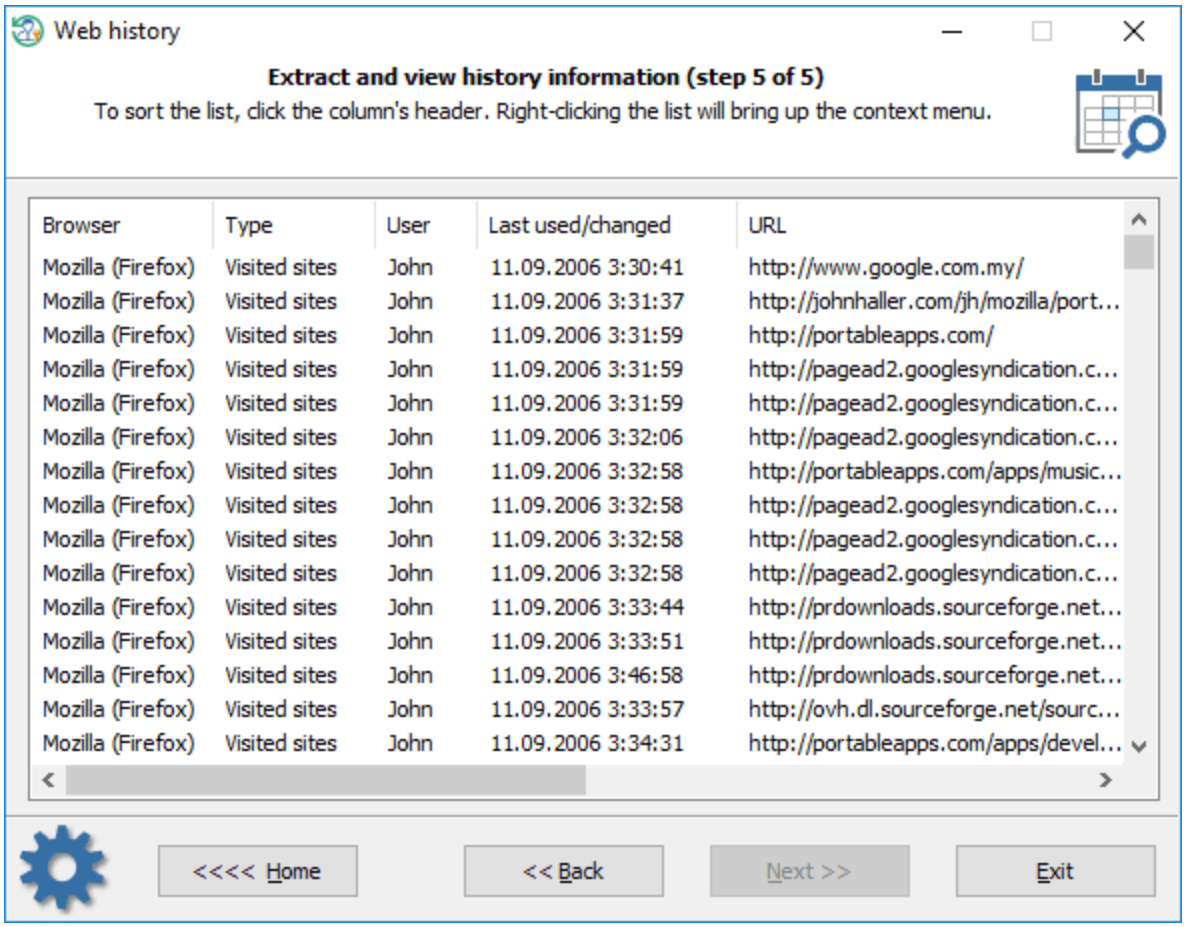
- Посещенных Web страниц
- Данные автозаполнения форм
- Сохраненные логины и пароли (если можно расшифровать мгновенно)
- Кукисы
- История закачек (не для всех браузеров)

Фильтры времени



Можно установить дополнительные фильтры по времени, чтобы пропустить ненужные элементы.

История Интернет



Статистику можно скопировать в буфер обмена или сохранить в файл. При необходимости, используя контекстное меню, вы также можете скрыть не интересующие вас записи.

Где браузеры хранят список посещенных Интернет страниц?

Internet Explorer
Посещенные места хранятся в файле index.dat. index.dat содержит различные записи: посещенные URL-адреса и открываемые в браузере файлы локального ПК, доступ к веб-почте, файлы cookie и т. д. Файл базы данных имеет собственный формат (Client UrlCache MMF) и впервые был представлен с выходом Internet Explorer 5. Формат index.dat файла не был сильно изменен с тех пор, физическое расположение, однако, может отличаться:
C:\Users\<USERNAME>\AppData\Local\Microsoft\History
C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\History
C:\Users\<USERNAME>\AppData\Roaming\Microsoft\Internet Explorer\UserData
Более старые Операционные Системы, например, Windows XP, использовали другие пути.

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

Microsoft Edge

Подобно Internet Explorer, Microsoft Edge хранит историю просмотра веб-страниц, кэш, файлы cookie, а также другую информацию в одном файле под названием WebCacheV01.dat, который, кажется, является преемником index.dat. В WebCacheV01.dat находится в каталоге:
C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\WebCache

Opera (старые версии)
История посещенных страниц хранится в файлах global_history.dat, global.dat и vlink4.файлы dat в текущем профиле программы. Файлы имеют разный формат (зависит от версии браузера).

Chrome (а также другие браузеры на базе Chromium)
Все посещенные URL-адреса хранятся в базе данных SQLite под названием history. Расположение history отличается и зависит от браузера. Например:
C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default

Firefox (а также другие браузеры на базе Mozilla)
Web история хранится либо в файле history.dat (формат mork) или в places.sqlite в более новых версиях. Типичное расположение C:\Users\<USERNAME>\AppData\Roaming\Mozilla\<PROGRAM>\Profiles\<PROFILENAME>. Например:
C:\Users\<USERNAME>\AppData\Roaming\Mozilla\Firefox\Profiles\owec6tnk.default

Где браузеры хранят данные автозаполнения форм?

Internet Explorer
Internet Explorer v4-6 сохраняет данные автозаполнения в специальном расположении реестра, называемом защищенным хранилищем. Несмотря на шифрование, все данные можно легко расшифровать и просмотреть, поскольку ключи шифрования хранятся вместе с защищаемыми данными. Расположение ключа реестра защищенного хранилища:
HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

Internet Explorer v7-9 использует другую интересную технику. Вместо шифрования конфиденциальных данных с помощью статического секретного ключа (IE 4-6), который можно легко вычислить, IE 7-9 для защиты данных использует исходный URL-адрес в качестве ключа шифрования. Таким образом, не зная веб-страницы, к которой принадлежат определенные данные, вы не сможете расшифровать сами данные. Более подробную информацию можно найти здесь. Reset Windows Password не поддерживает извлечение данных автозаполнения форм IE 7-9. Для этого лучше использовать PIEPR. Ключи реестра, где хранятся зашифрованные данные:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage1
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\FormData

Internet Explorer v10+ и Microsoft Edge имеют еще лучшую защиту. Все записи данных хранятся в Windows Vault и защищены при помощи DPAPI. Нет никакой возможности расшифровать данные без предоставления пароль и мастер-ключа владельца. Хитрая часть заключается в том, что RWP может расшифровать эти данные/пароли мгновенно, при условии что браузер сохранил его под учетной записью системы. Расположение Windows Vault для пользовательских данных:
C:\Users\<USERNAME>\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28

Opera (старые версии)
Данные автозаполнения форм можно обнаружить в следующих файлах:
C:\Users\<USERNAME>\AppData\Roaming\Opera\Profile\typed_history.xml
C:\Users\<USERNAME>\AppData\Roaming\Opera\Profile\search_field_history.dat

Chrome (и другие браузеры на базе Chromium)
Данные форм автозаполнения хранятся в файлах history и Web Data, оба имеют формат SQLite. Типичный путь для браузера Chrome:
C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default

Firefox (и другие браузеры на базе Mozilla)
Это либо formhistory.dat (более старые версии браузера) или formhistory.sqlite файл. Типичное расположение C:\Users\<USERNAME>\AppData\Roaming\Mozilla\<PROGRAM>\Profiles\<PROFILENAME>. К примеру:
C:\Users\<USERNAME>\AppData\Roaming\Mozilla\Firefox\Profiles\owec6tnk.default\formhistory.sqlite

Где браузеры хранят свои пароли?

Internet Explorer
Internet Explorer v4-6 хранит веб-пароли в защищенном хранилище.
HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

Пароли Internet Explorer v7-9 хранятся в следующем разделе реестра:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2

Расположение сохраненных паролей по умолчанию в 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

Некоторые версии IE также могут сохранять пароли HTTP basic authentication в хранилище учетных данных (Windows Vista и более поздне операционные системы). DPAPI используется для защиты этих записей.
C:\Users\<USERNAME>\AppData\Roaming\Microsoft\Credentials

Программа достаточно умна, чтобы извлечь некоторые дополнительные данные, которые хранятся в других местах. Например, Reset Windows Password позволяет анализировать базы данных Chrome для поиска элементов Internet Explorer, хранящихся там после переноса данных.

Opera (старые версии)
Все пароли хранятся в файле wand.dat в зашифрованном виде вместе с ключами дешифрования. Пароли могут быть легко расшифрованы только если не установлен мастер-пароль.
C:\Users\<USERNAME>\AppData\Roaming\Opera\Profile\wand.dat

Chrome (и другие браузеры на базе Chromium)
Браузеры на основе Chromium защищают пароли пользователей Windows при помощи DPAPI и хранят их в файле Login Data, который фактически является базой данных SQLite. Типичное расположение этого файла для Google Chrome:
C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default\Login data

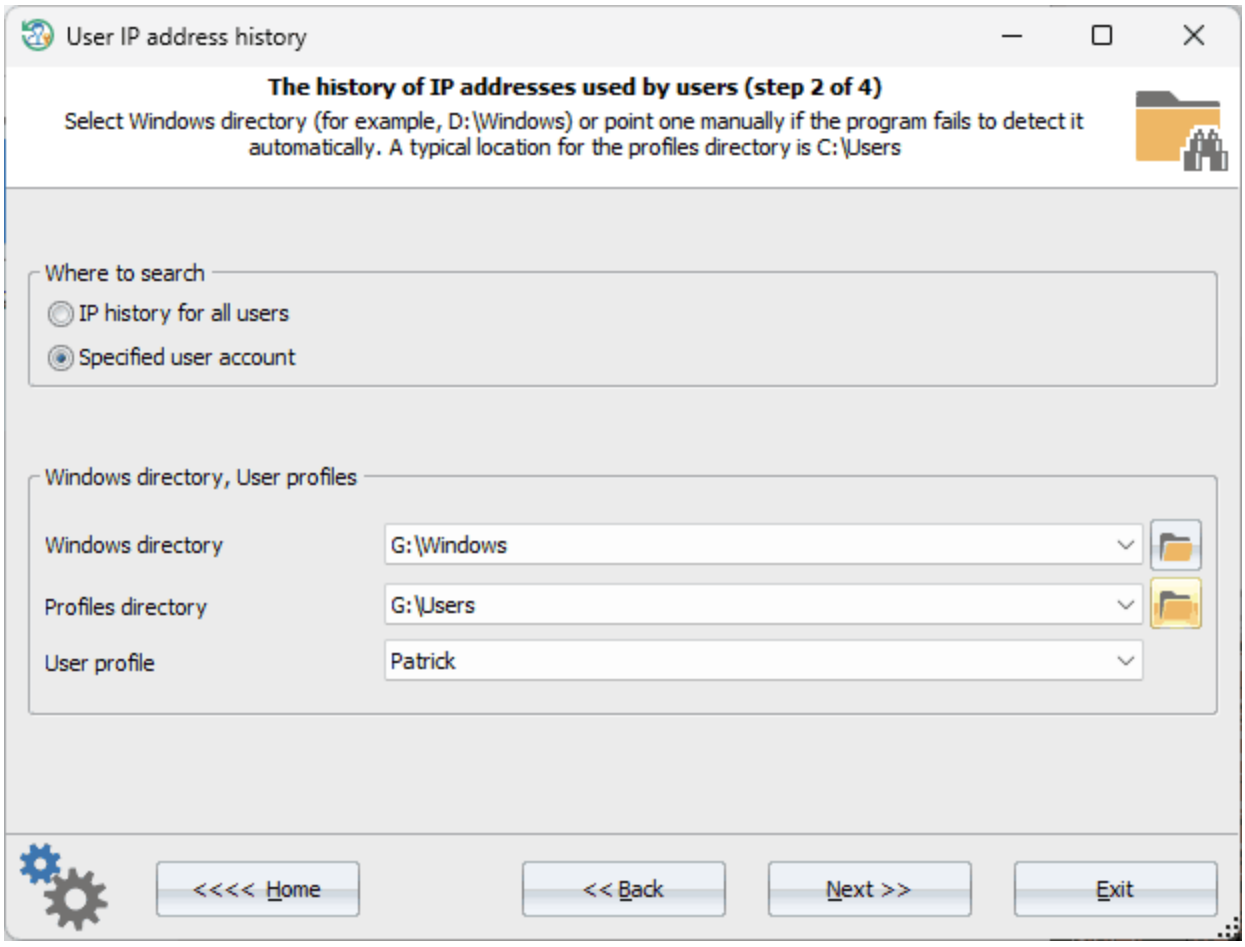
Firefox (и другие браузеры на базе Mozilla)
Mozilla прошла долгий путь развития формата хранения паролей. Изначально это был простой текстовый файл signons.txt. Затем в версии 2 появился signons2.txt, который имел префикс "#2C" в начале файла. Затем ему на смену пришел signons3.txt с префиксом "#2D" в версии 3 и т. д. После этого база данных signons.sqlite вступила в игру. Но это еще не конец истории. Firefox v32.x и выше имеет новое хранилище для паролей - logins.json, который представляет собой файл в формате JSON. Несмотря на кажущееся разнообразие, защита данных практически одинакова.

Типичное расположение файлов: C:\Users\<USERNAME>\AppData\Roaming\Mozilla\<PROGRAM>\Profiles\<PROFILENAME>.

3.6.8 История IP адресов пользователей

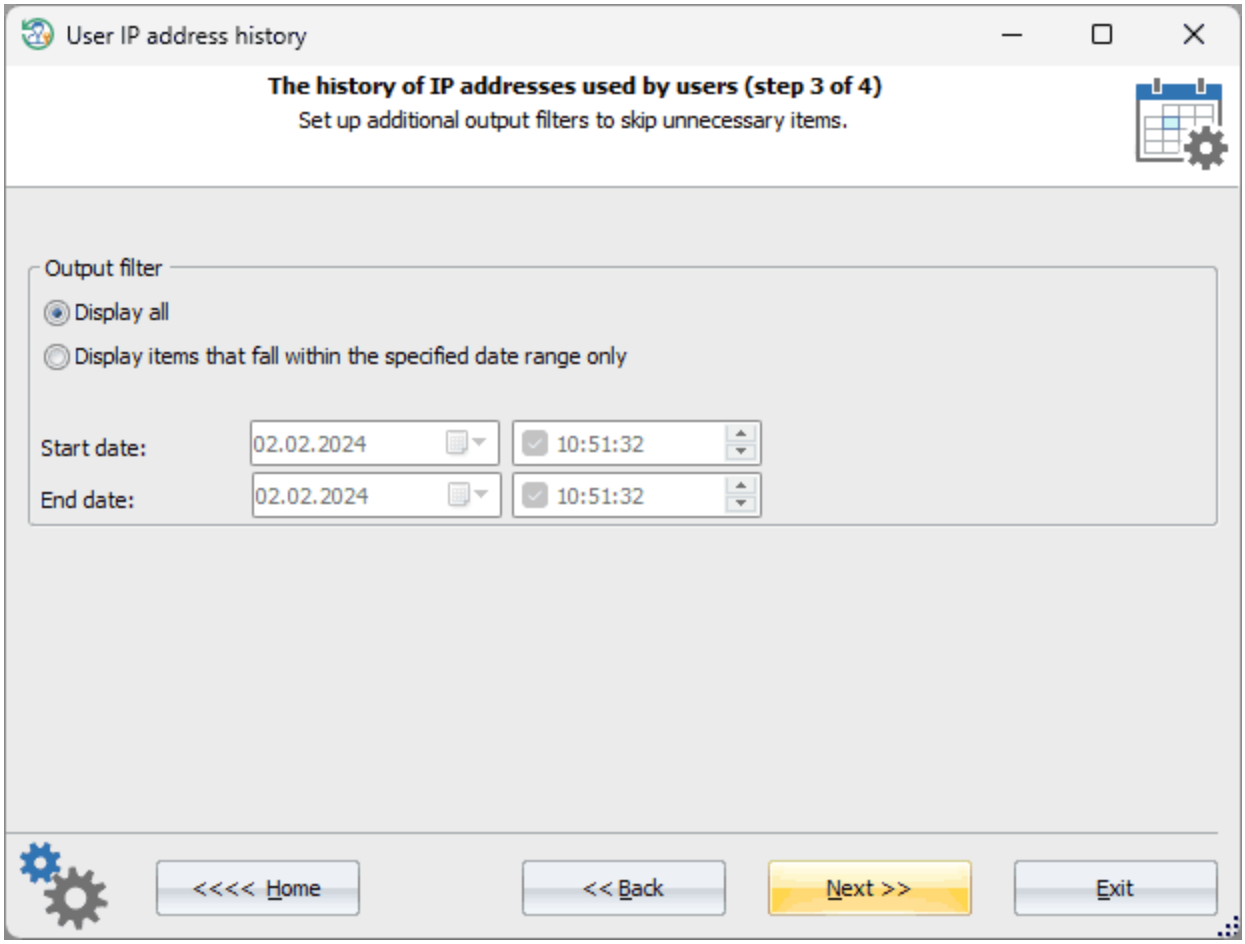
Это новейшая и уникальная функция (на момент создания больше нет ни в одной другой программе), позволяющая извлечь историю внешних IP-адресов пользователей в операционной системе Windows. Теперь вы можете проанализировать сетевую активность пользователей отследив IP-адреса, с которых осуществлялся выход в сеть, а также время.
Аналогично текстовым паролям, Microsoft декларирует, что история IP-адресов не хранится нигде в системе. Однако, это оказалось не совсем так. Несмотря на то, что информация о внешних IP разбросана по системе, оказалось вполне реально расшифровывать и вытаскивать ее для любого пользователя.

Выбор пользователя



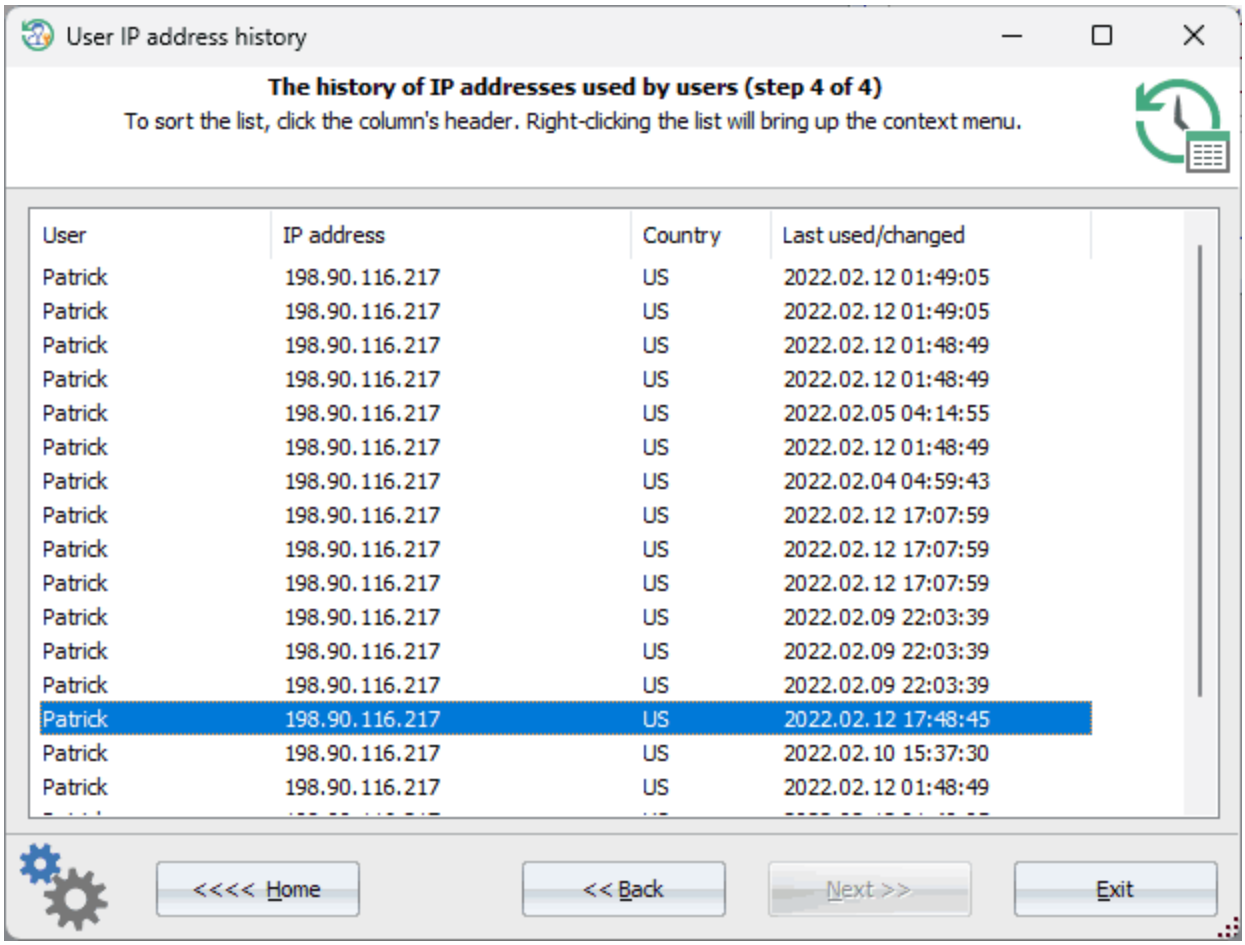
Выберите пользователя системы, историю IP-адресов которого необходимо извлечь.

Фильтры времени



На следующем шаге мастера выберите период, за который хотите получить информацию.

История IP адресов пользователей



Программа извлекает историю IP пользователей из нескольких мест Windows включая такие, которые требуют дальнейшей расшифровки. Во время расшифровки вы можете увидеть запрос на пароль пользователя.

Расшифрованную историю IP-адресов можно скопировать в буфер обмена или сохранить как HTML отчет.

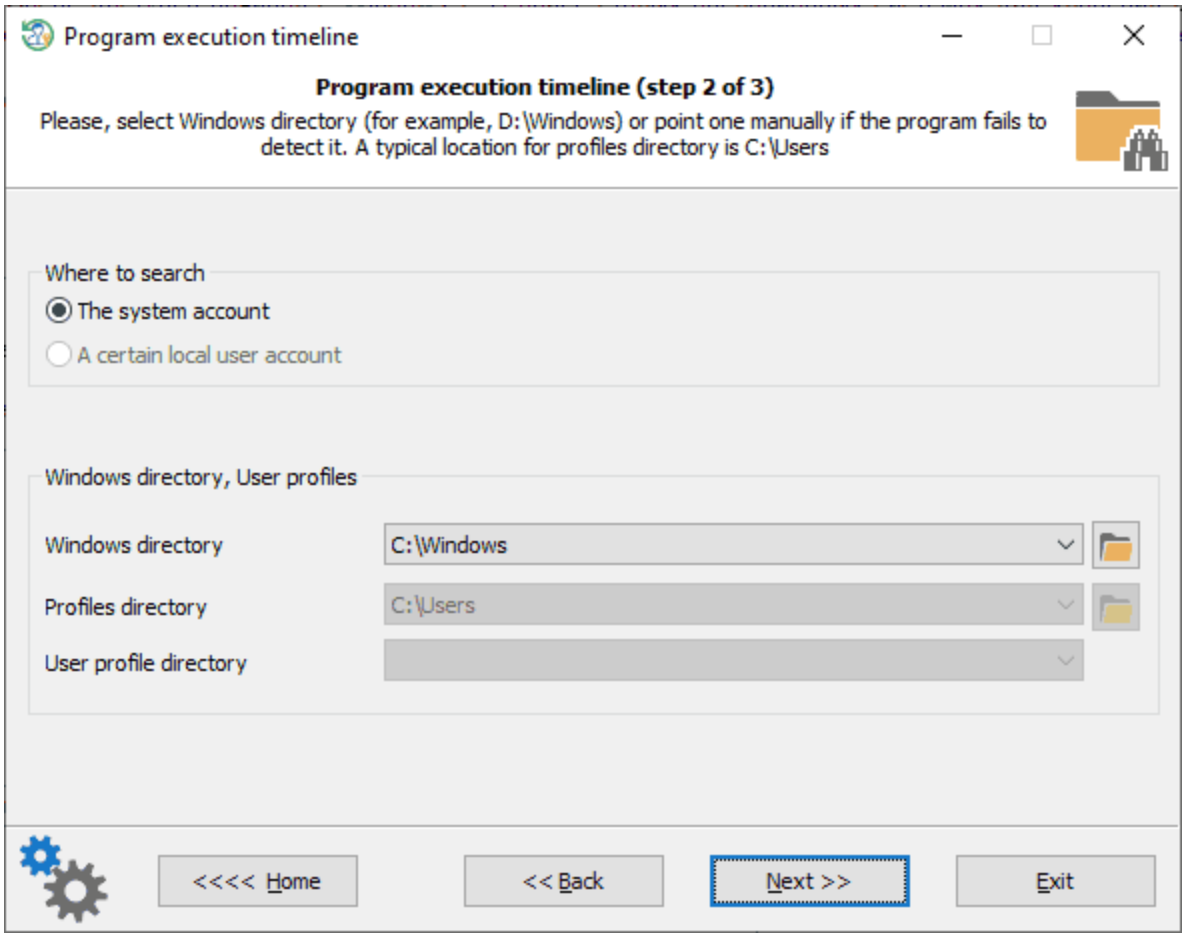
3.7 Криминалистический анализ

3.7.1 История запуска программ

Вы, наверное, не удивитесь, но в ОС Windows существует много артефактов, кэширующих информацию об открываемых документах или запускаемых файлах. Один из таких - AMCache, который хранит данные о запускаемых и устанавливаемых программах. AMCache доступен начиная с Windows 7. В более старых операционных системах для хранения данных о запускаемых программах использовался формат BCF. Физически оба формата представляют собой файлы, находящиеся в папке %WINDIR% \appcompat\Programs. AMCache.hve это обычный файл реестра, тогда как RecentFileCache.bcf - простой бинарный файл.

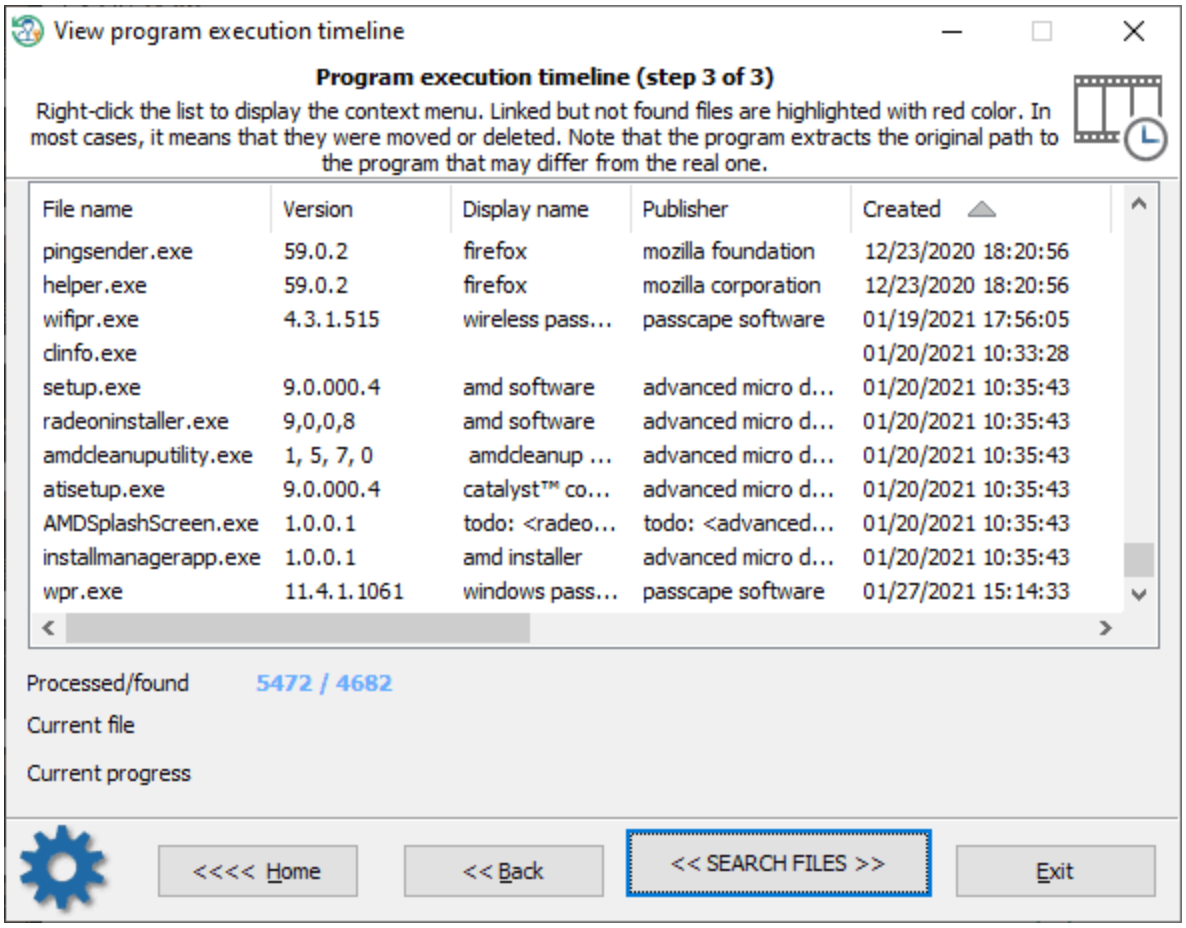
Программа поддерживает оба формата, однако в старом формате BCF не содержатся данные о времени запуска программ.

Выбор каталога Windows



Выбираем каталог Windows, найденный программой.

Последние запускаемые программы



Нажимаем кнопку << *ПОИСК ФАЙЛОВ* >> и ждем пока программа выполнит поиск и анализ файлов.

Список файлов можно отсортировать по дате и сохранить в текстовый или HTML файл.

Красным цветом выделены файлы, ссылки на которые остались, но сами они не обнаружены. Например, были перемещены или удалены.

3.7.2 Временная шкала активности Windows

Временная шкала - это сравнительно новая функция Windows 10, появившаяся впервые в версии **1803**. Она показывает вашу прошлую активность, то, над чем вы работали ранее. Например, приложения, которые вы открыли, файлы, которые вы использовали, веб-сайты, которые вы просматривали и т.д. В Windows 10 настройки временной шкалы находятся в меню **Пуск -> Настройки -> Конфиденциальность -> История действий**. Если вы хотите запретить Windows собирать данные о вашей активности, просто снимите флажок рядом с надписью *'Показывать историю моей активности на этом устройстве*'.

<USER_PROFILE>\AppData\Local\ConnectedDevicesPlatform является домашним каталогом для **CPDS** файлов. Файл **CPDS**, скорее всего, означает **C**onnected **P**latform **D**evice **S**ettings. Это файл в формате JSON, который содержит настройки для управления профилем временной шкалы. Помимо общих настроек, указанный выше каталог содержит до трех файлов .**CPDS**, соответствующих локальной, доменной или учетной записи Майкрософт в профиле пользователя.

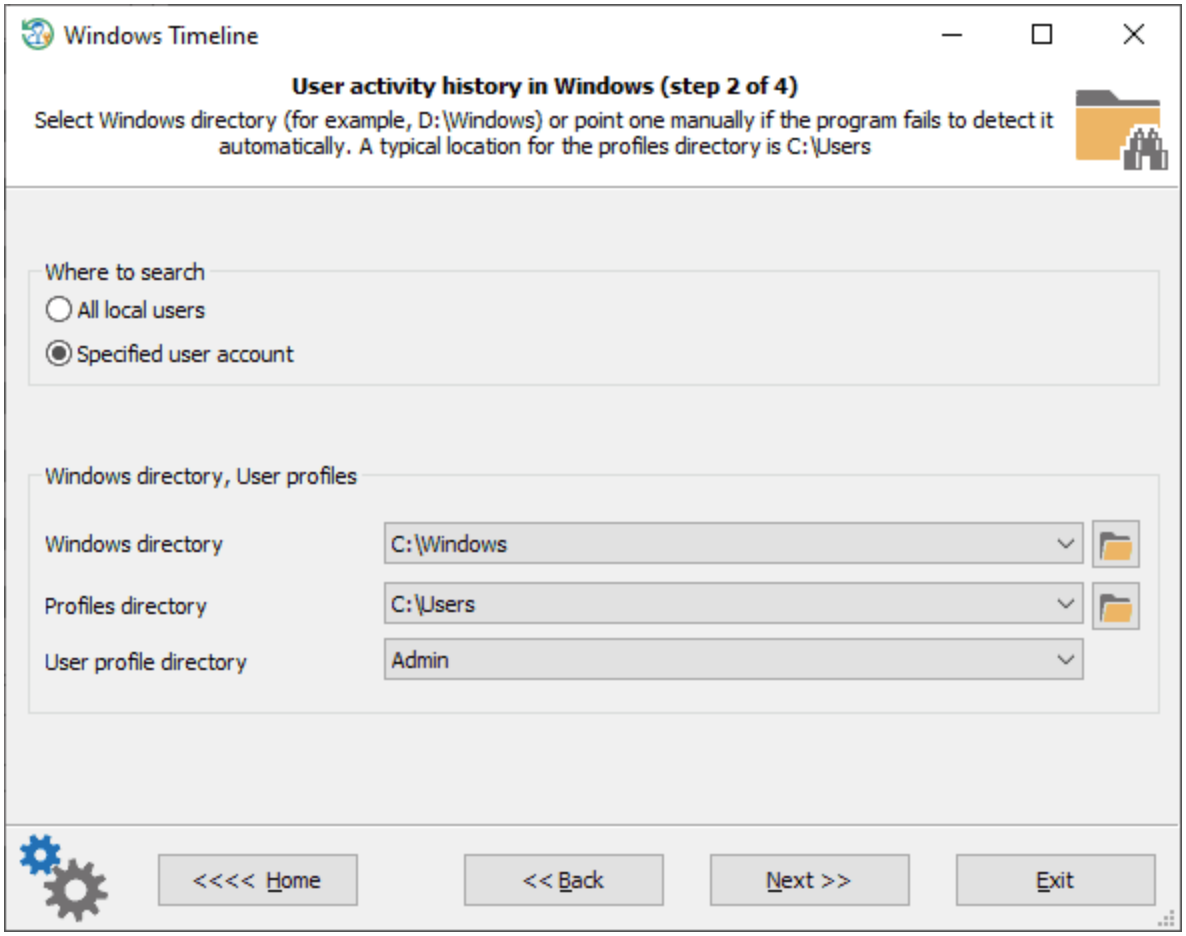
Временная шкала Windows 10 хранит активность пользователя в файле **ActivitiesCache.db**, представляющий собой базу данных SQLite. Вы можете найти эту базу в каталоге **<USER_PROFILE>\AppData\Local\ConnectedDevicesPlatform\<PROFILE_NAME>\ActivitiesCache.db**

Почти вся информация, относящаяся к активности пользователя, сведена в пару таблиц этой базы: **Activity_PackageId** и **Activity**. По умолчанию, записи из таблиц хранятся системой в течение 30 дней до тех пор, пока не будут помечены как удаленные.

Reset Windows Password отображает в удобочитаемом виде хранящиеся во временной шкале Windows данные об активности любого пользователя. Программа извлекает также некоторую дополнительную информацию. Например, над какой программой работал определенный пользователь, когда и как долго, документы, которые он открывал из приложения, активное и общее время использования, активное устройство и т.д.

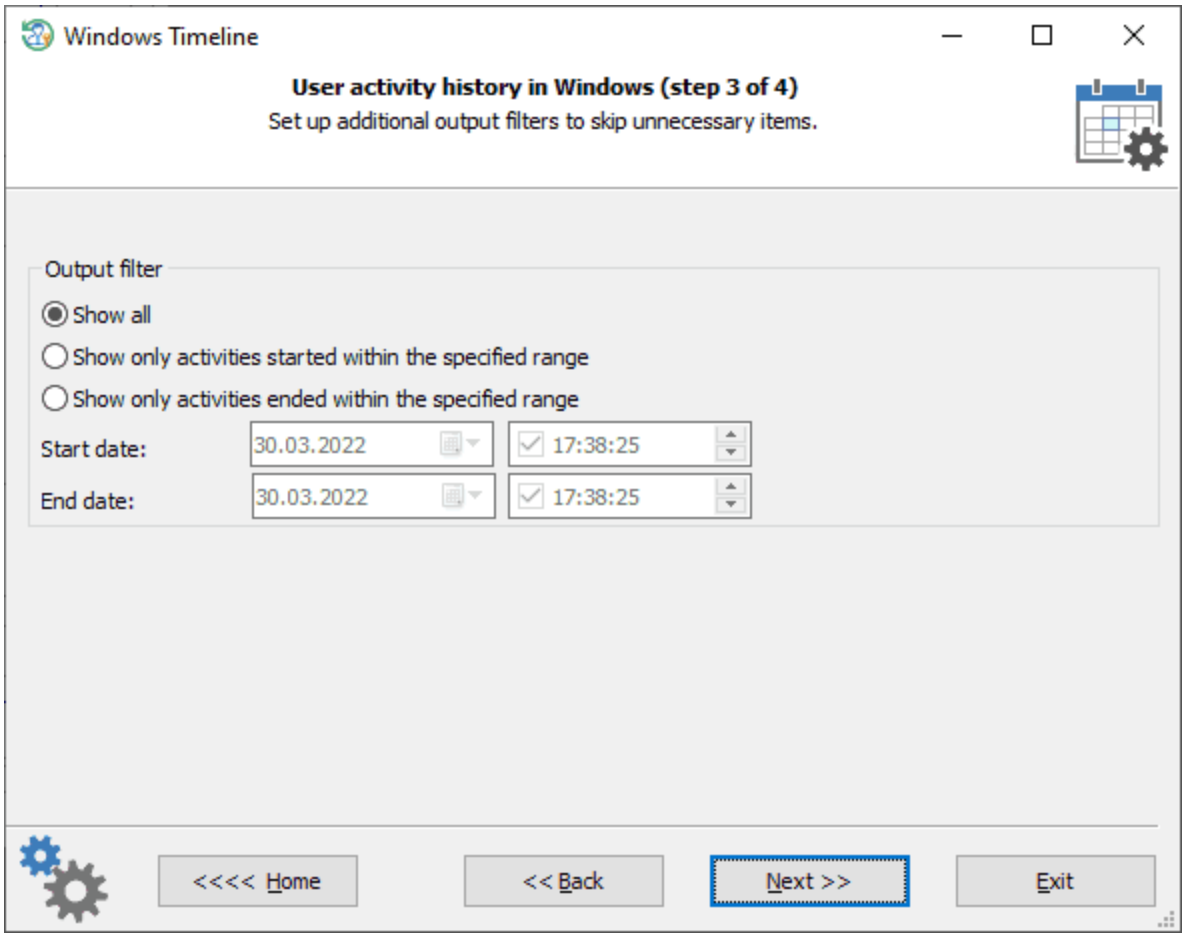
Таким образом, программа значительно упрощает использование и анализ временной шкалы активности, нежели чем ручной разбор и анализ. 3-шаговый рабочий процесс поможет вам выбрать начальную учетную запись, настроить дополнительные временные фильтры и отобразить временную шкалу активности пользователя. Просто, как 1-2-3.

Выбор учетной записи для анализа временной шкалы Windows



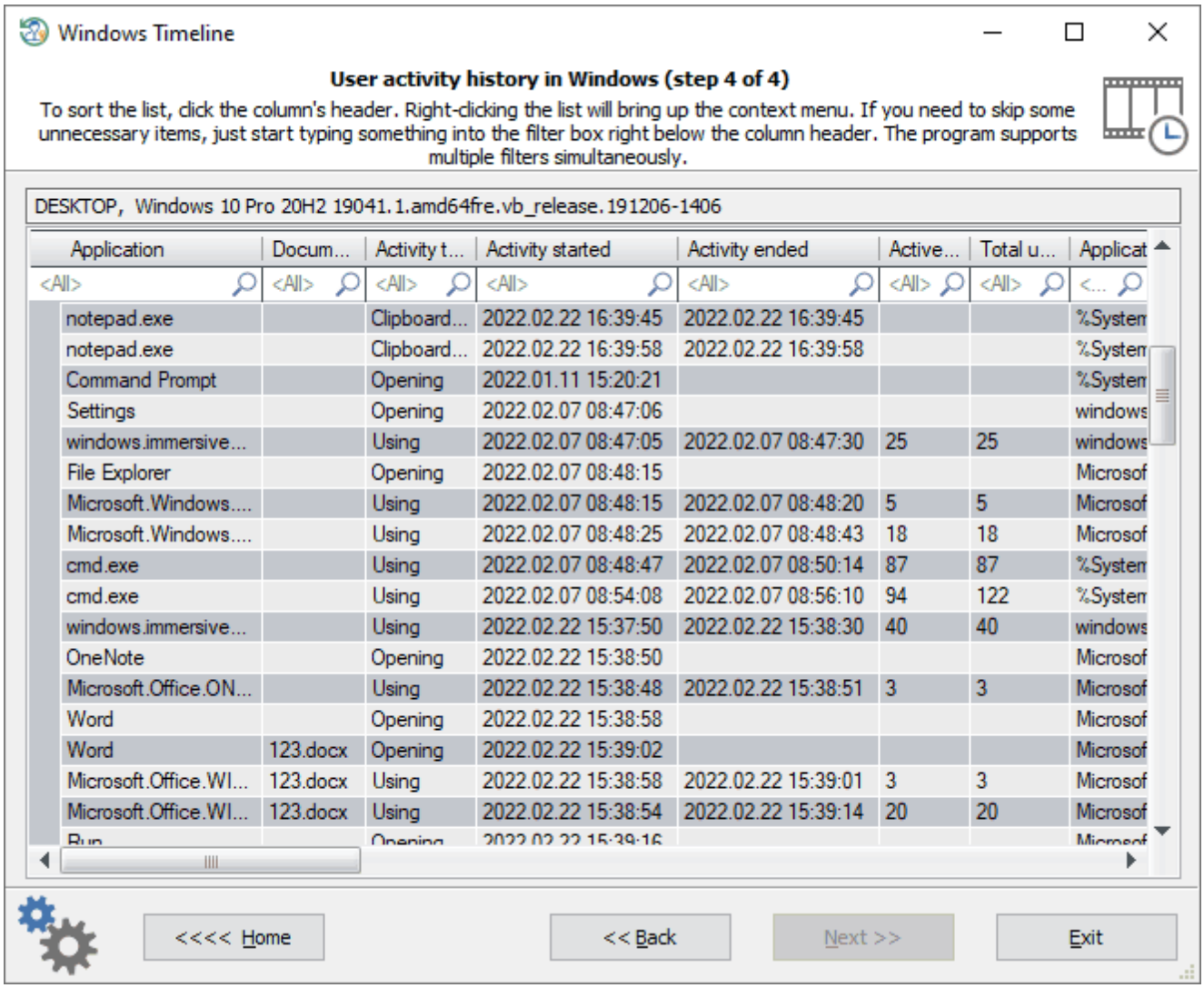
Выберите пользователя, историю активности которого нужно просмотреть. По умолчанию, отмечены все пользователи.

Настройка фильтров отображения временной шкалы активности



Настройка дополнительных временных фильтров позволяет пропустить показ ненужной активности пользователей.

Временная шкала активности Windows



Excel-подобная таблица позволяет наиболее удобно представить извлеченные из базы данные. Можно отсортировать таблицу, щелкнув на заголовке столбца. Если вам нужно отфильтровать ненужные элементы, просто начните вводить текст в поле фильтра прямо под заголовком столбца. Программа поддерживает несколько фильтров одновременно.

Вот краткое описание того, какая информация содержится в каждом столбце таблицы.

Application - краткое имя приложения, которое сгенерировало запись об активности пользователя
Document name - файл, который пользователь открывал или редактировал в приложении
Activity type - тип операции. Например: отправка уведомления, аутентификация, открытие приложения/файла/URL, редактирование приложения/файла/URL, операция с буфером обмена, системная операция.
Activity started - время начала активности
Activity ended - время окончания активности
Active usage - сколько времени (в секундах) приложение было в фокусе пользователя и интенсивно им использовалось
Total usage - сколько всего времени (в секундах) приложение использовалось пользователем
Application path - полный путь к приложению

Document location - полный путь к документу (который открывался/редактировался в приложении)
Parent application - родительское приложение текущей активности. Например, для операции вставки в буфер обмена это приложение, из которого были скопированы данные.
Source host - URL-адрес, представляющий кроссплатформенное сопоставление идентификаторов для приложения
Clipboard content - содержимое буфера обмена Windows (только если **Activity type** - операция с буфером обмена).
User - имя пользователя. Обратите внимание, что один профиль пользователя может содержать 3 учетных записи. Таким образом, этот столбец может содержать до 3 разных имен для одного профиля пользователя.
Account type - тип пользователя: локальный, доменный или учетная запись Майкрософт
User status - показывает, вовлечен ли пользователь в работу с приложением
User timezone - часовой пояс, в котором устройство, используемое для создания активности, находилось во время создания активности
Device - название устройства (включая его модель, тип и производителя), используемого для создания активности
Status - состояние, используемое для идентификации объекта активности: активно, обновлено, удалено или проигнорировано

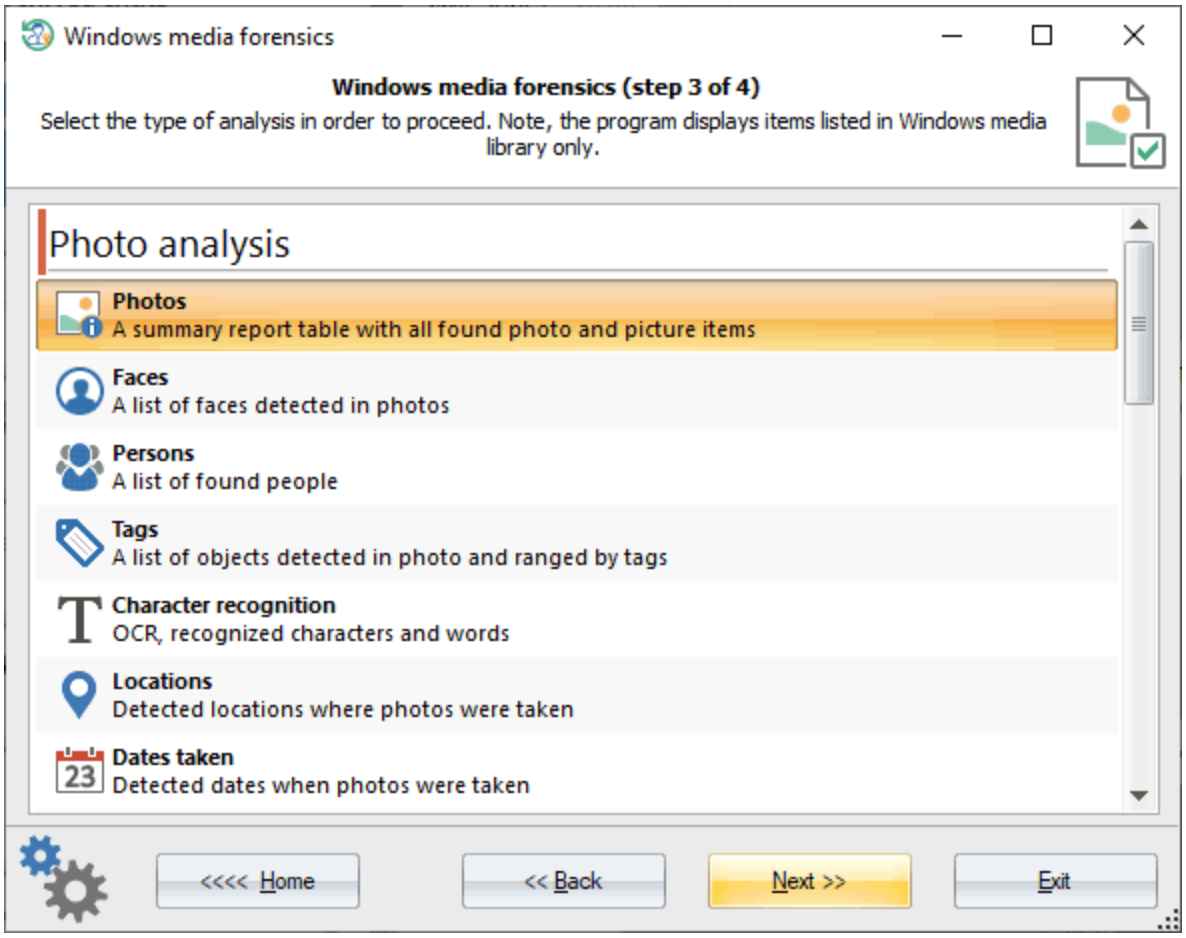
3.7.3 Анализ Windows Media

Утилита для экспертизы Windows Media анализирует и отображает в удобочитаемом формате артефакты фотографий и видео, которые хранятся в приложении Windows Photos. Windows Photos предоставляет огромное количество информации, которая может быть полезна следователям при проведении цифрового криминалистического анализа.

Приложение Windows Photos доступно в операционных системах начиная с Windows 10 и в более поздних версиях. База данных приложения находится в:
C:\Users\%username%
\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\LocalState\MediaDb.v1.sqlite

Дополнительные фото, видео и медиа базы данных можно найти по таким путям:
C:\Users\%username%\AppData\Local\Packages\Microsoft.ZuneVideo_8wekyb3d8bbwe
C:\Users\%username%\AppData\Local\Packages\Microsoft.ZuneMusic_8wekyb3d8bbwe

Вы можете использовать функцию резервного копирования программы, чтобы сохранить данные для дальнейшего анализа.

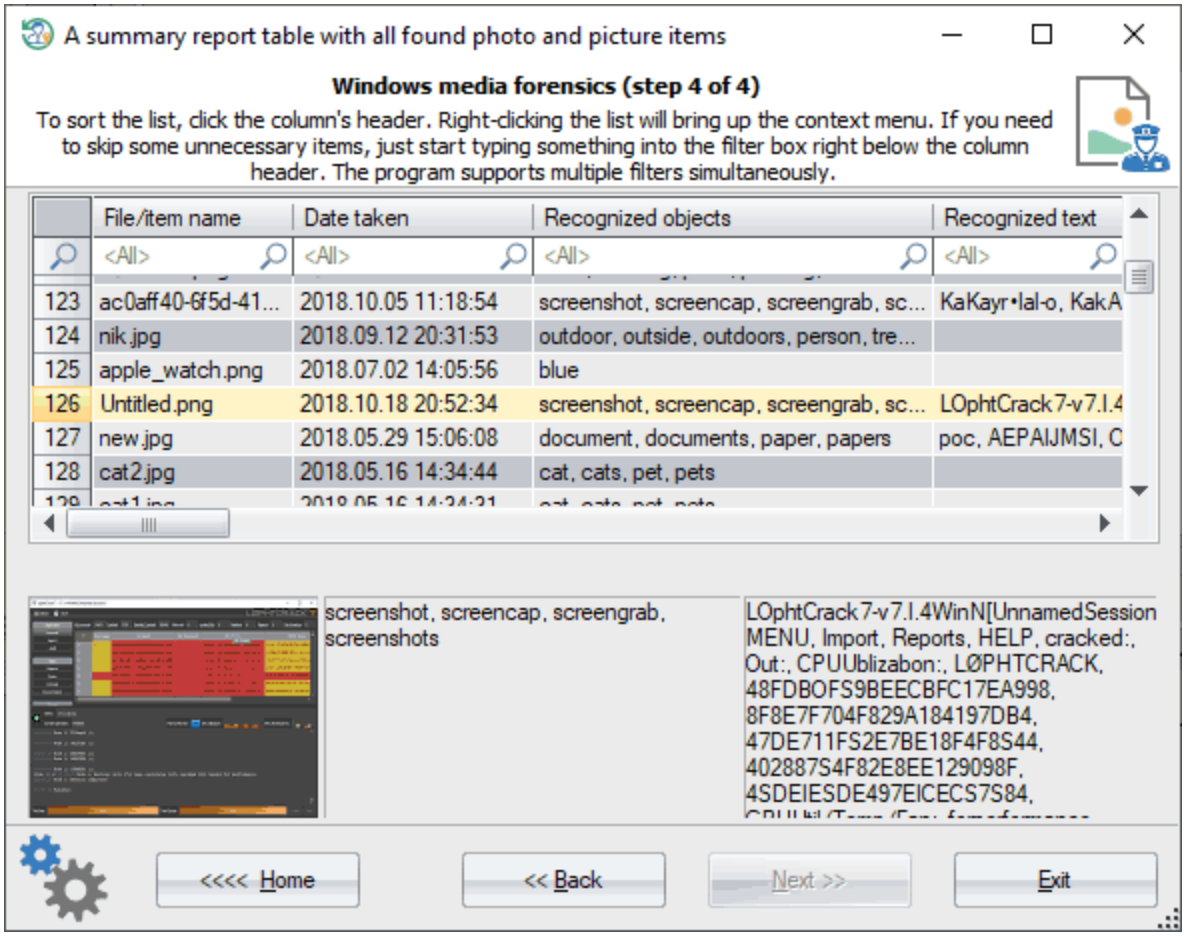


Утилита для экспертизы Windows Media состоит из нескольких частей:

- Библиотека изображений
- Библиотека видео
- Активность пользователя
- Библиотека приложения Photo
- Активность пользователя в Photos
- Библиотека приложения Media player
- Активность пользователя в Media player

3.7.3.1 Библиотека изображений

3.7.3.1.1 Изображения



Этот отчет содержит общую информацию о фотографиях и изображениях. А именно:

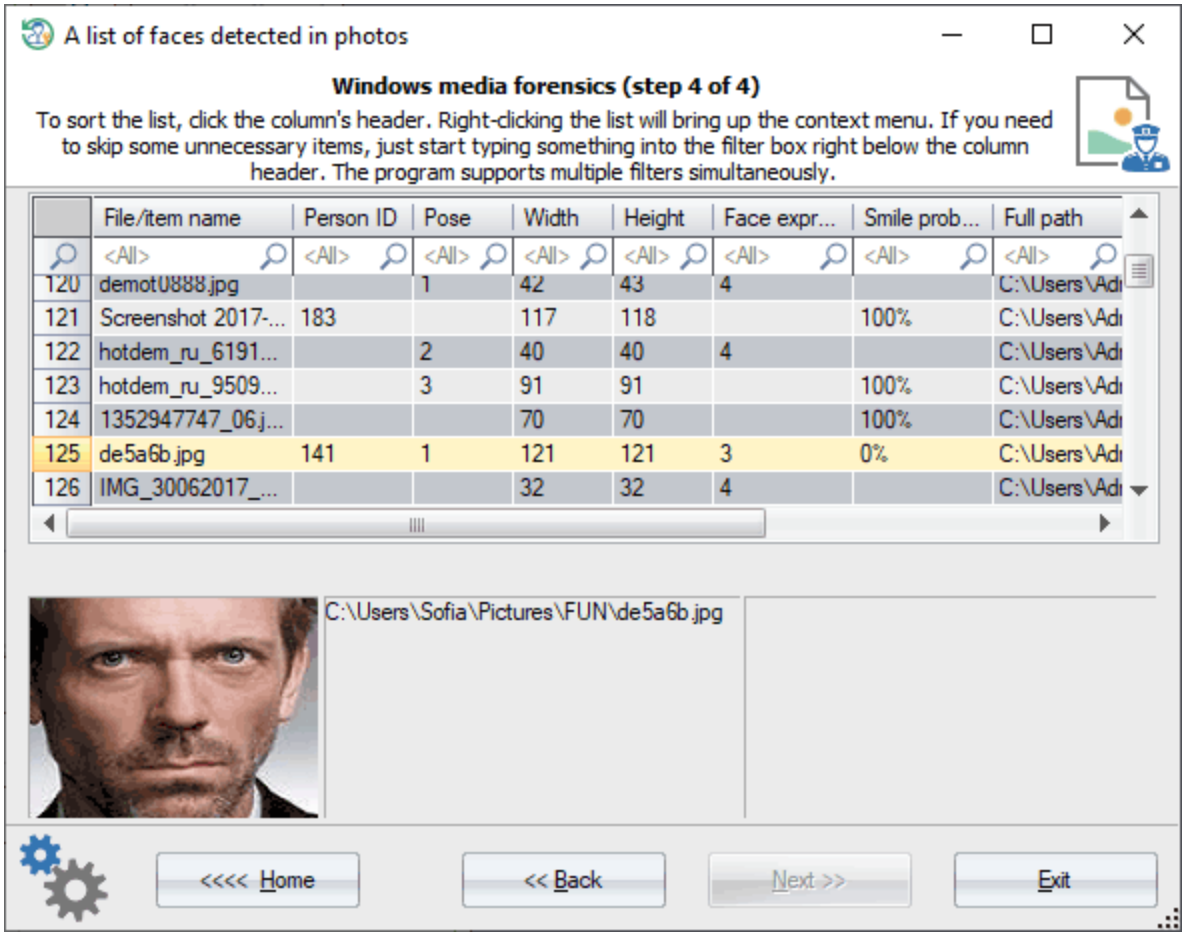
- Имя файла
- Когда сделана фотография
- Распознанные объекты (ранжирование по заранее определенным тегам)
- Распознанный текст. Обратите внимание, международные символы не распознаются должным образом, если в исходной операционной системе не установлен соответствующий язык.
- Количество лиц, найденных на фотографии
- Размер файла
- Ширина изображения
- Высота изображения
- Страна
- Регион
- Координаты широты
- Координаты долготы
- Подпись к изображению
- Полный путь к файлу
- Автор изображения
- Авторское право на изображения
- Путь к дубликату, если найден
- Качество изображения
- Производитель камеры

- Модель камеры
- Диафрагма камеры
- Фокусное расстояние камеры
- ISO
- Выдержка камеры
- Приложение в котором редактировалось изображение
- Время создания/изменения/редактирования
- Время последнего просмотра в библиотеке
- Название альбома, к которому принадлежит изображение

Таблица отчета содержит поля фильтров, расположенные прямо под заголовками столбцов. Эти фильтры можно использовать для сортировки ненужных элементов или для быстрого поиска определенных изображений. Например, если вам нужно проверить, есть ли какие-либо скриншоты с кредитными картами, просто введите 'visa' в фильтр 'Распознанный текст', чтобы найти все файлы изображений, содержащие слово 'visa'.

Вы можете использовать контекстное меню для копирования отдельных данных или всего текста в буфер обмена, сохранения отчета в файл или создание архива с выбранными записями.

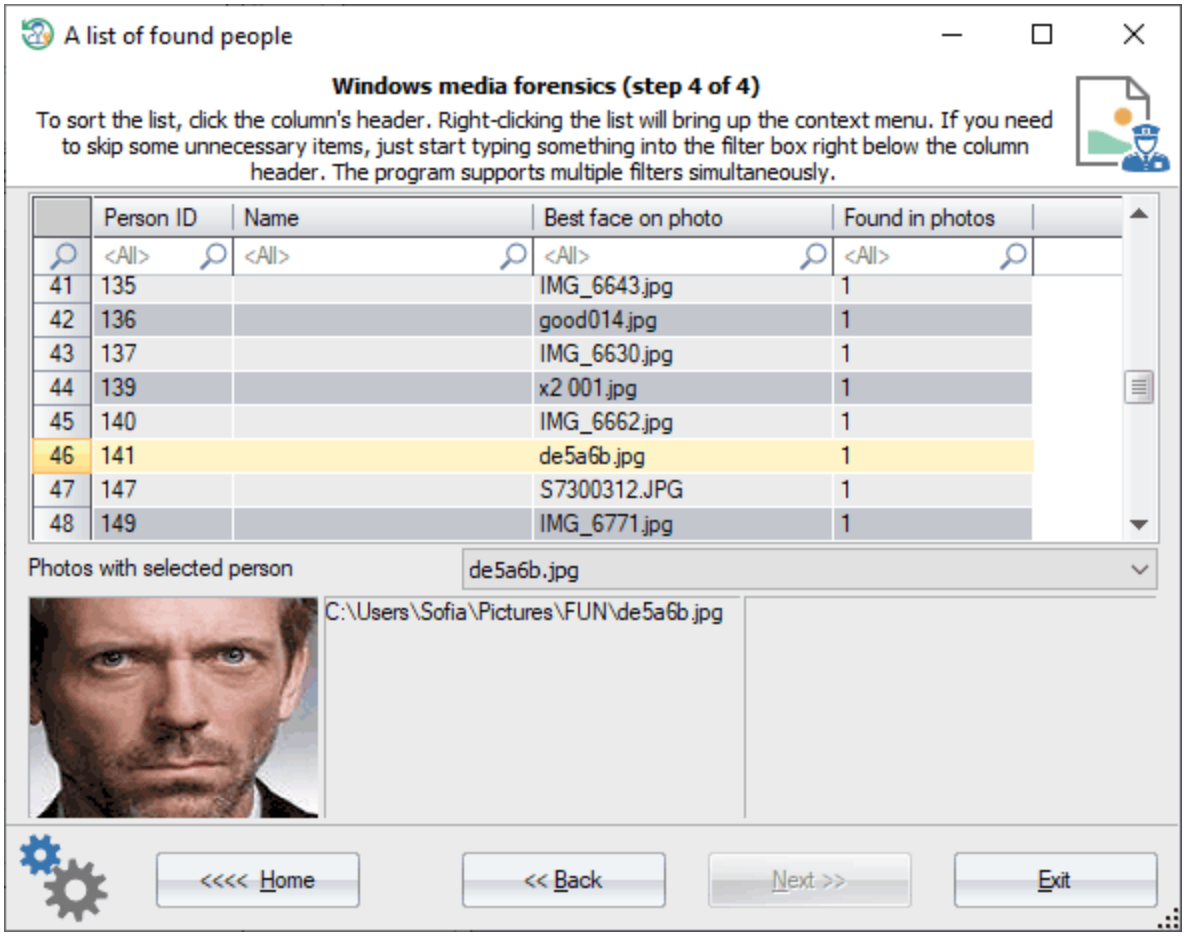
3.7.3.1.2 Лица



Отчет **Лица** содержит список найденных лиц и их свойств:
- Имя файла в котором было найдено лицо
- Идентификатор человека
- Позиция лица
- Ширина (в пикселях)
- Высота (в пикселях)
- Выражение
- Вероятность улыбки
- Полный путь к файлу изображения

Чтобы найти другие лица, связанные с этим человеком, откройте отчет Люди.

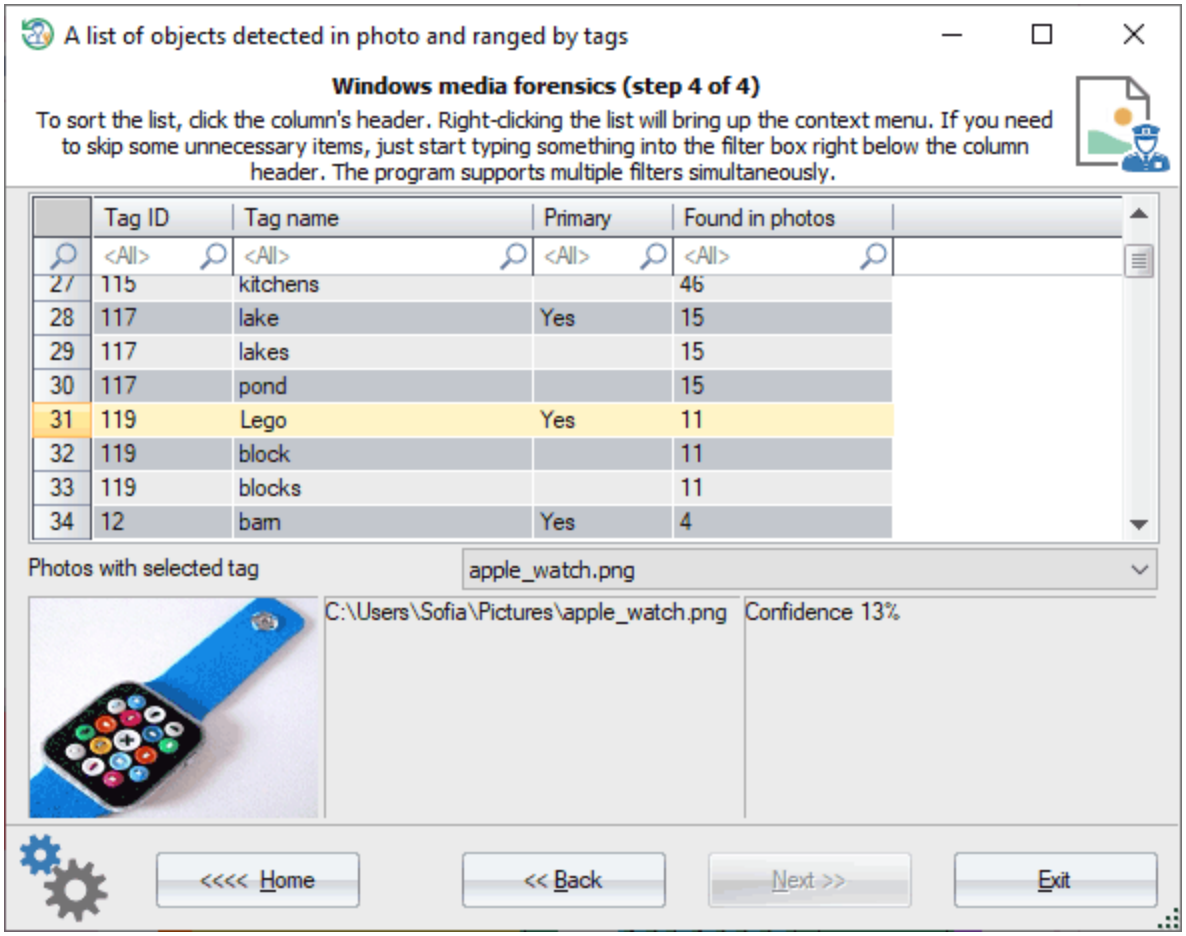
3.7.3.1.3 Люди



В отчете **Люди** отображаются люди, сгруппированные по идентификатору. Каждая запись содержит:
- Идентификатор персоны
- Имя (отображается только если пользователь непосредственно задал его ранее)
- Файл изображения, содержащий фотографию наиболее высокого качества
- Количество фотографий с найденным человеком

Чтобы просмотреть больше фотографий с этим человеком, отметьте его в таблице, затем выберите файл изображения из выпадающего списка под таблицей.

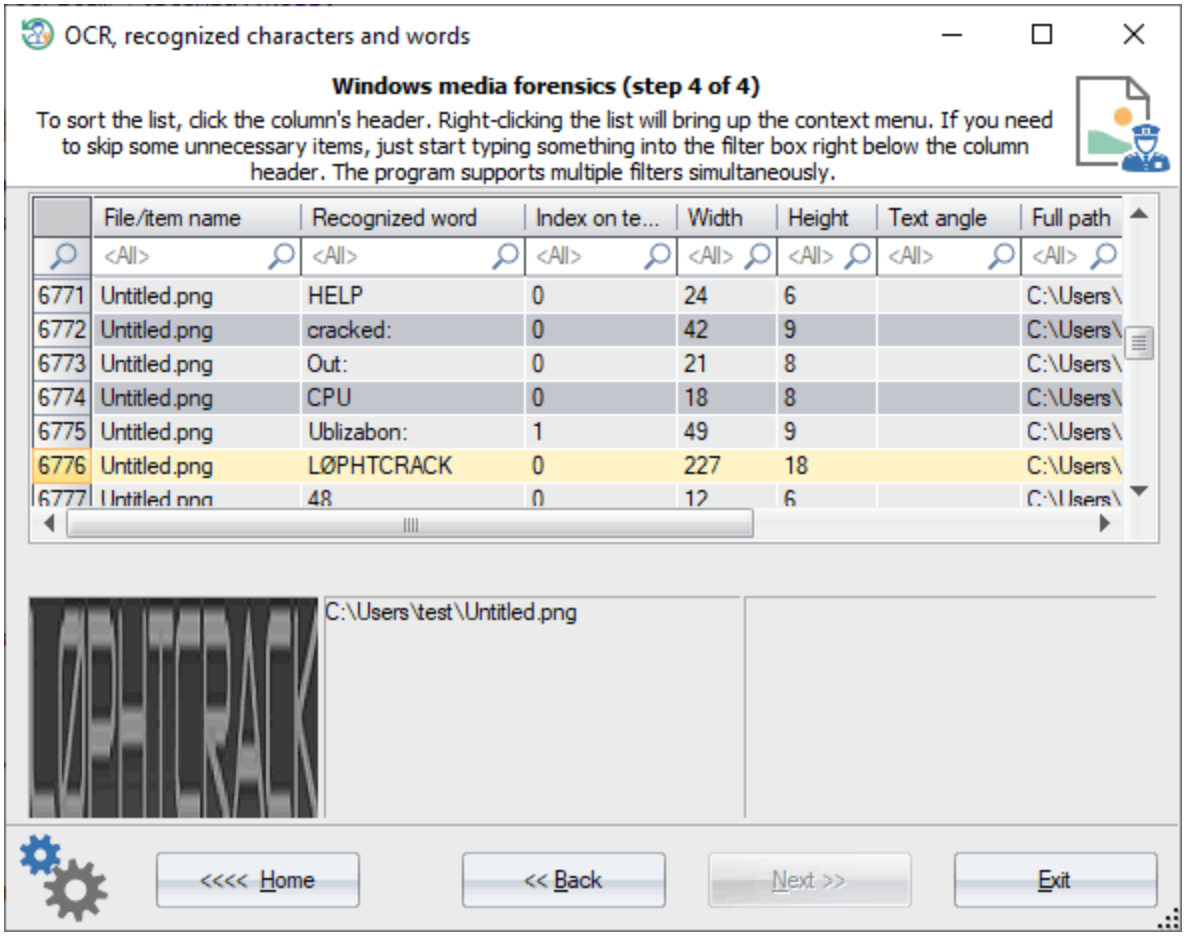
3.7.3.1.4 Тэги



В таблице тегов отображается список объектов и фотографий, связанных с этими объектами. Каждый тег обладает следующими свойствами:

- Идентификатор тэга
- Название тэга
- Основной или нет
- Количество изображений с этим тэгом

3.7.3.1.5 Распознавание текста

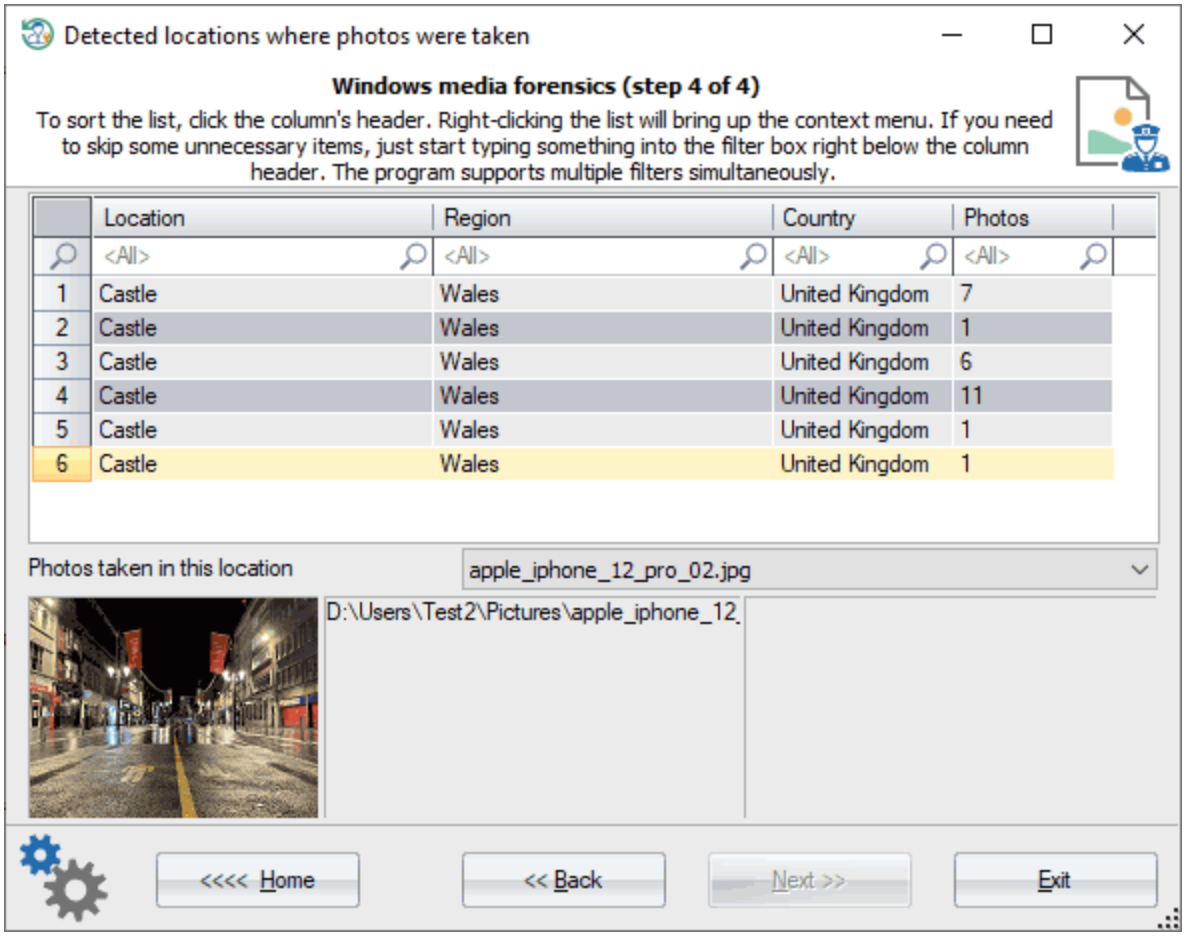


Windows Photo имеет простой механизм оптического распознавания символов. Вы можете использовать функцию распознавания текста для поиска текста и анализа его свойств:

- Имя файла изображения
- Распознанное слово
- Индекс слова в текстовой строке, начиная с нуля
- Ширина слова в пикселях
- Высота слова
- Угол наклона
- Полный путь к файлу

Забавно, что помимо очевидного использования, эта функция может идентифицировать некоторые виды водяных знаков на изображениях.

3.7.3.1.6 Местоположения

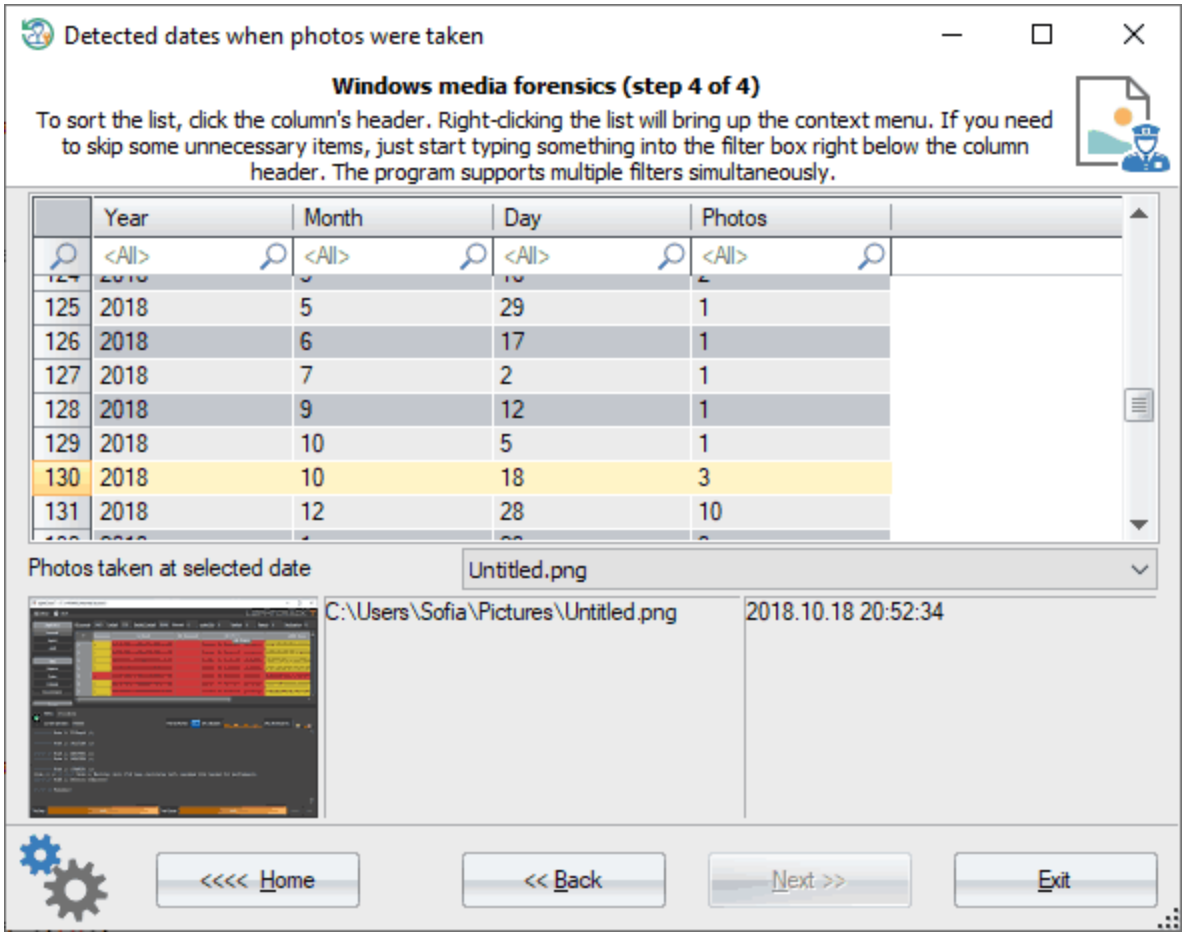


Если исходные изображения содержат какие-либо теги EXIF, связанные с местоположением, эта информация используется для заполнения таблицы **Местоположений**:

- Точное место
- Регион
- Страна
- Фотографии, сделанные в этом месте

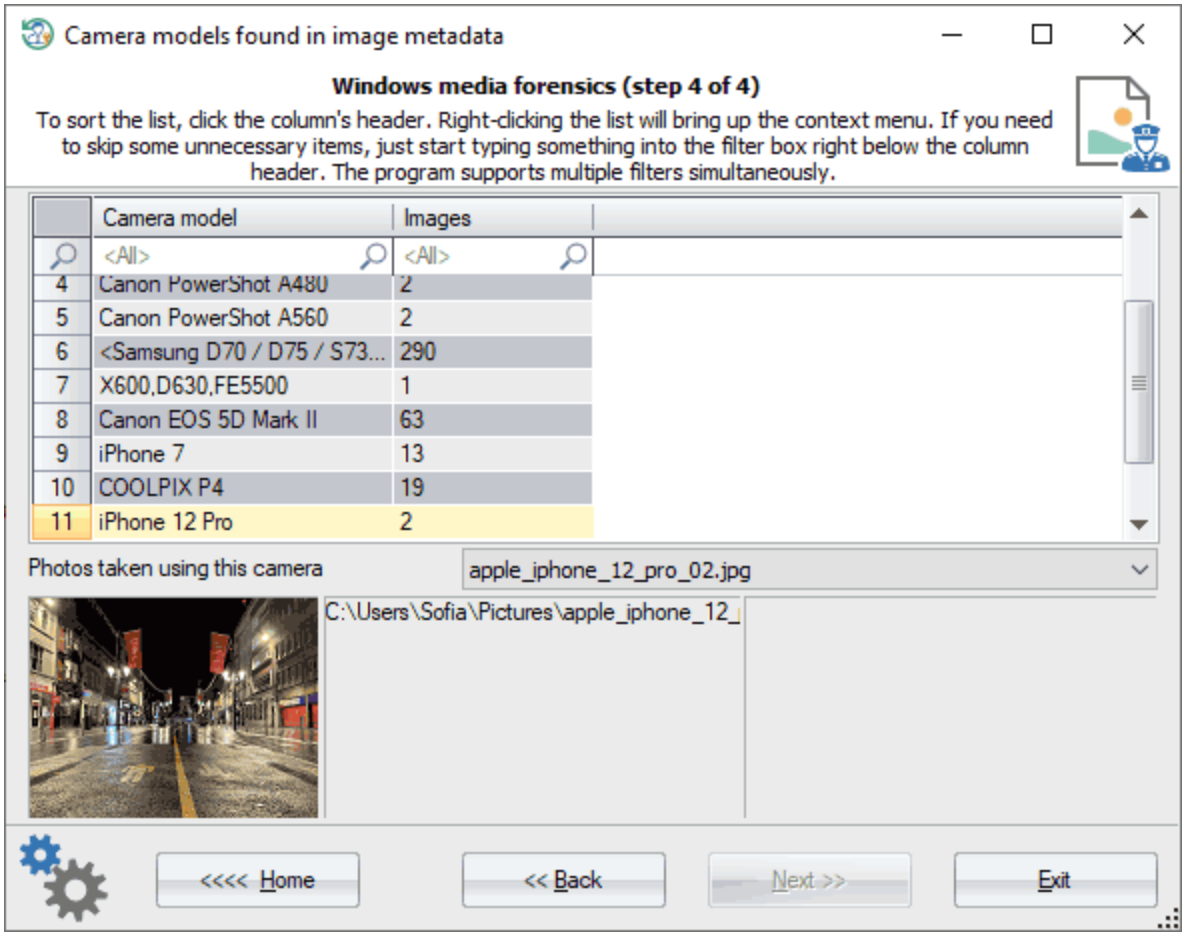
Большинство мобильных устройств хранят метаданные с информацией о местоположении в создаваемых ими фотографиях.

3.7.3.1.7 Даты созданий



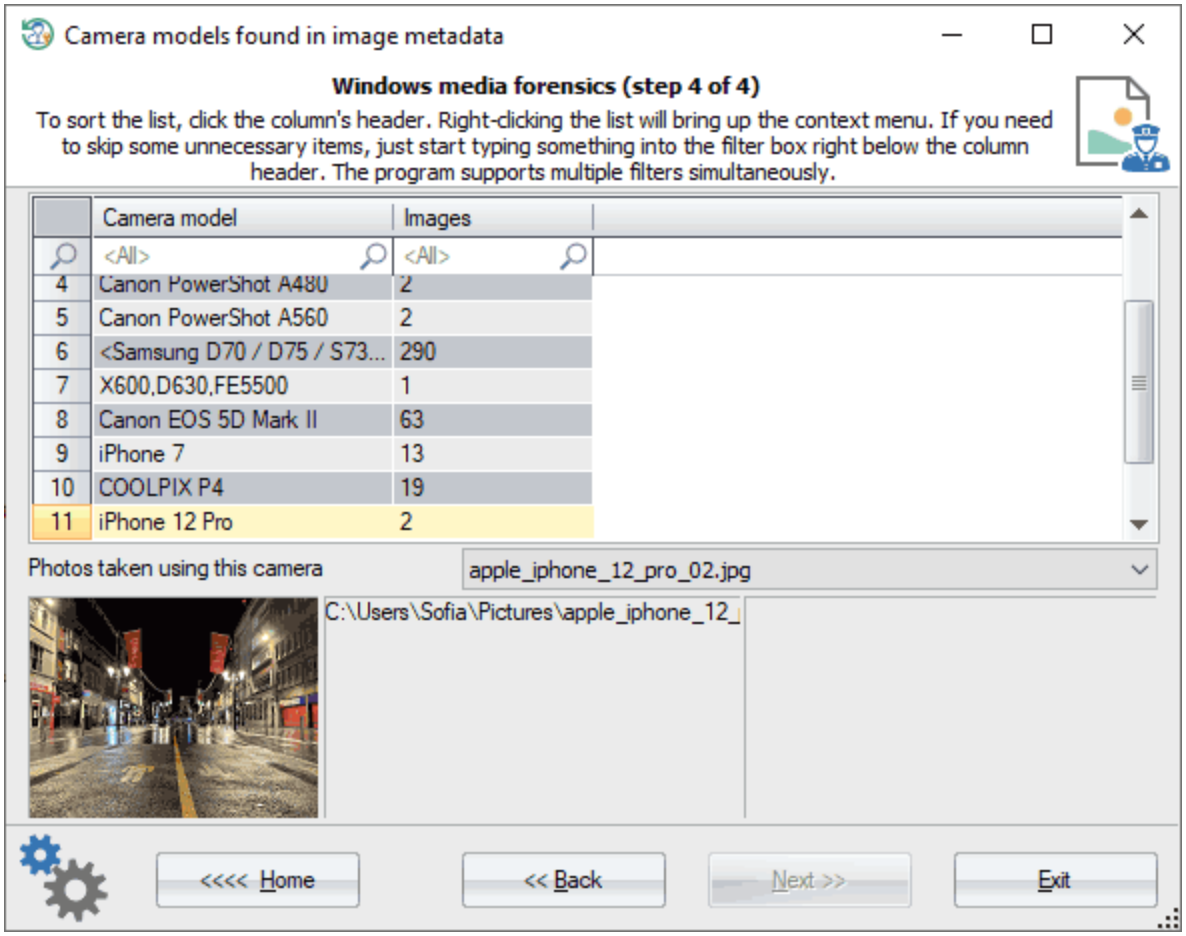
Отчет о **дате съемки** удобен, если вам нужно отобразить время, когда были сделаны снимки, и фотографии за определенную дату.

3.7.3.1.8 Модели камер



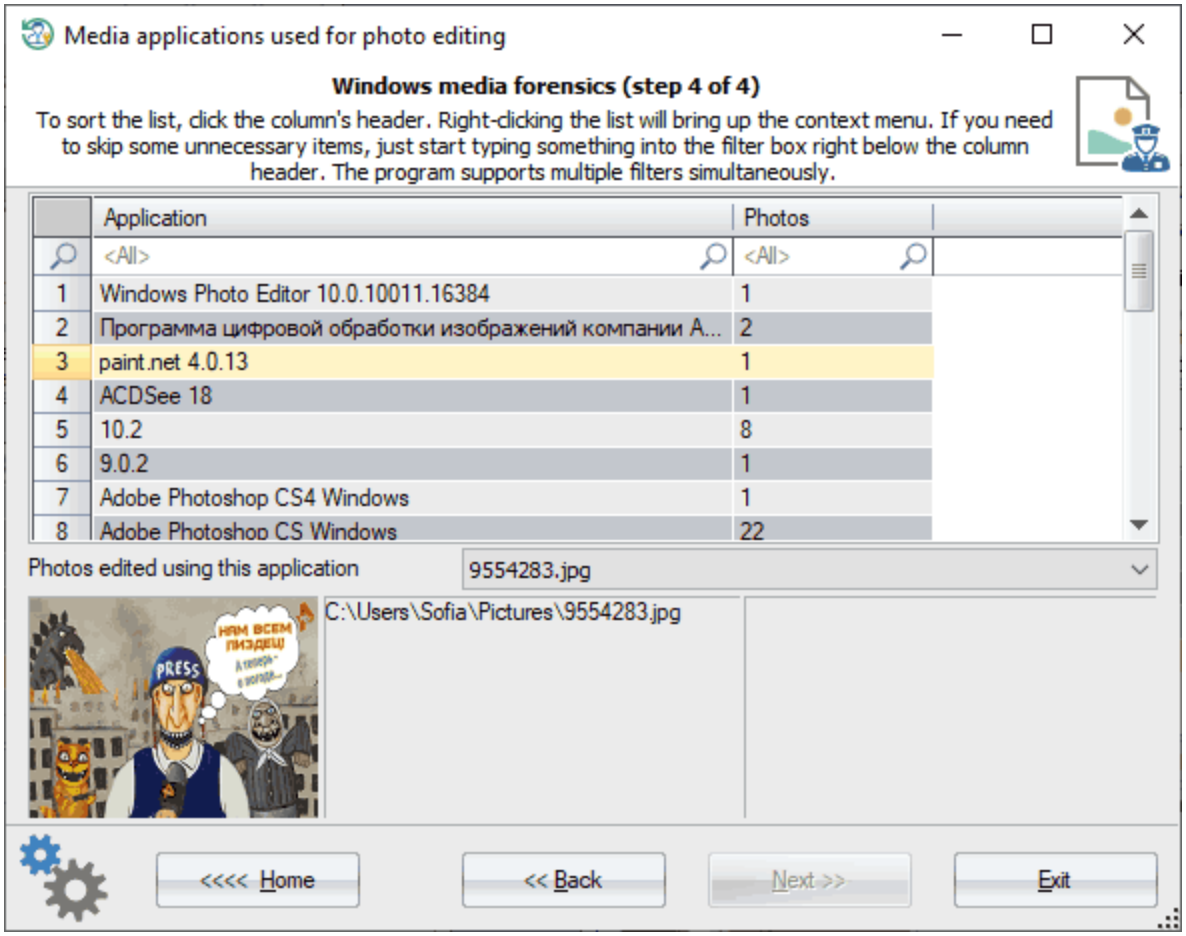
В этом отчете изображения группируются по моделям камер, используемых для съемки.

3.7.3.1.9 Производители камер



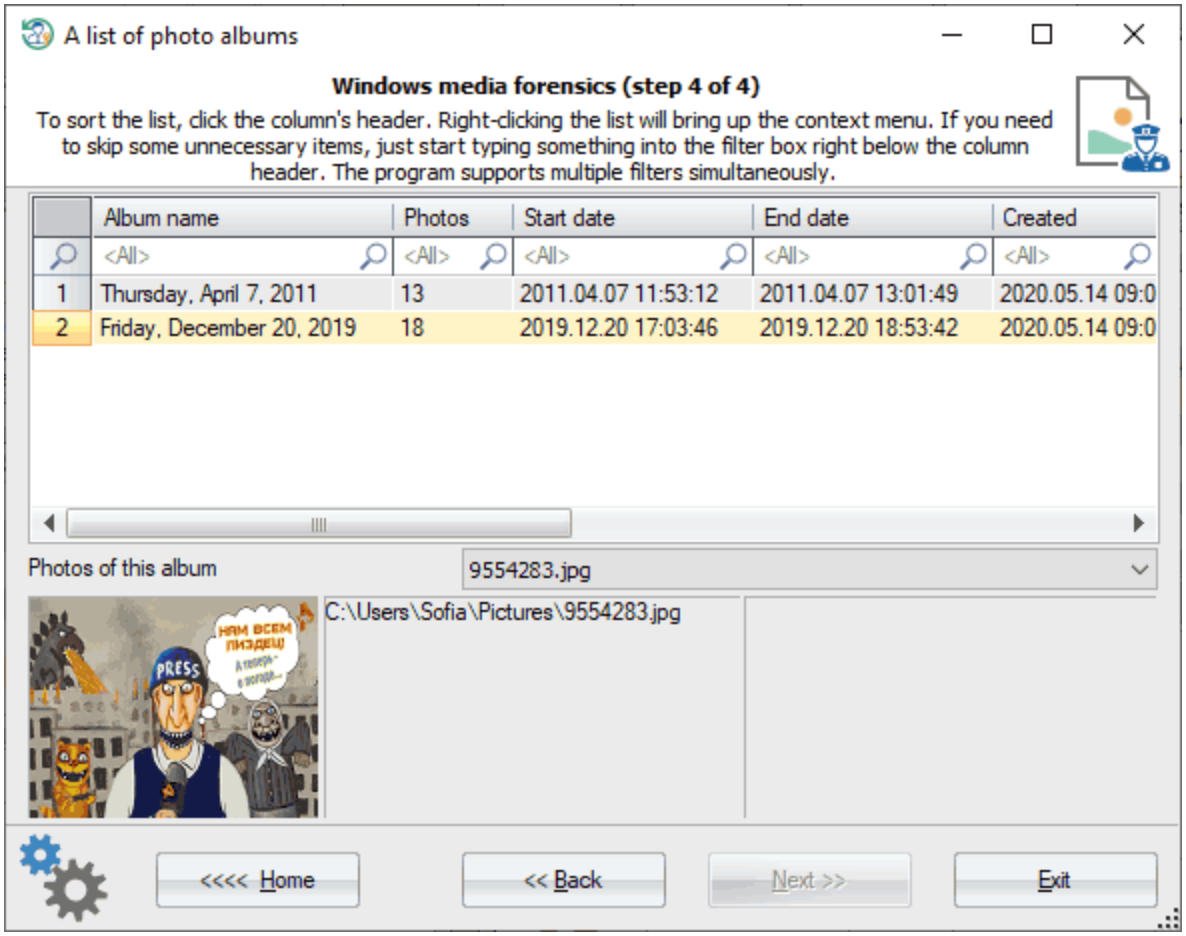
То же, что и в предыдущем отчете, но элементы сгруппированы по производителям камер.

3.7.3.1.10 Мультимедийные приложения



Этот отчет создает список всех найденных программ редактирования мультимедиа и фоторедакторов.

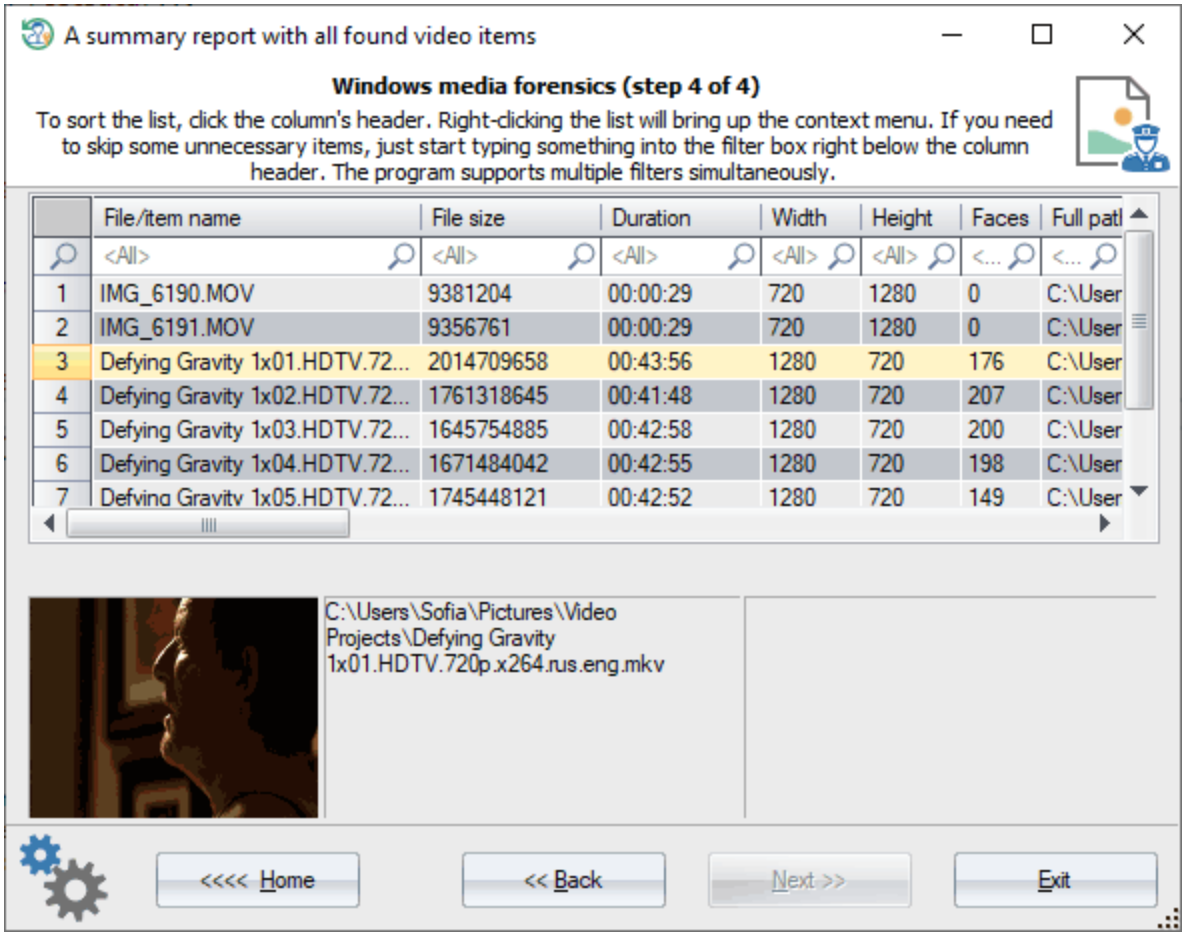
3.7.3.1.11 Альбомы



В этом отчете отображаются альбомы, созданные приложением Windows Photo.

3.7.3.2 Видео библиотека

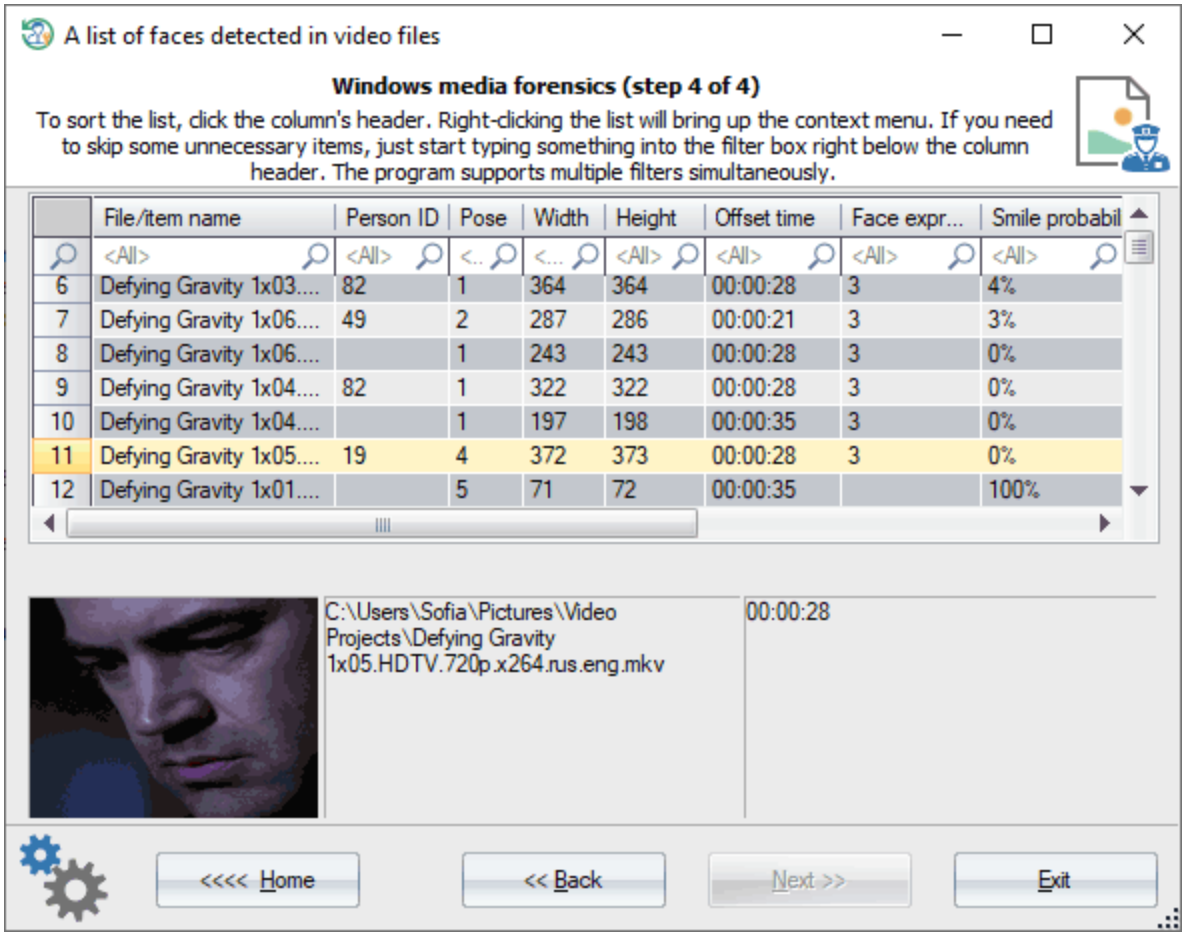
3.7.3.2.1 Видео файлы



Видеоотчет включает в себя общую сводную информацию об элементах видео в фотогалерее Windows. А именно:

- Имя видеофайла
- Размер файла
- Продолжительность видео
- Размер (ширина и высота) видео
- Количество обнаруженных лиц
- Полный путь к файлу
- Автор видео
- Авторское право на видео
- Заголовок видео
- Путь к дубликату, если он найден
- Дата производства или монтирования
- Время создания/изменения/редактирования
- Время последнего просмотра в библиотеке
- Название альбома, к которому принадлежит это видео

3.7.3.2.2 Лица

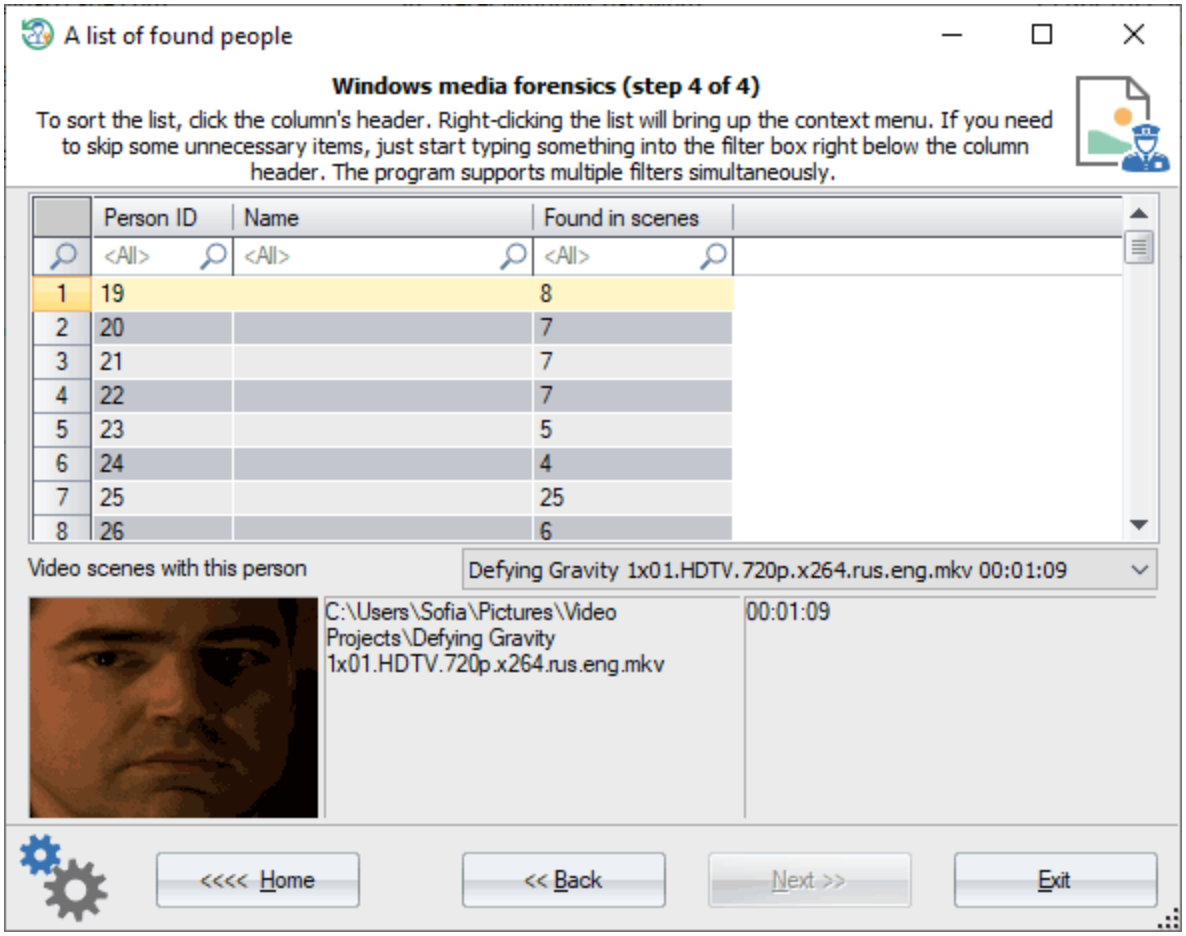


Этот отчет извлекает информацию о найденных в видео лицах и отображает их свойства:

- Имя видеофайла в котором найдено лицо
- Идентификатор человека
- Положение лица
- Ширина и высота лица в пикселях
- Время от начала видео, где найдено лицо
- Выражение
- Вероятность улыбки
- Полный путь к видеофайлу

Кликните мышкой на изображении лица, чтобы просмотреть полную сцену, в которой оно было найдено.

3.7.3.2.3 Люди

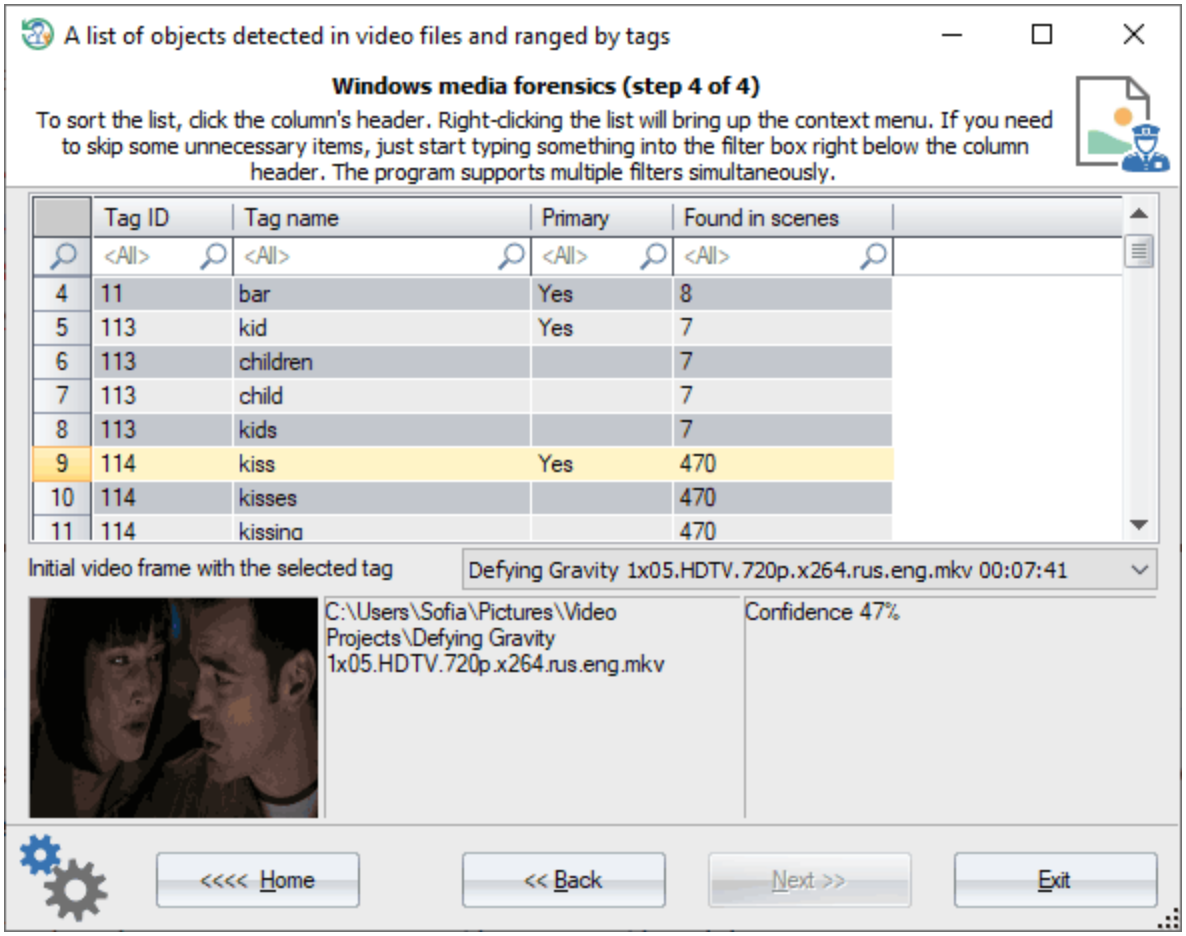


Этот отчет делает тоже самое, что отчет для идентификации людей на фотографиях, за тем лишь исключением, что вместо фотографий используются видеофайлы. В нем всего 3 поля:

- Идентификатор человека
- Имя человека. Отображается пустым, если пользователь не задал его непосредственно.
- Количество сцен, в которых найдено это лицо

Чтобы просмотреть сцены с этим человеком, выделите его в таблице, а затем выберите сцену из выпадающего списка под таблицей.

3.7.3.2.4 Тэги

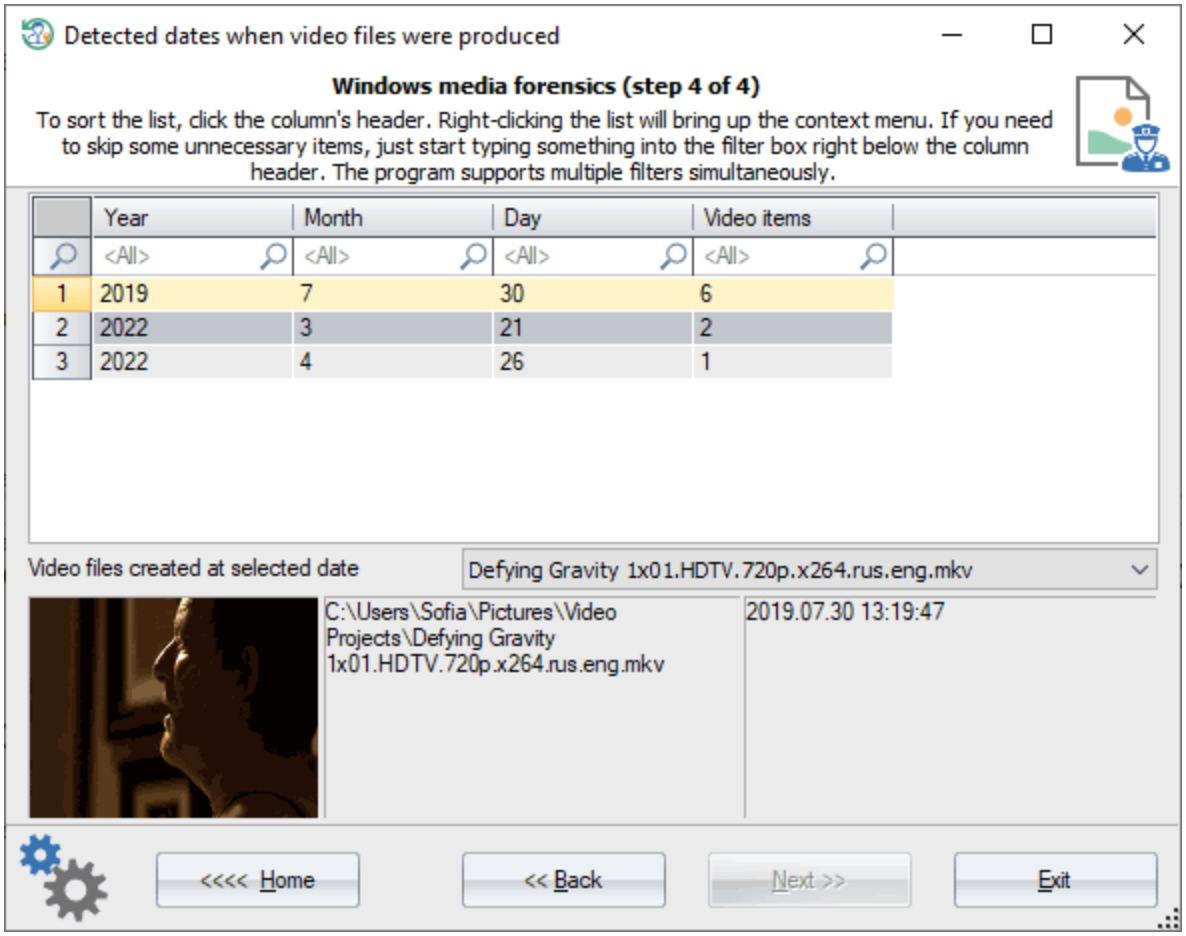


В таблице **тегов** элементы видео группируются по найденным тегам. Каждый тег обладает следующими свойствами:

- Идентификатор тэга
- Наименование тэга
- Основной или вспомогательный
- Количество сцен, в которых он найден

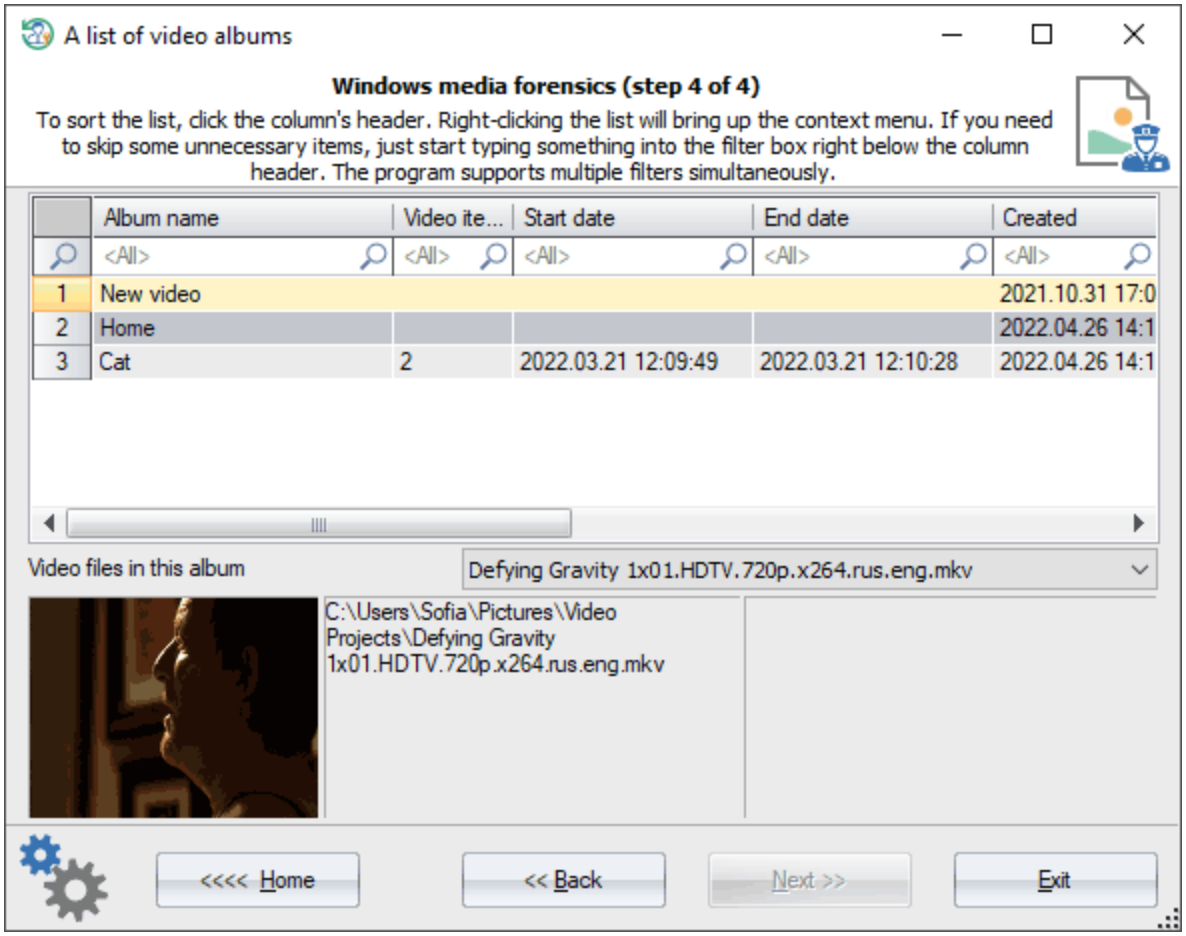
Поле со списком под таблицей содержит список видео со временным смещением, в котором был обнаружен тег. В начале идут сцены с наиболее вероятными совпадениями.

3.7.3.2.5 Даты производства



Отчет о **дате создания** удобен, если вам нужно сгруппировать видео элементы по времени их создания/компиляции.

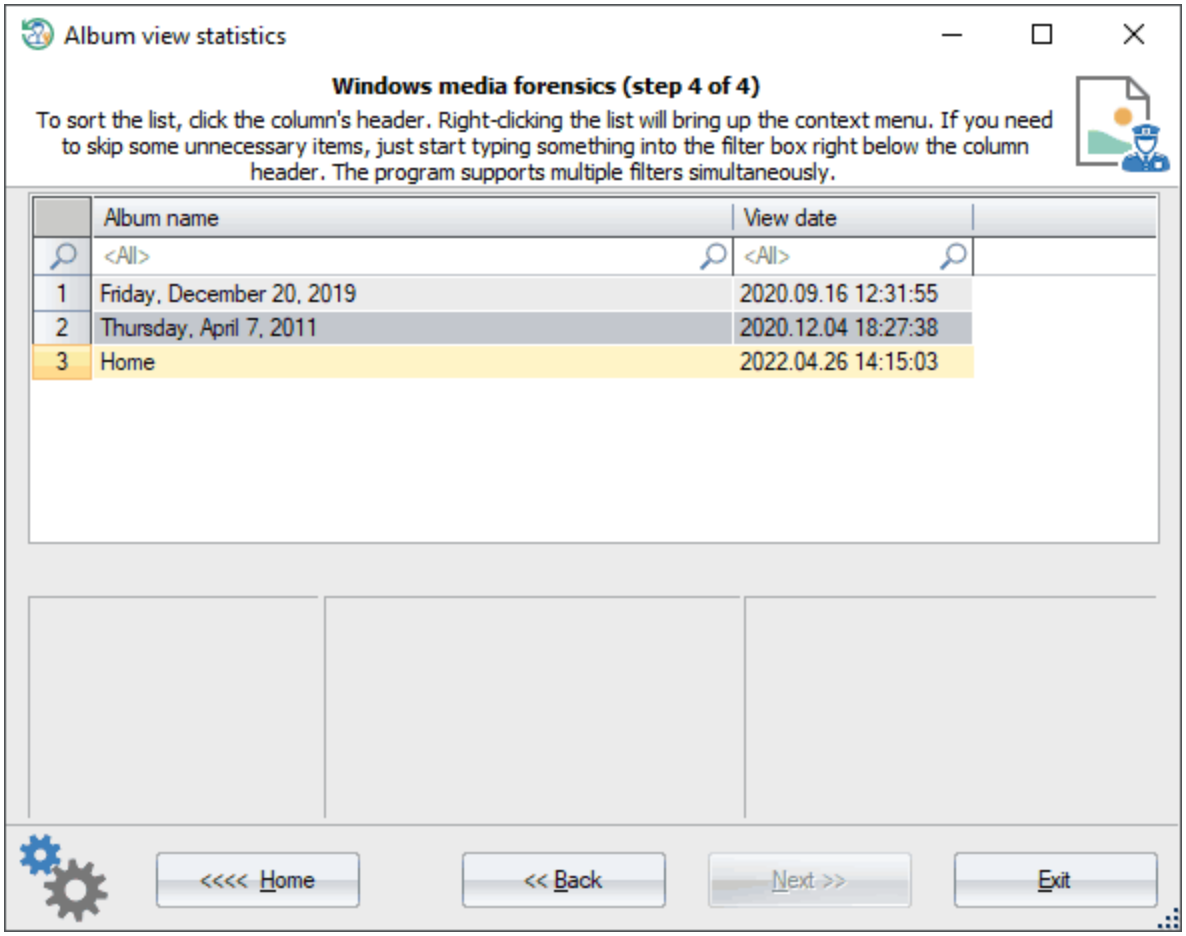
3.7.3.2.6 Альбомы



В этом отчете отображаются видеоальбомы, созданные в приложении Windows Photo.

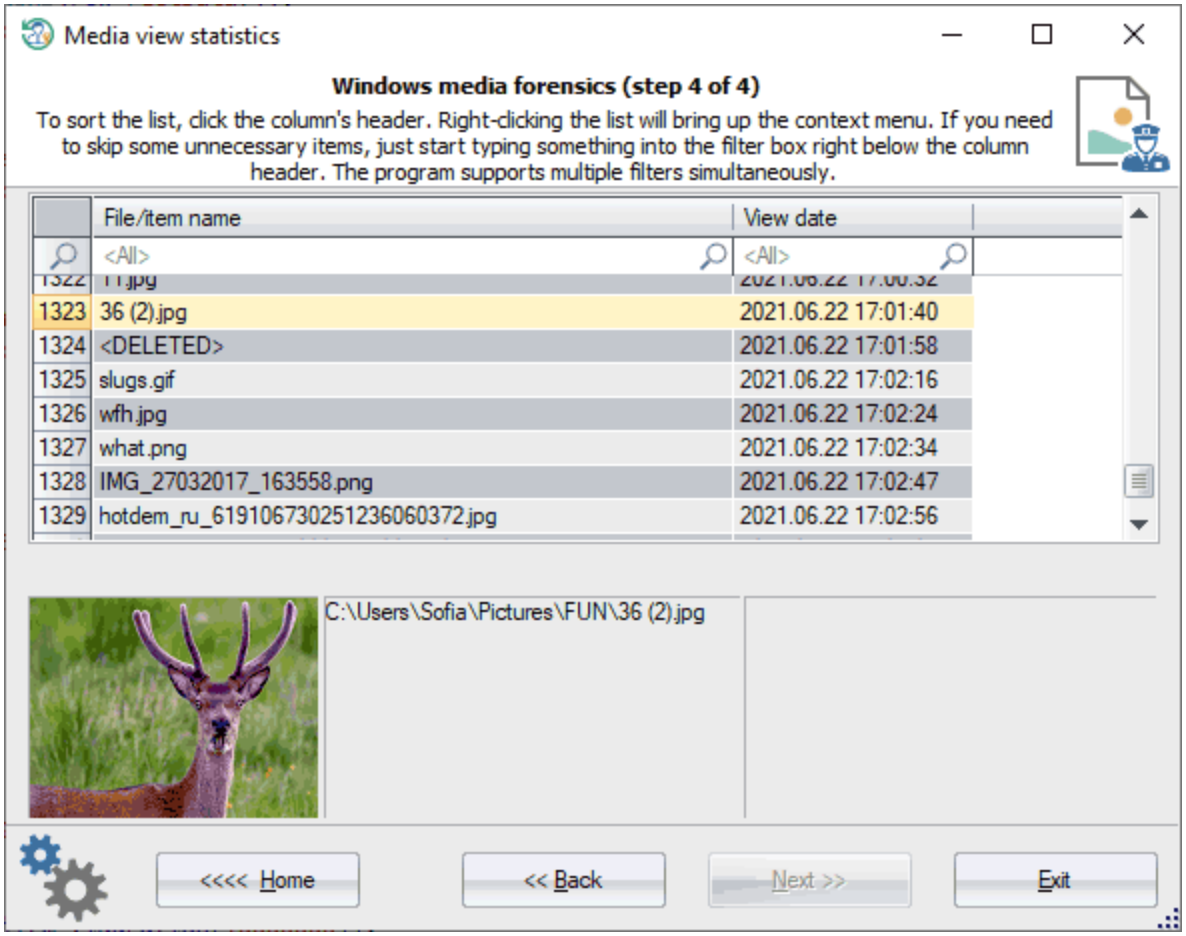
3.7.3.3 Действия пользователя в медиа библиотеке

3.7.3.3.1 Просмотры альбомов



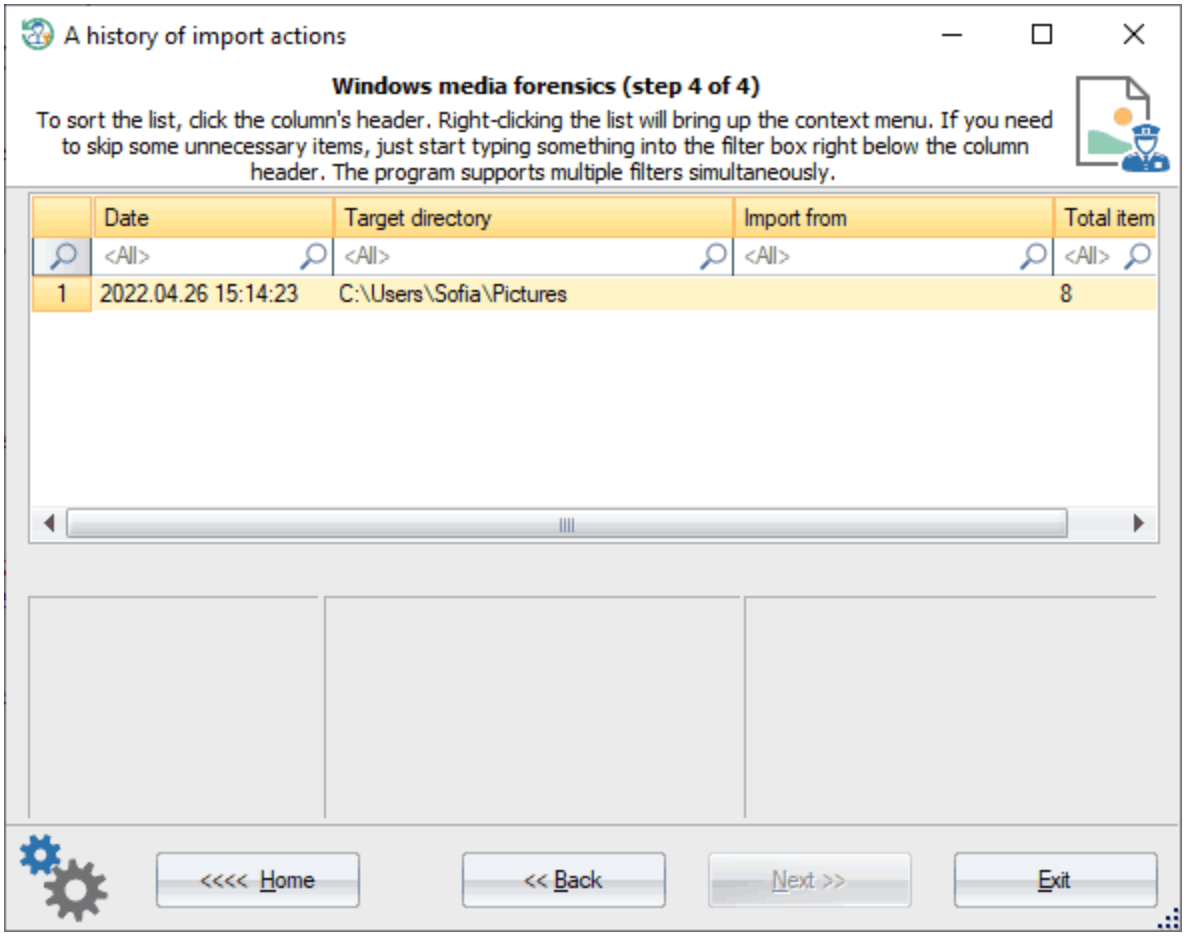
Статистика просмотра по фото- и видео-альбомам.

3.7.3.3.2 Просмотры файлов



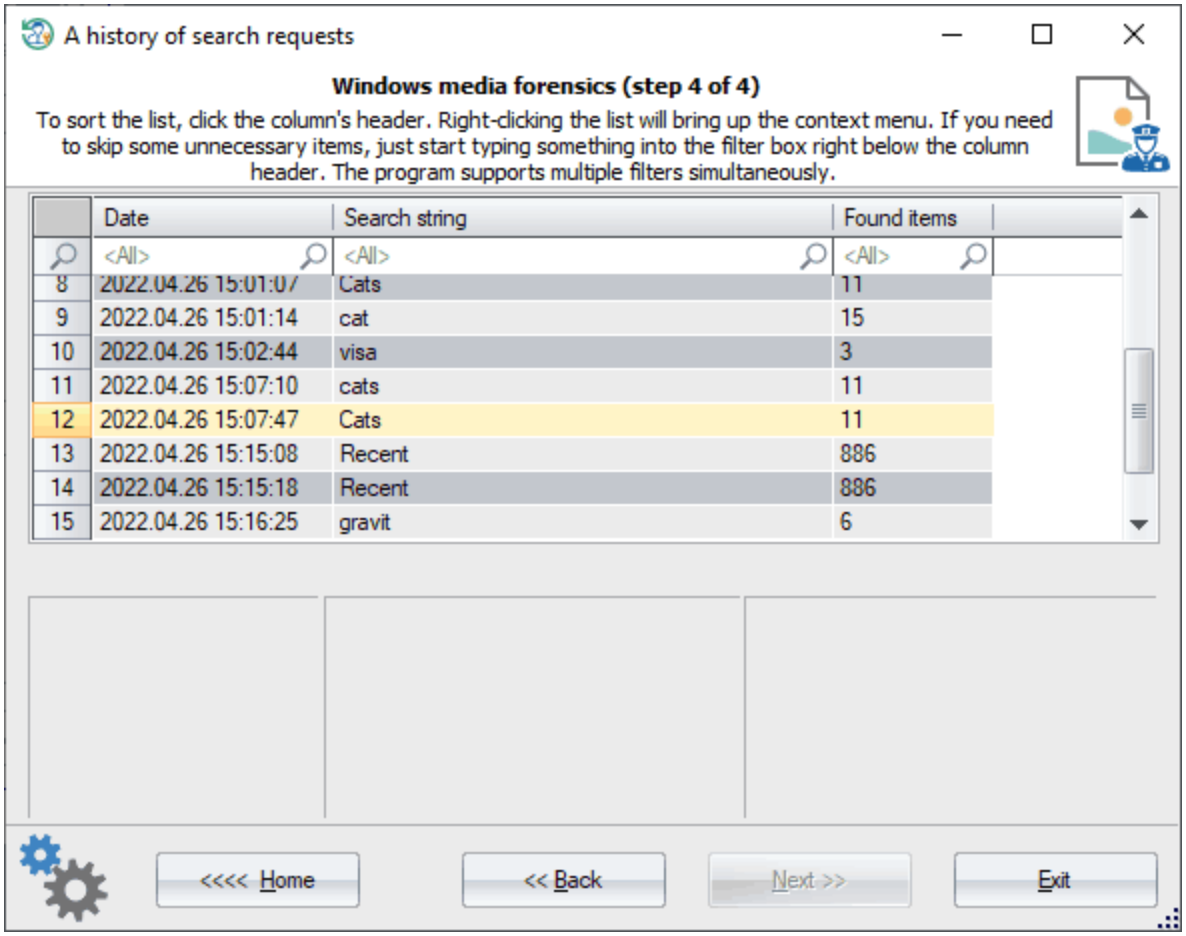
Статистика просмотров фото- и видео-файлов в библиотеке фотографий Windows.

3.7.3.3.3 История импорта



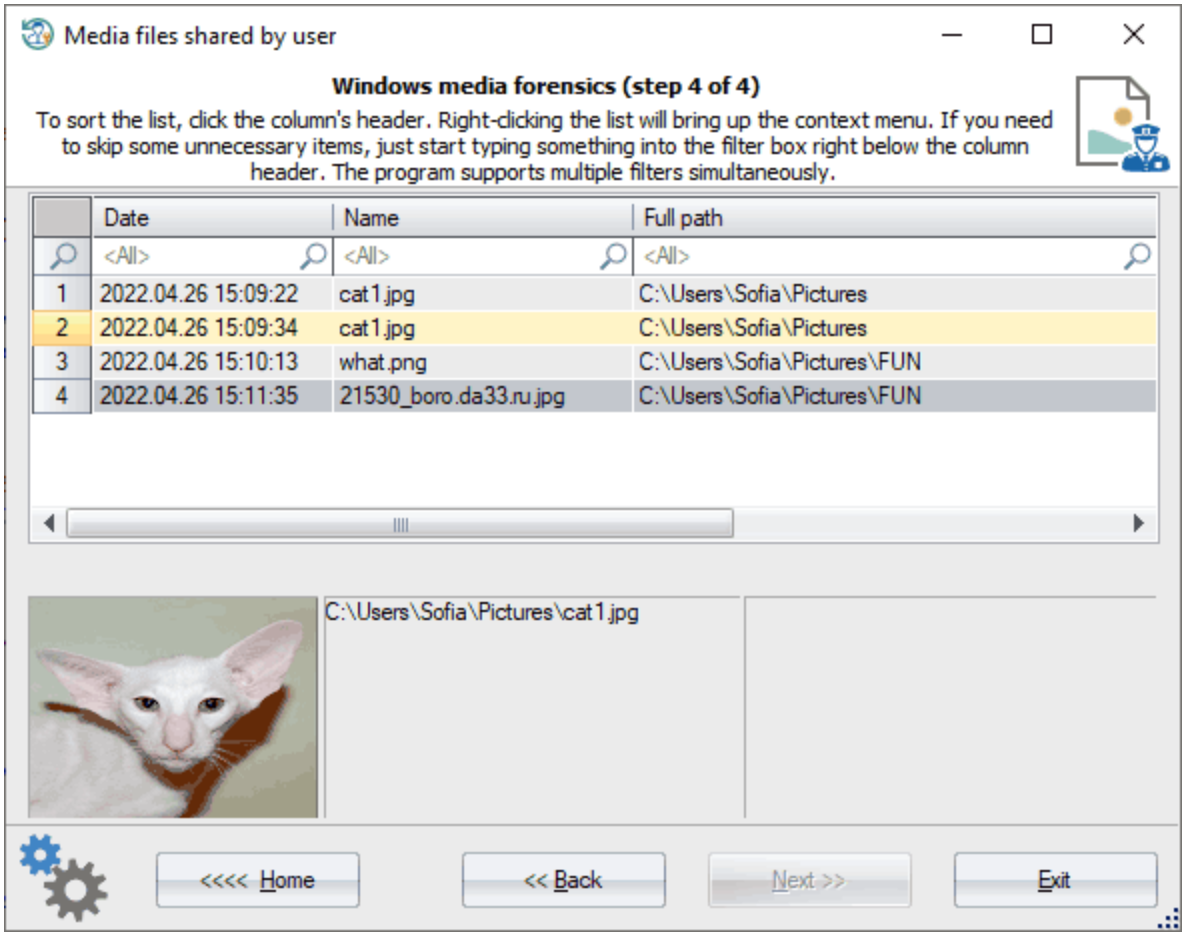
История операций импорта в библиотеке фотографий Windows.

3.7.3.3.4 История поиска



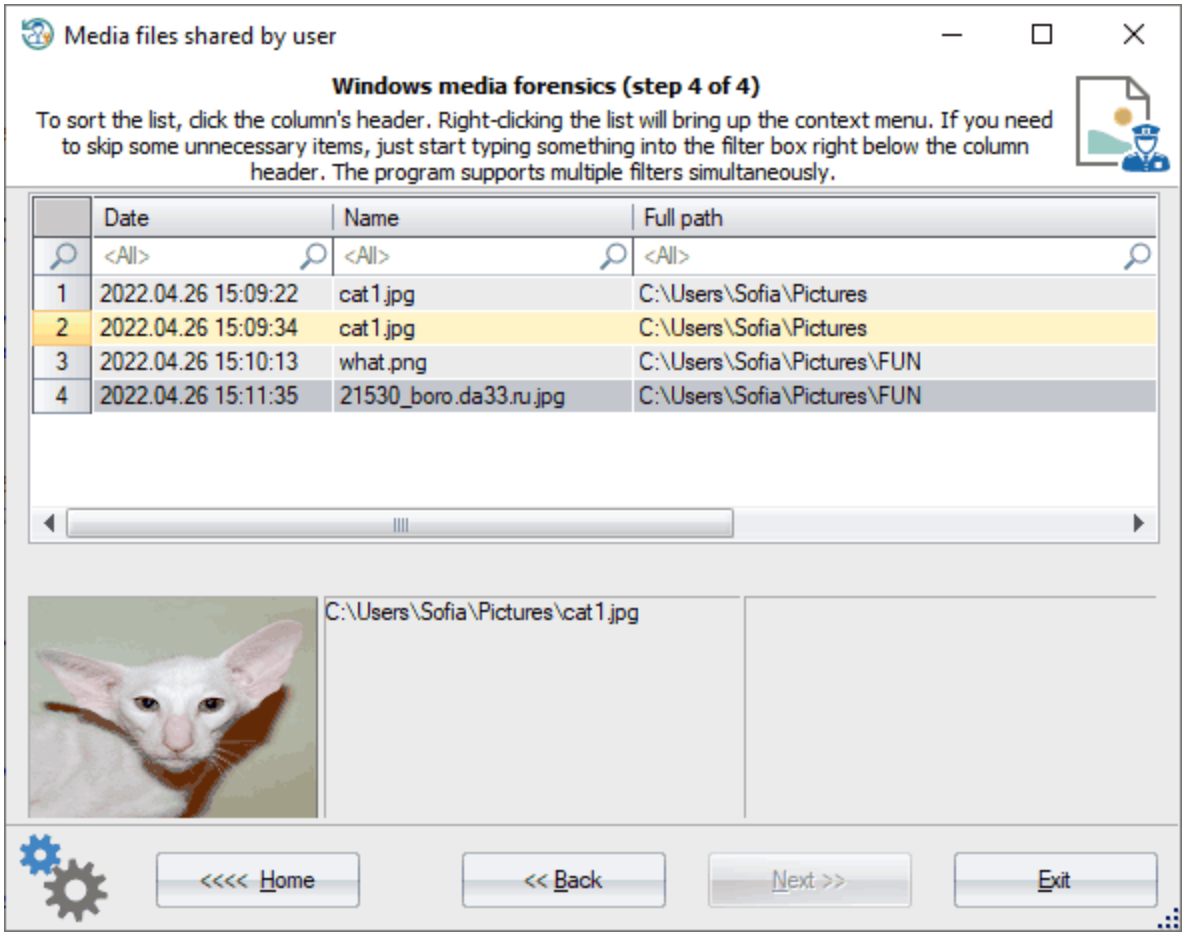
История поисковых запросов в Windows Photo.

3.7.3.3.5 Выложенные данные



История элементов, которыми пользователь поделился из библиотеки фотографий Windows.

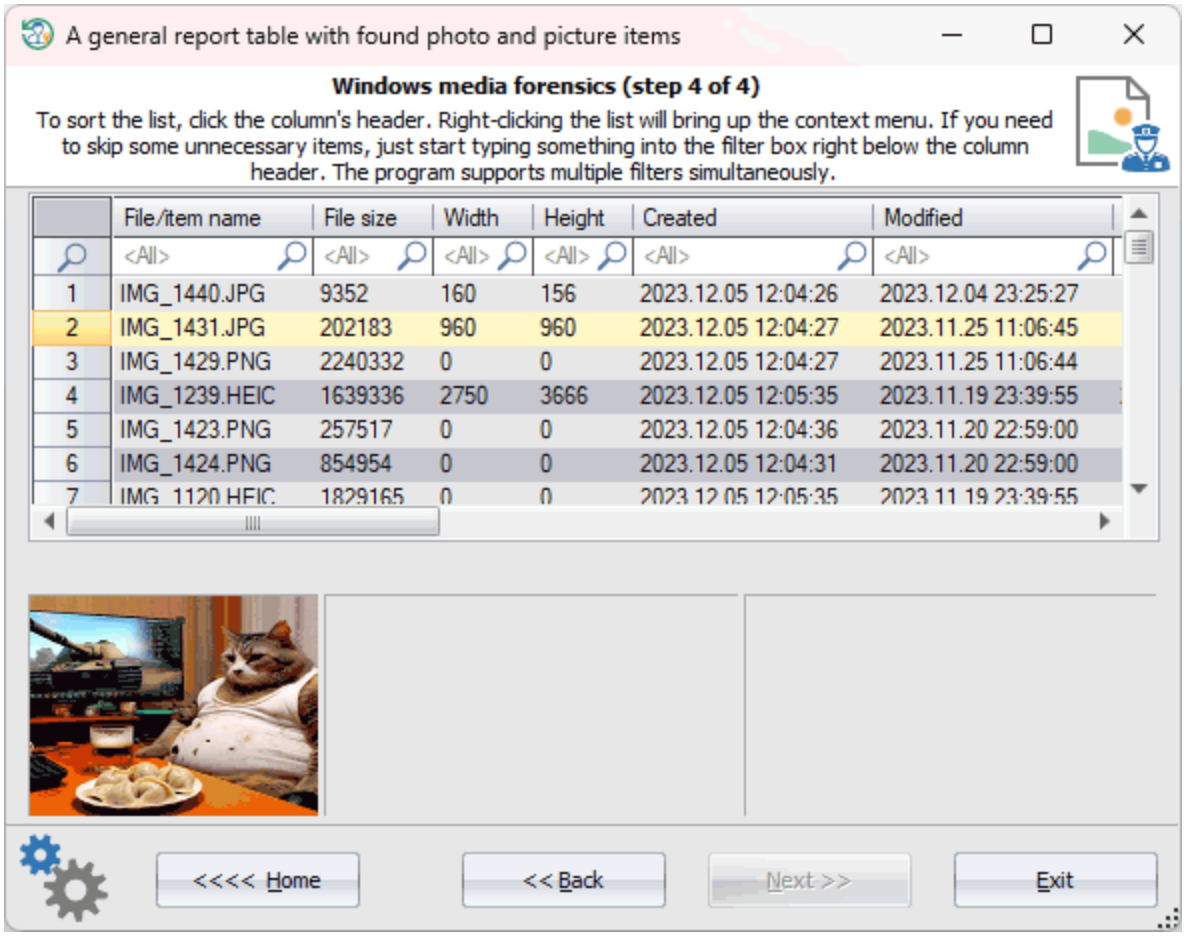
3.7.3.3.6 История печати



История элементов, напечатанных пользователем в библиотеке фотографий Windows.

3.7.3.4 Фото библиотека

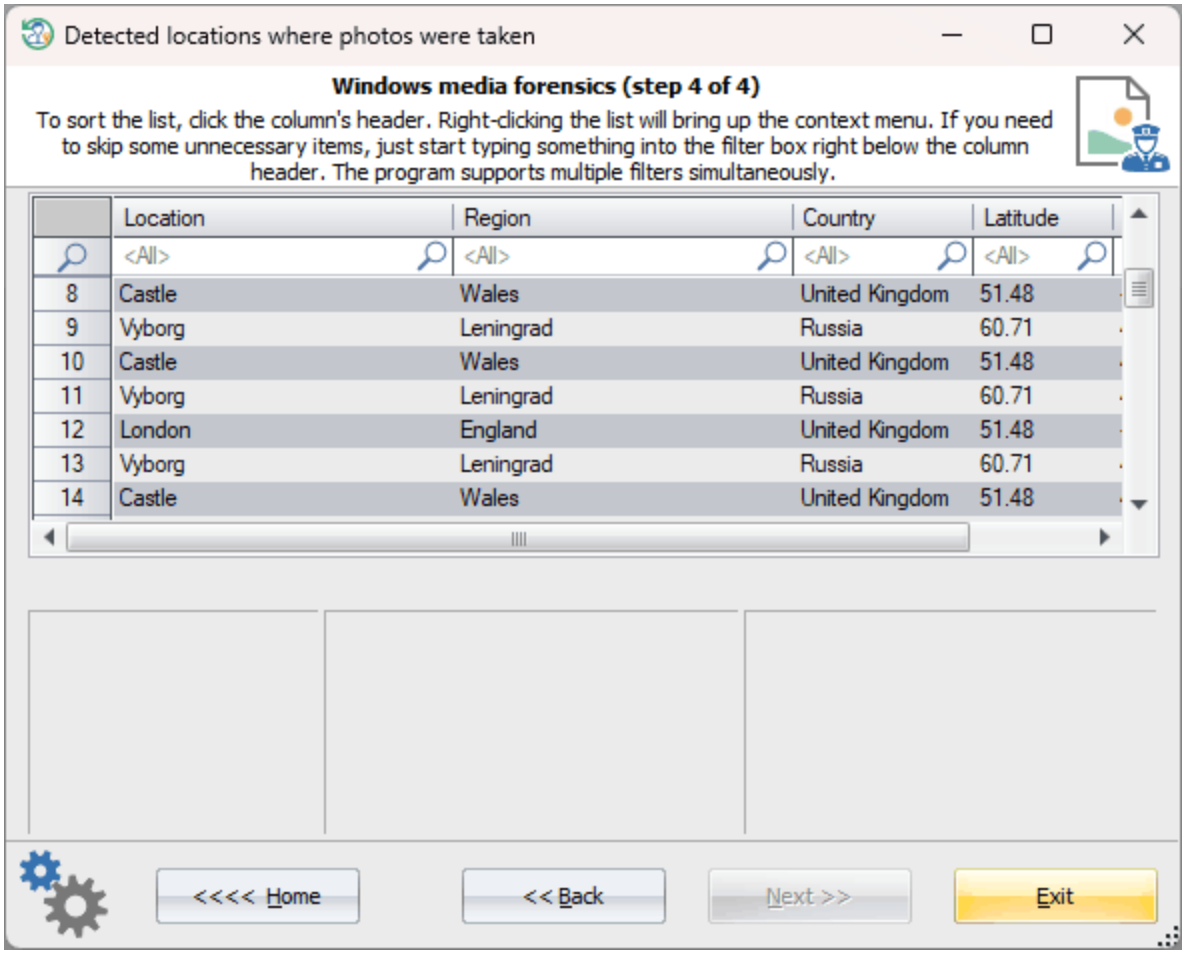
3.7.3.4.1 Изображения



В этом отчете содержится информация об изображениях, которые хранятся в программе **Photos** (Операционные Системы Windows 10 и новее):

- Имя файла
- Размер файла
- Ширина изображения
- Высота изображения
- Дата создания и последнего изменения
- Когда сделана фотография
- Время добавления в библиотеку
- Координаты широты
- Координаты долготы
- Тестовые тэги, если есть

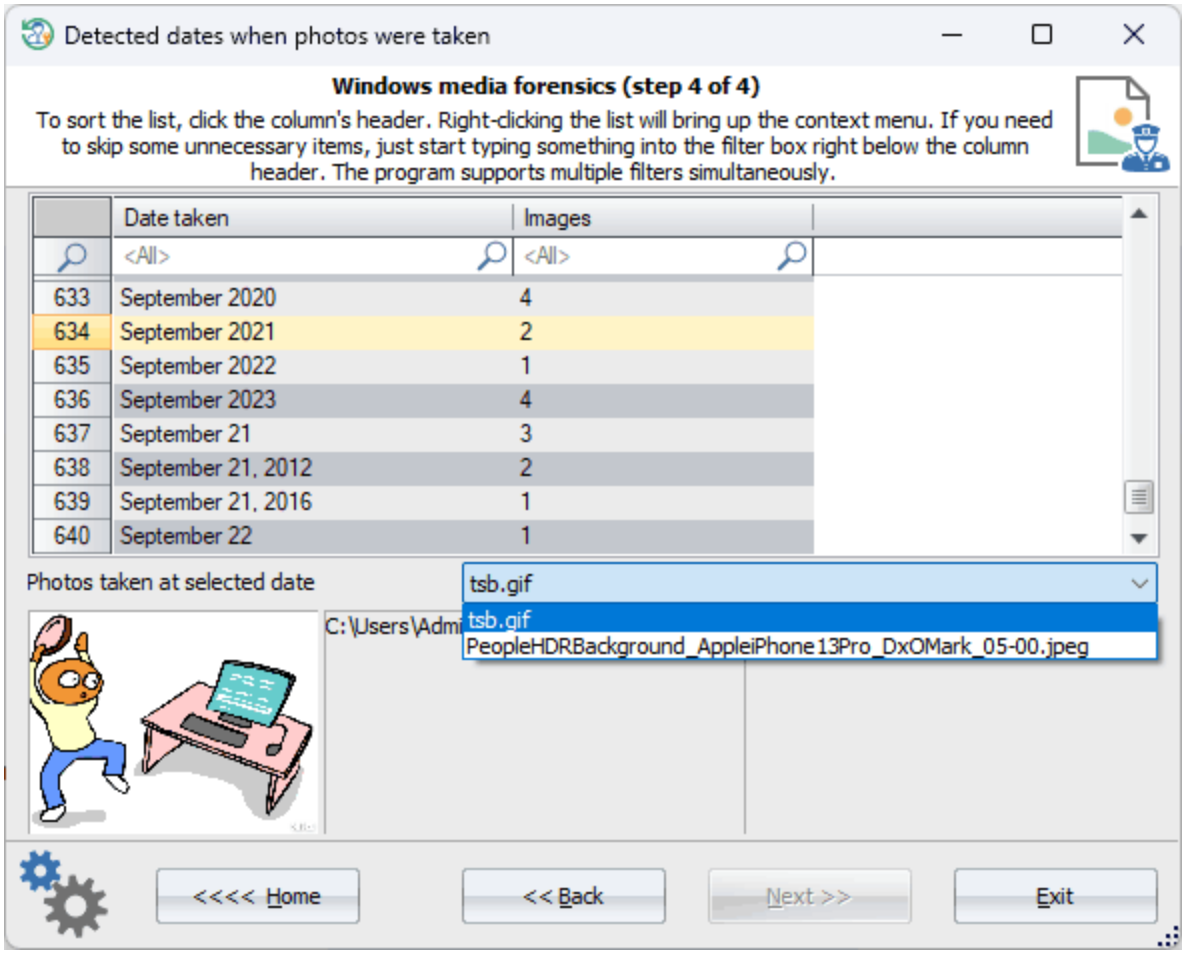
3.7.3.4.2 Места



Большинство мобильных устройств хранят метаданные о местоположении, где были сделаны фотографии. Если такая информация имеется, то она будет отображена в данной таблице, а именно:

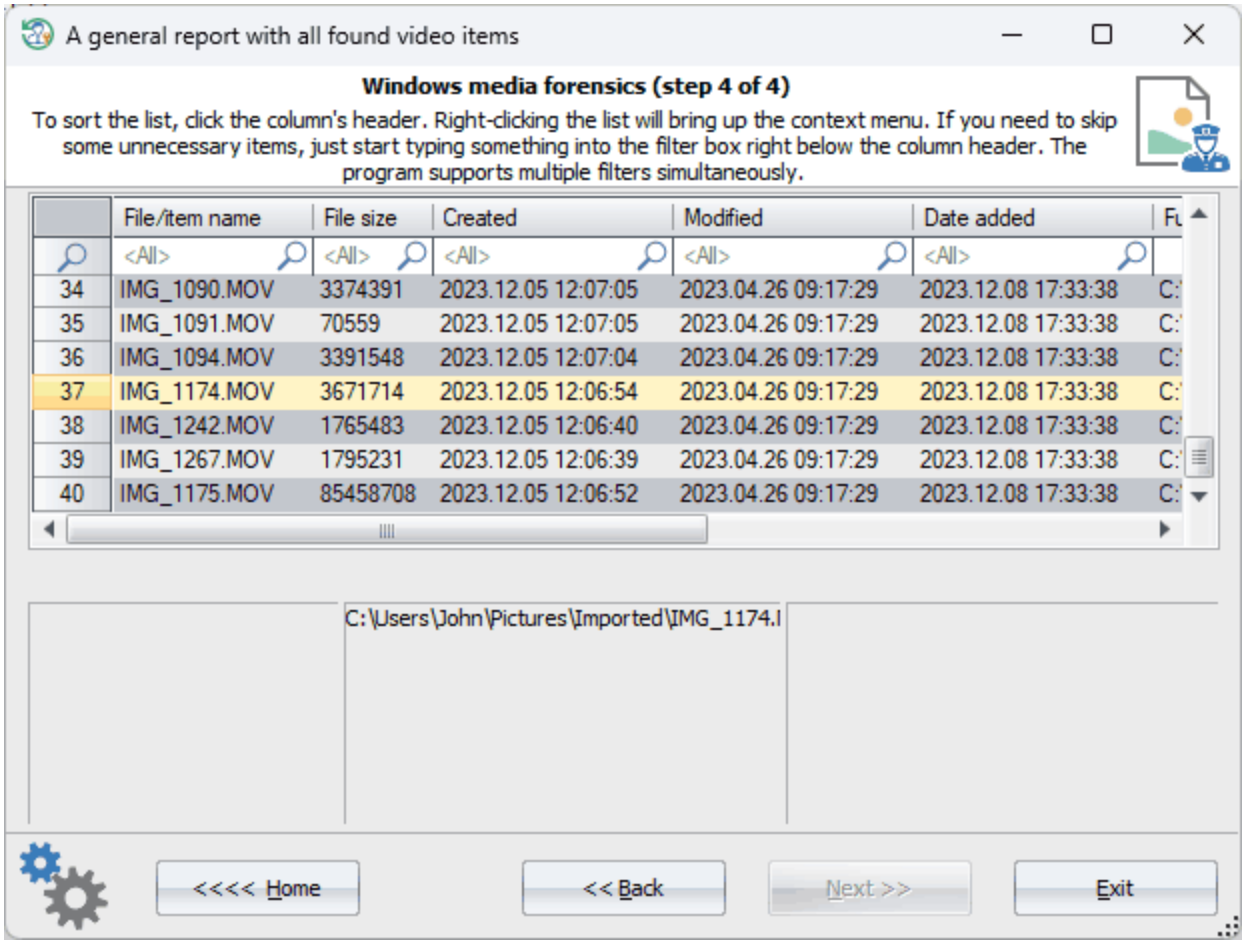
- Населенный пункт
- Регион
- Страна
- Точная широта
- Точная долгота

3.7.3.4.3 Даты созданий



Удобная группировка фотографий и изображений по **дате съемки**. В таблице можно выбрать группировку по годам или месяцам и посмотреть, какие фото были сделаны в выбранное время.

3.7.3.4.4 Видео

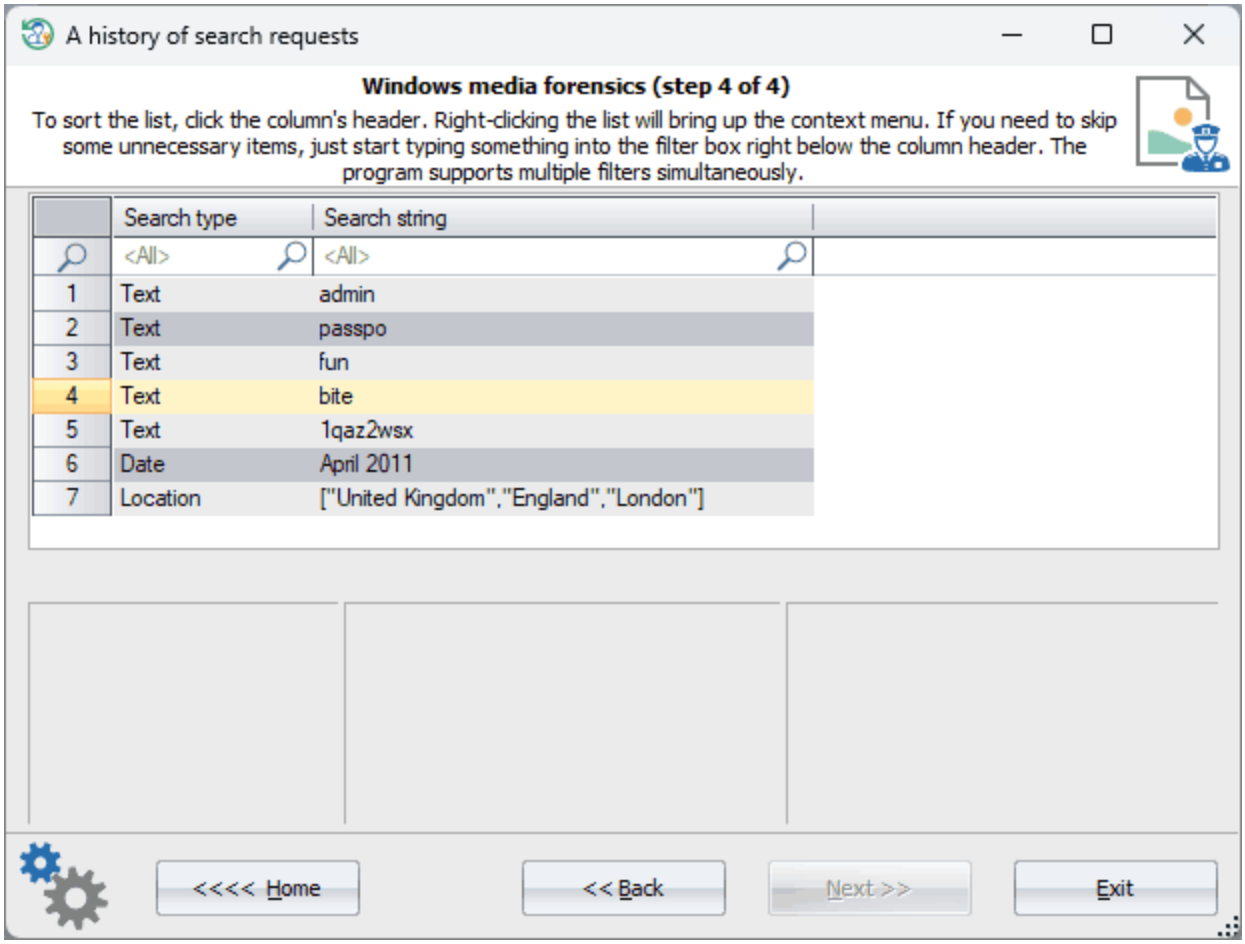


Видео включает в себя информацию о видео элементах, которые хранятся в программе **Photos**. А именно:

- Имя видеофайла
- Размер файла
- Время создания/изменения/редактирования
- Полный путь к файлу
- Продолжительность видео

3.7.3.5 Действия пользователя в фото библиотеке

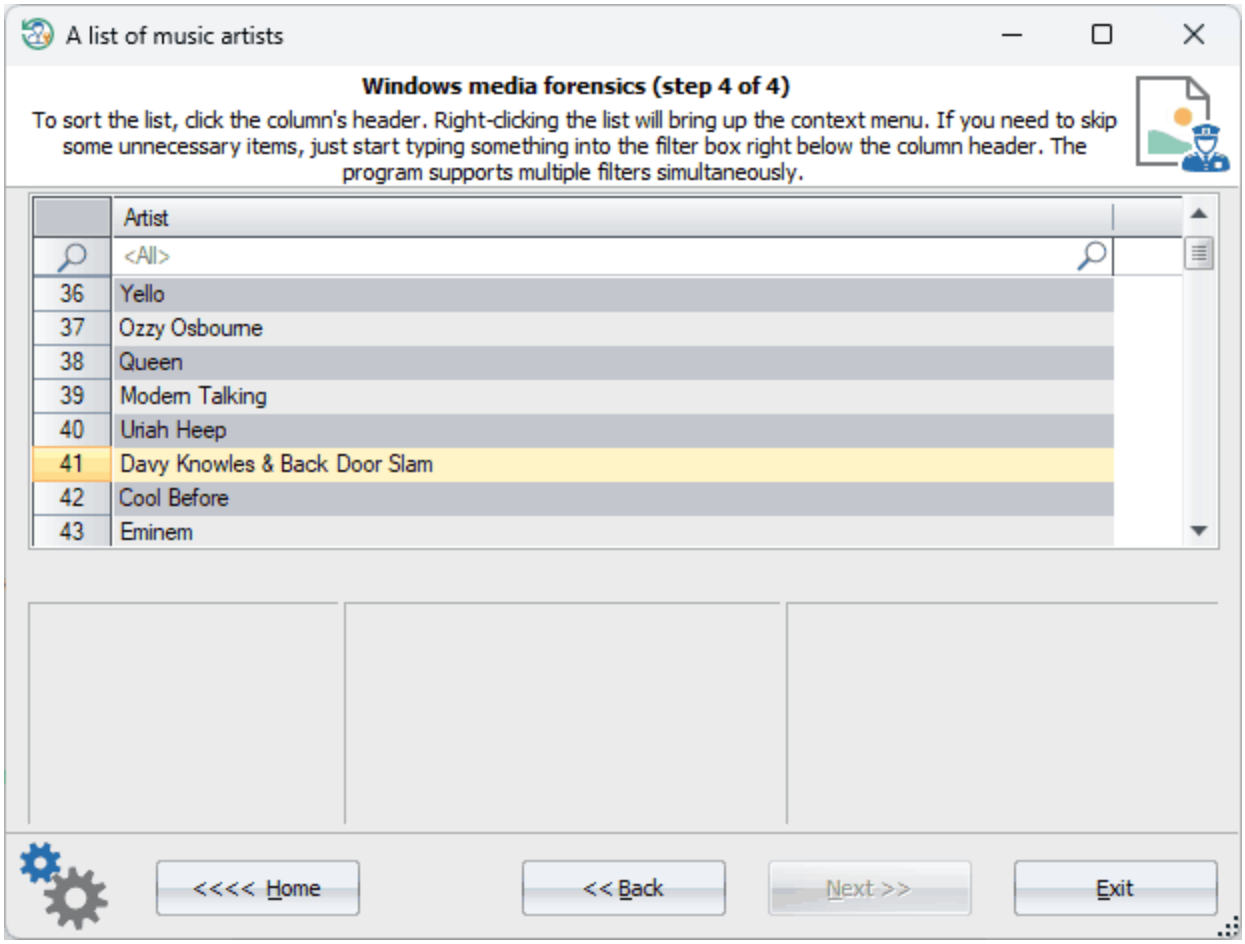
3.7.3.5.1 История поиска



История поисковых запросов в программе **Photos**.

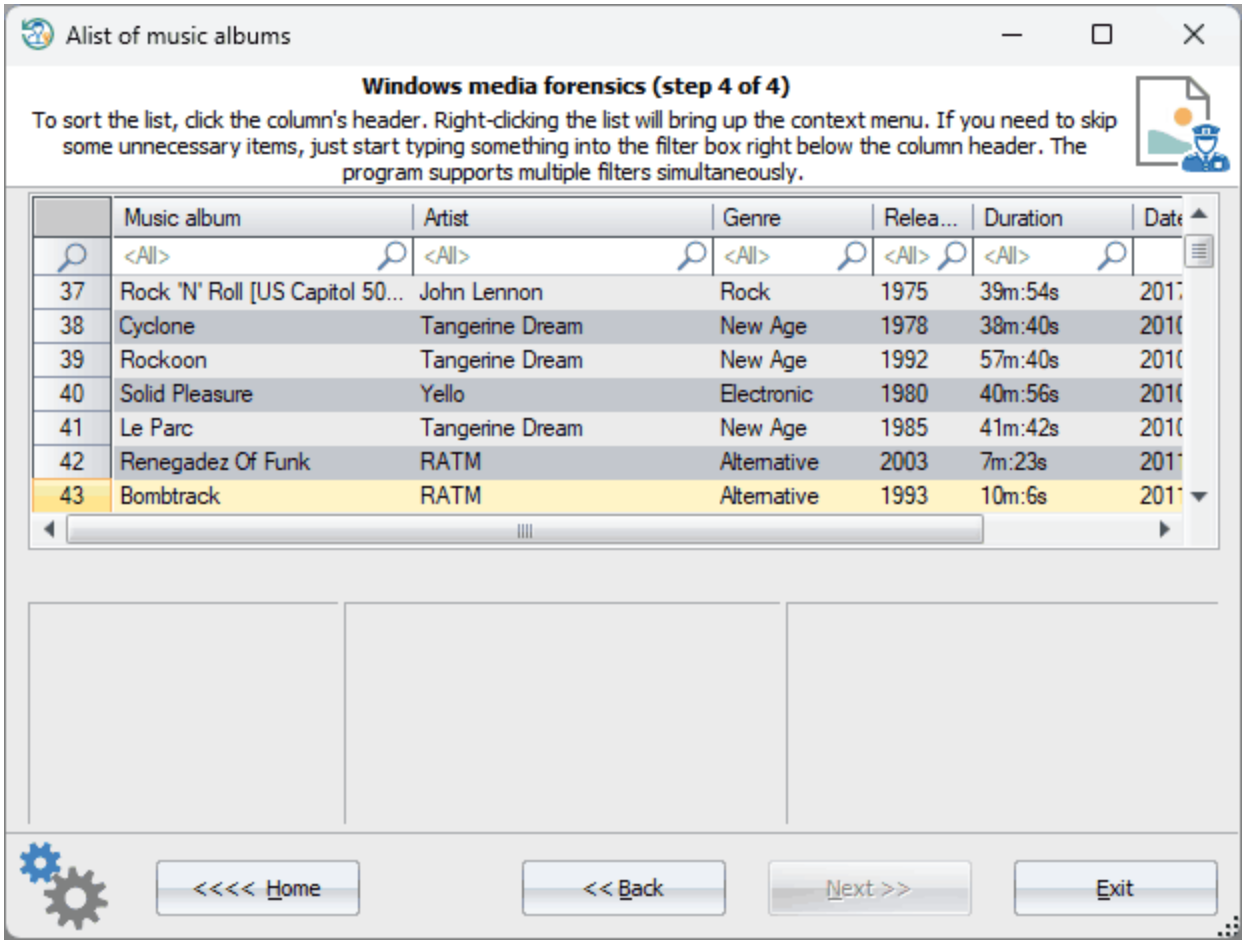
3.7.3.6 Медиа проигрыватель

3.7.3.6.1 Исполнители



Этот отчет содержит список артистов в **Медиа Проигрывателе** (Media Player, не Windows Media Player !).

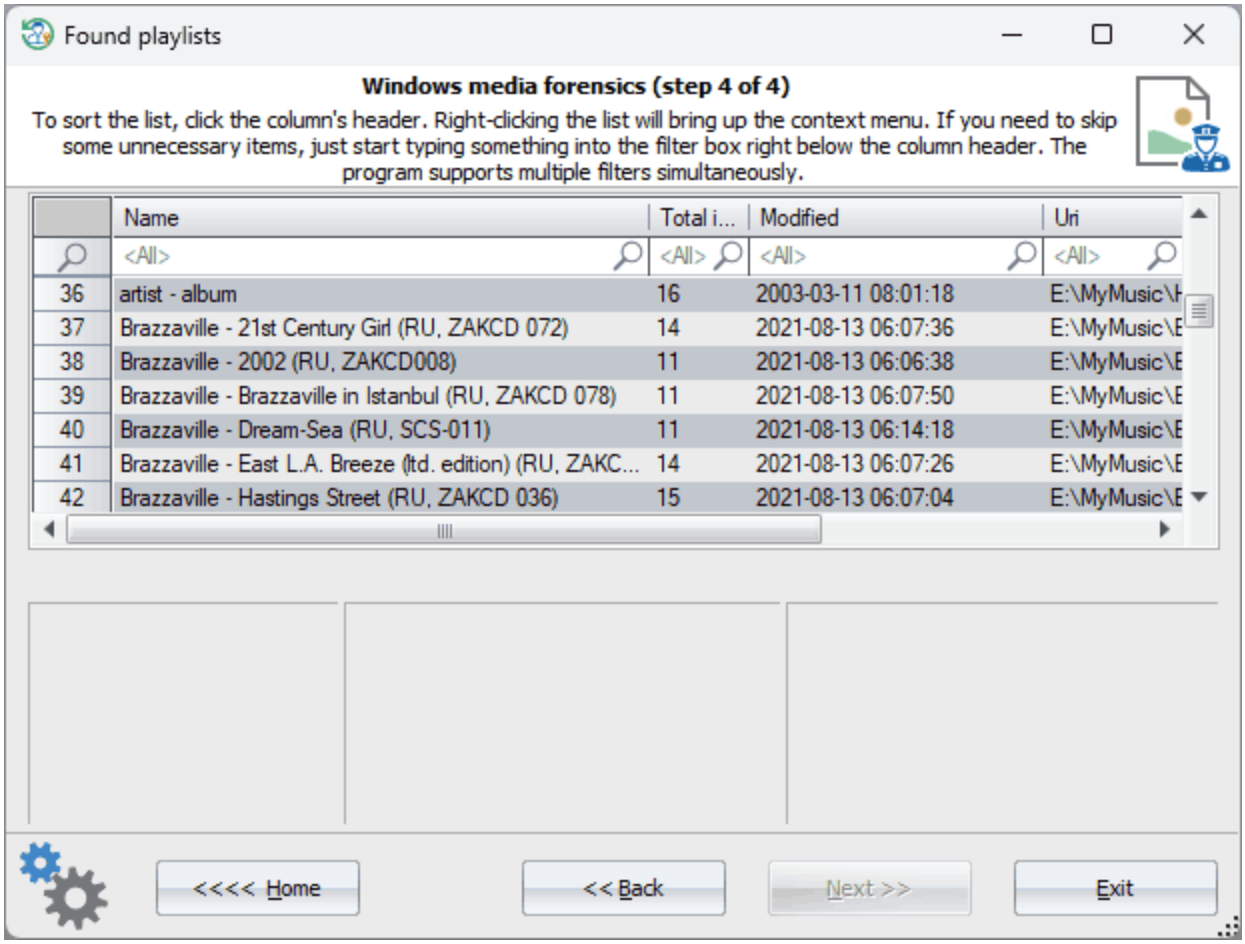
3.7.3.6.2 Альбомы



Полный список всех альбомов, хранящихся в программе **Media Player**. Таблица содержит:

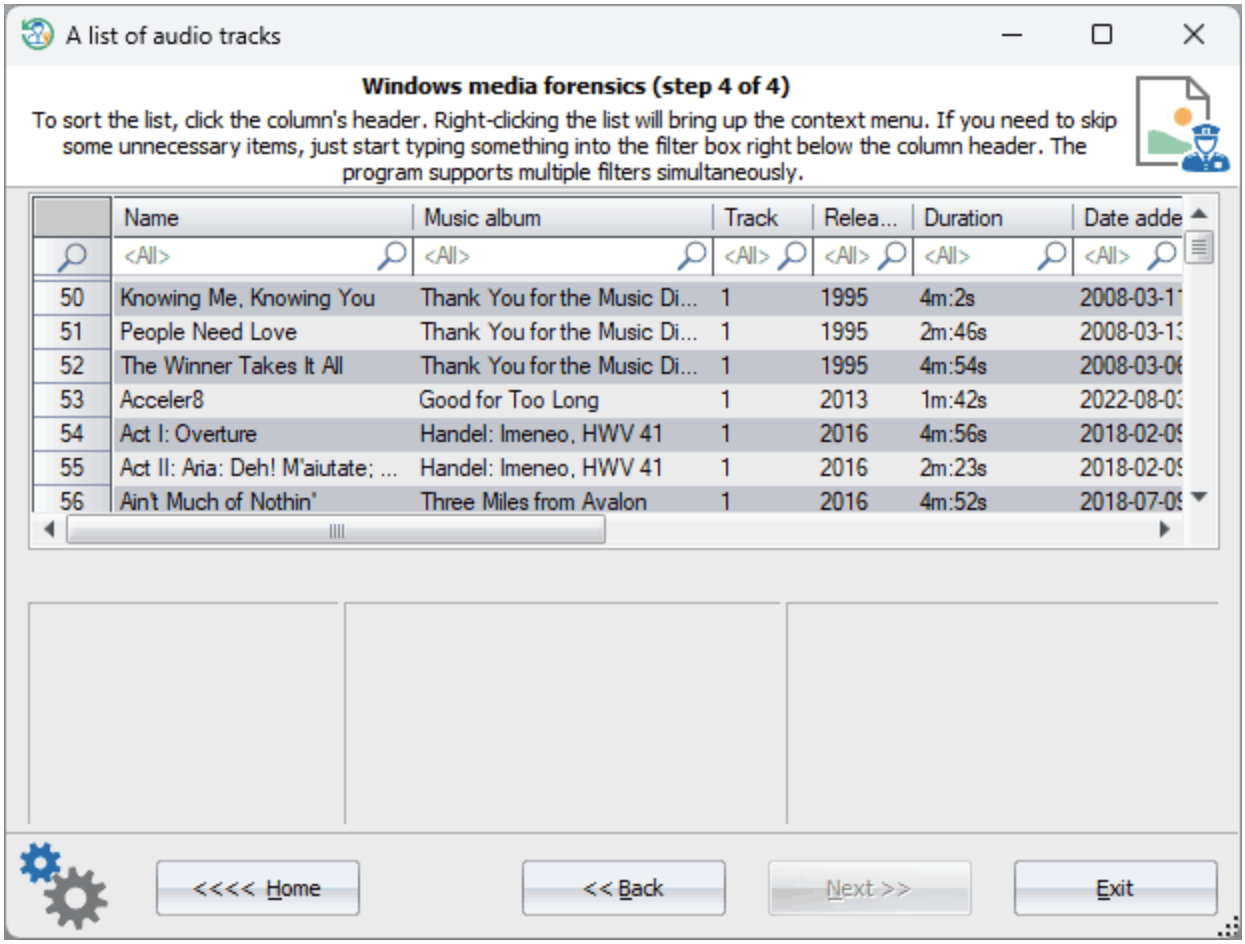
- Имя альбома
- Имя исполнителя
- Музыкальный жанр
- В каком году был релиз
- Общее продолжительность альбома
- Время добавления на компьютер

3.7.3.6.3 Плэйлисты



Список всех плейлистов, хранящихся в **Media Player**.

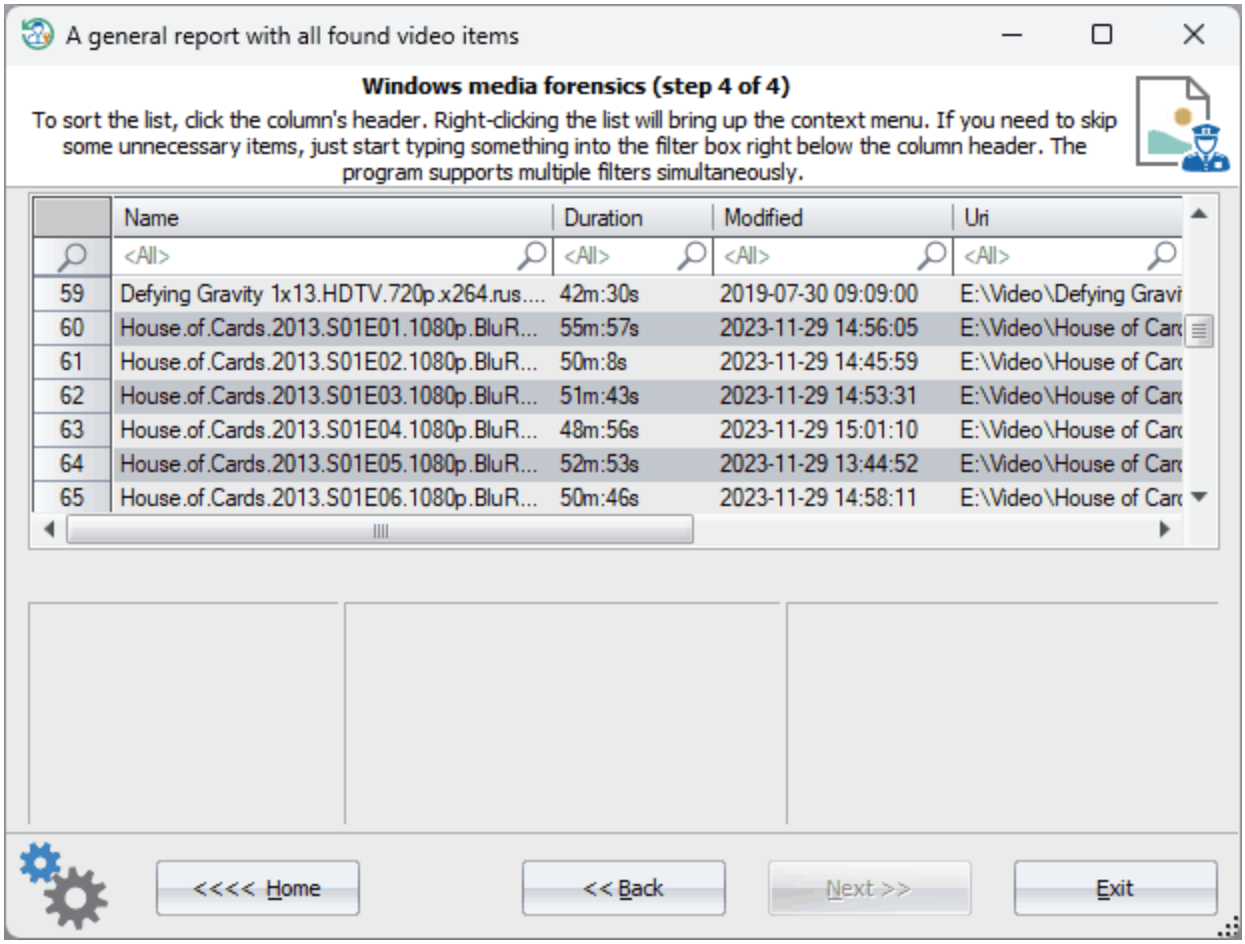
3.7.3.6.4 Аудио дорожки



Аудиодорожки включает в себя следующую информацию:

- Имя трека
- Наименование альбома
- Номер трека в альбоме
- Дата релиза альбома
- Продолжительность трека
- Время добавления на компьютер
- Тип аудио формата
- Полный путь к треку

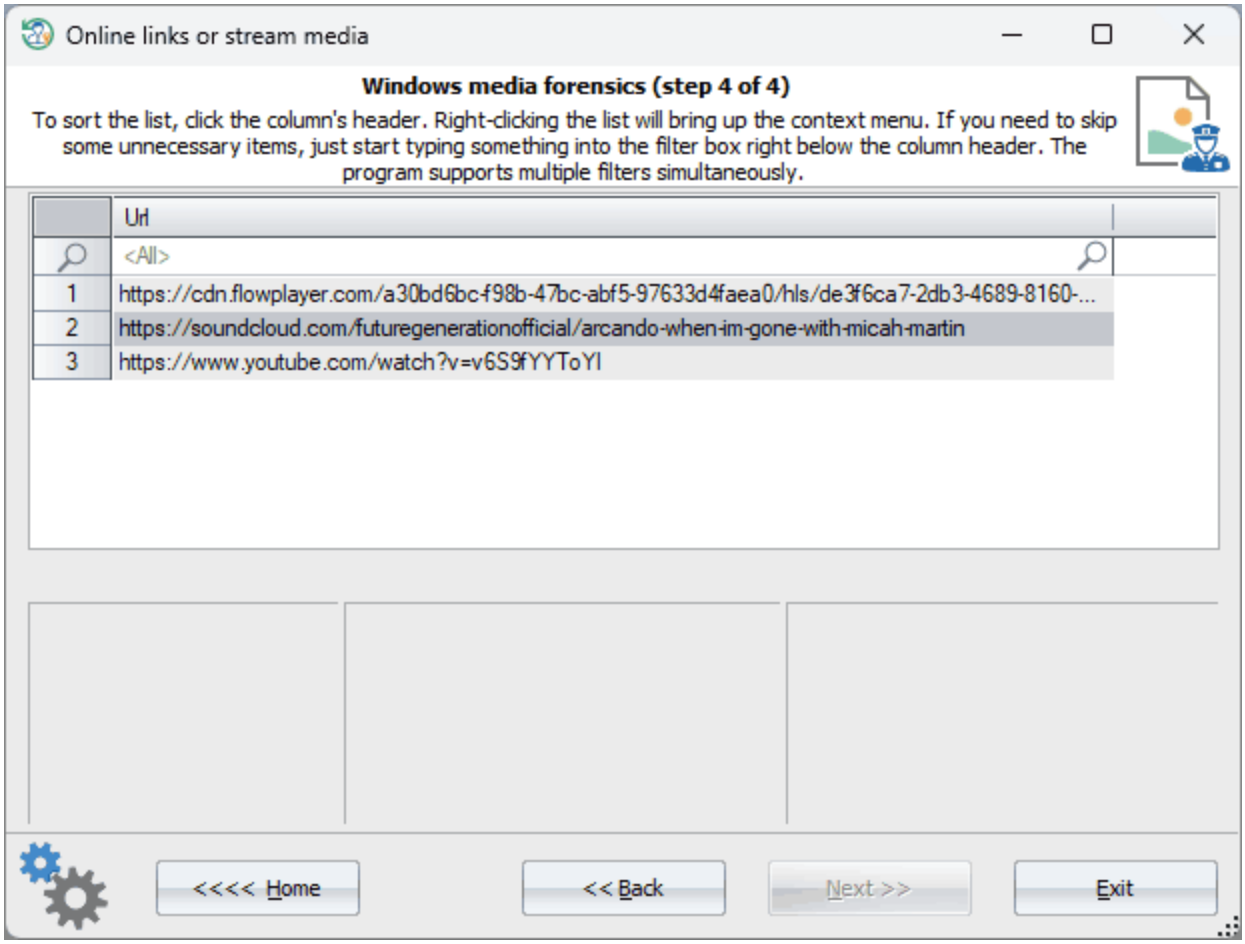
3.7.3.6.5 Видеоматериалы



Видеофайлы включает в себя информацию об элементах видео в программе **Media Player**. А именно:

- Имя видеофайла
- Продолжительность видео
- Время последнего изменения
- Полный путь к файлу

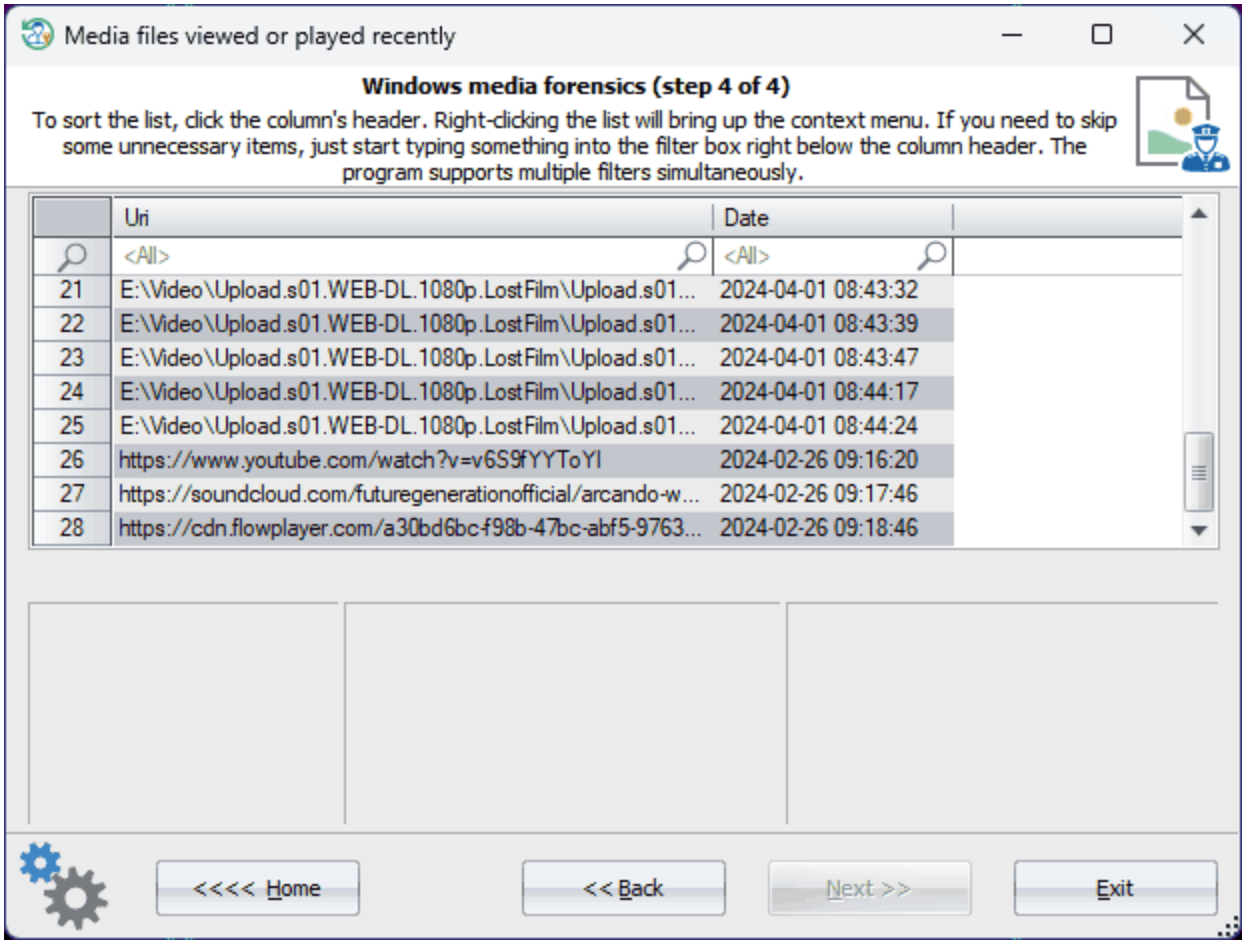
3.7.3.6.6 Онлайн элементы



Данный отчет включает в себя ссылки на онлайн или потоковые видео, которые хранятся в **Media Player**.

3.7.3.7 Действия пользователя в медиа проигрывателе

3.7.3.7.1 История файлов



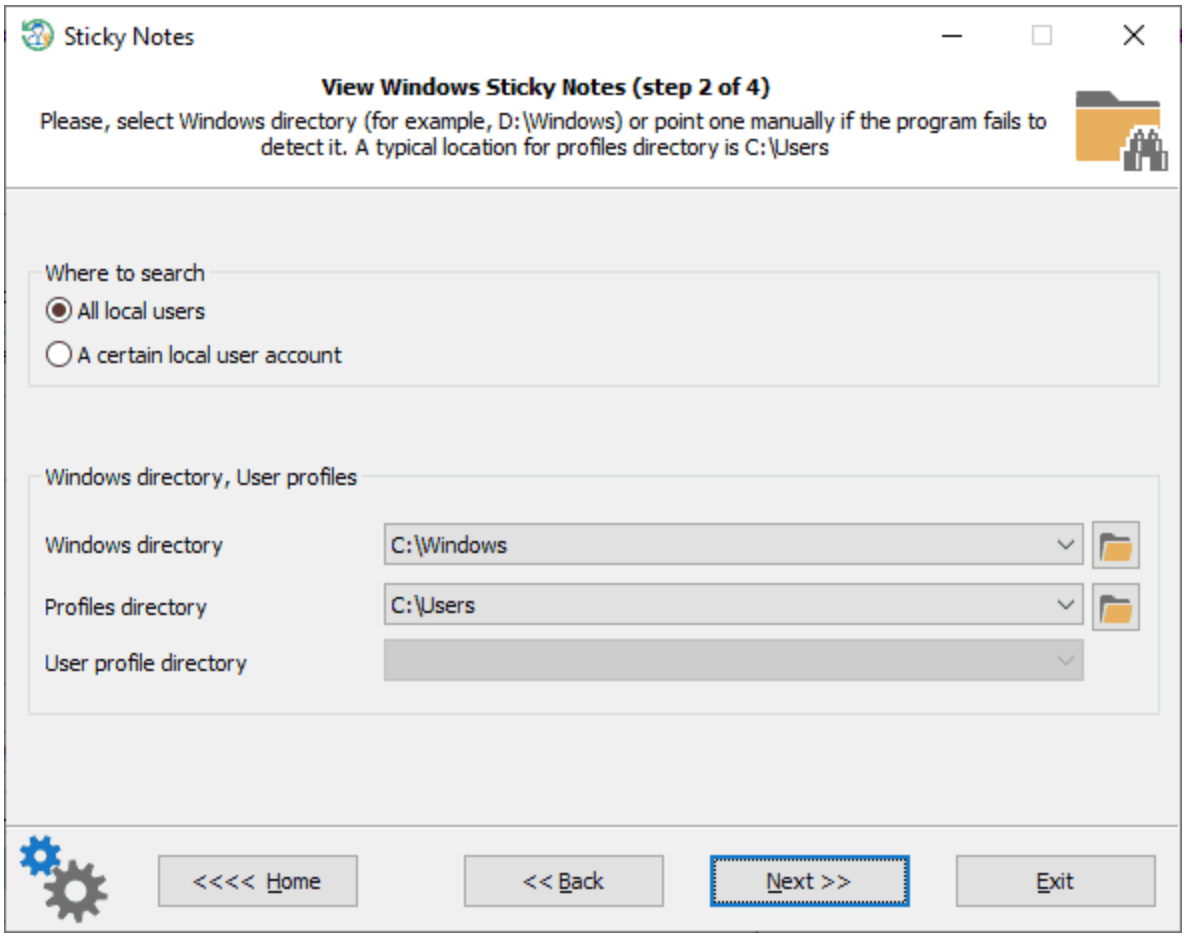
Файлы, которые открывались в последнее время в **Media Player**.

3.7.4 Записки Windows

Записки (**Sticky Notes**) - это приложение Microsoft для заметок на рабочем столе, которое входит в состав Windows, начиная с Windows 7.

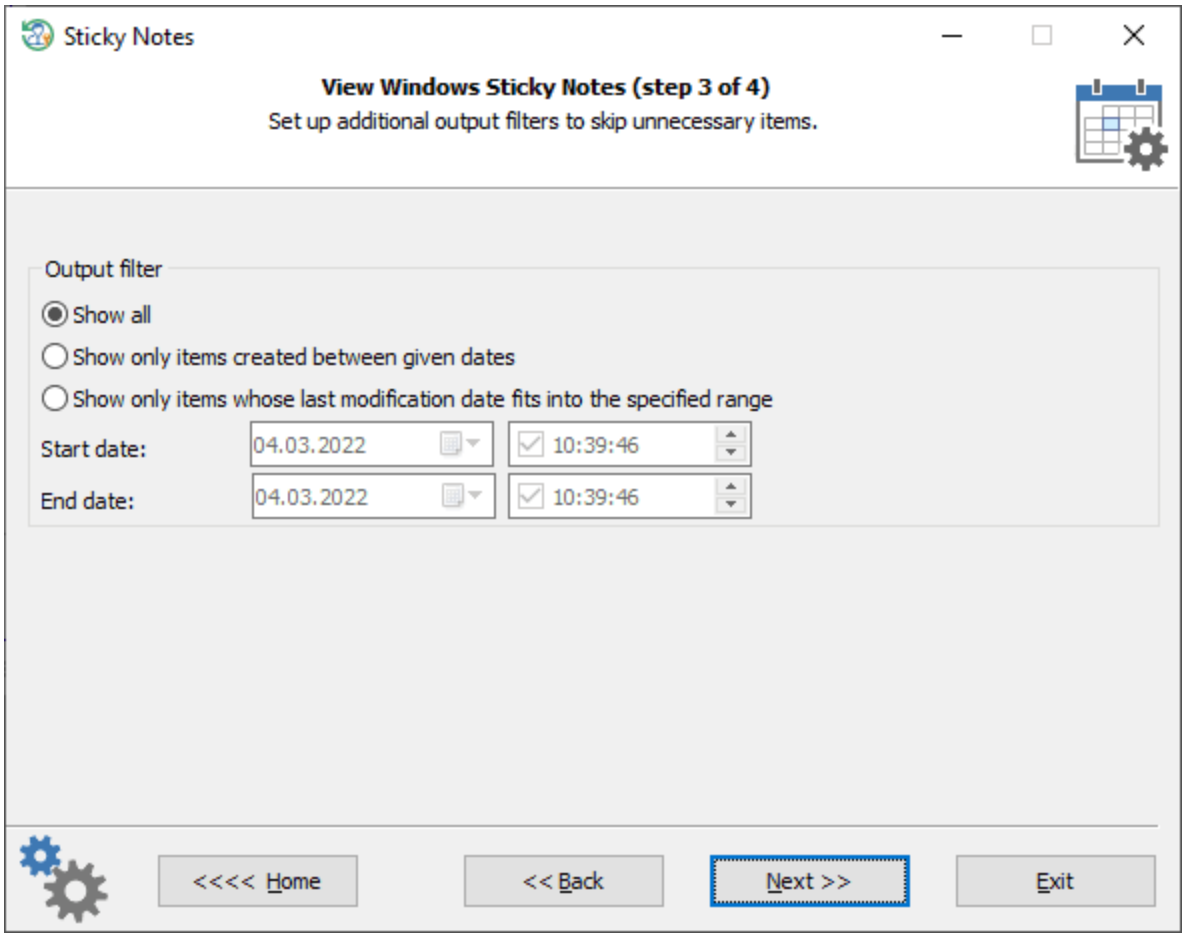
Reset Windows Password умеет отображать сохраненные (и некоторые удаленные) записки для всех пользователей Windows, а также для всех поддерживаемых операционных систем (в разных версиях Windows записки хранятся в разных местах).

Выбор пользователя



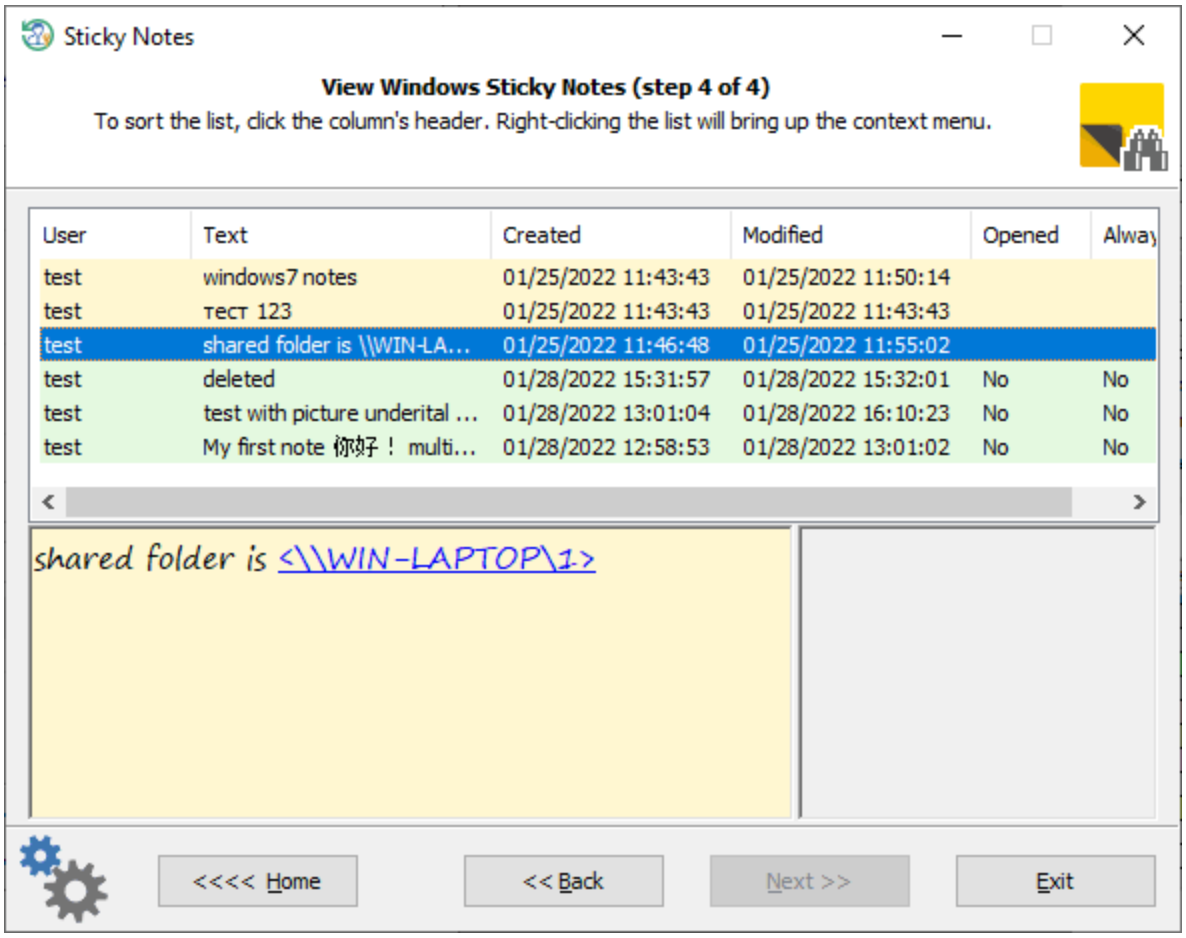
На первом шаге Мастер программы предлагает выбрать учетную запись, чьи записки нам надо найти. По-умолчанию предлагается поиск для всех локальных пользователей.

Установка фильтров отображения



Если записок очень много, можно включить опцию поиска по дате создания или по дате последнего изменения.

Записки Windows



Найденные записки отображаются в той цветовой гамме, в которой они были созданы. Программа поддерживает записки Windows 10 с включенными картинками. Найденные записки можно скопировать в буфер обмена или сохранить в файл.

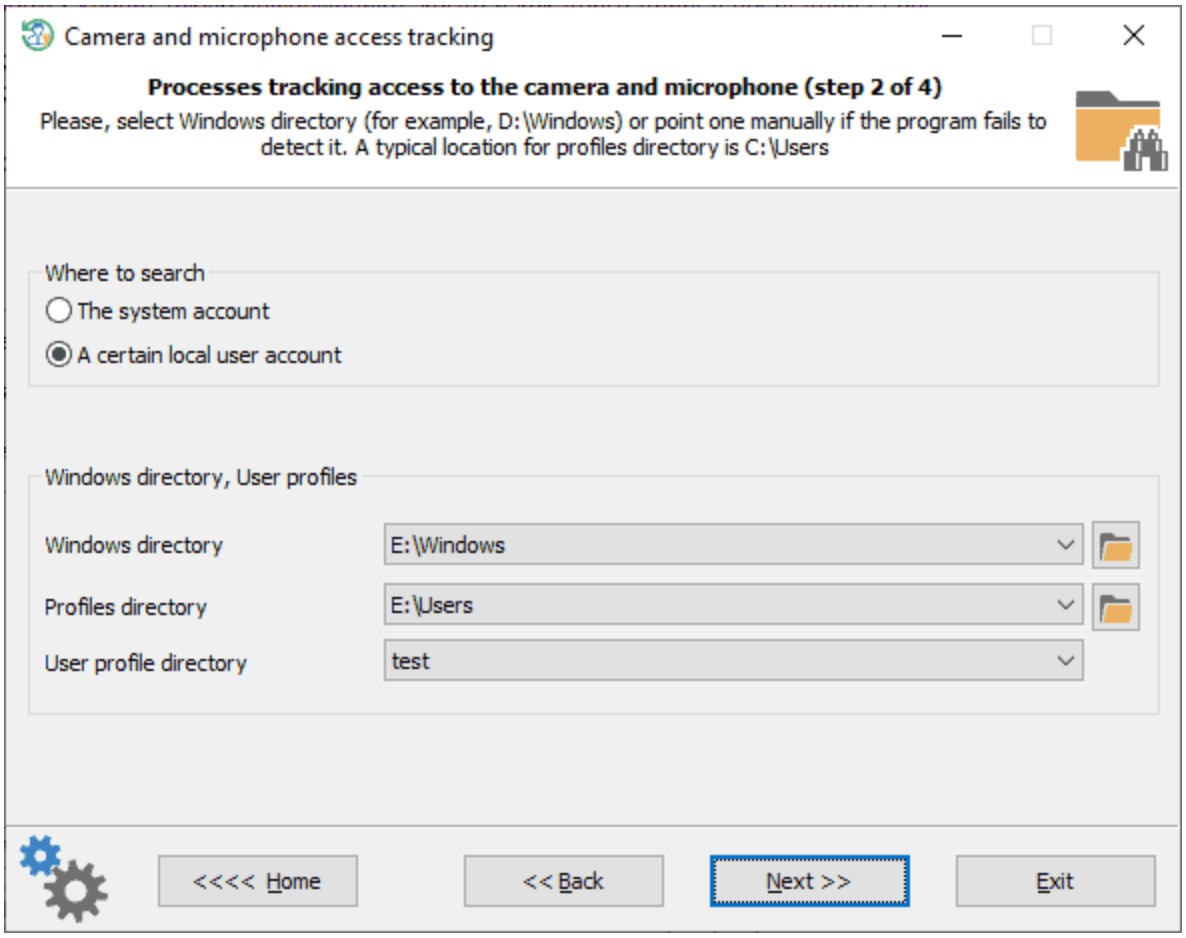
3.7.5 Отслеживание доступа к камере и микрофону

Эту функцию Reset Windows Password можно использовать в качестве судебной экспертизы, чтобы выяснить, какая программа или процесс использовали микрофон или камеру (а также некоторые дополнительные устройства, такие как датчики местоположения, если Windows хранит такую информацию), когда и как долго длился последний сеанс.

Windows хранит эту информацию в ключах реестра
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\microphone
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\webcam

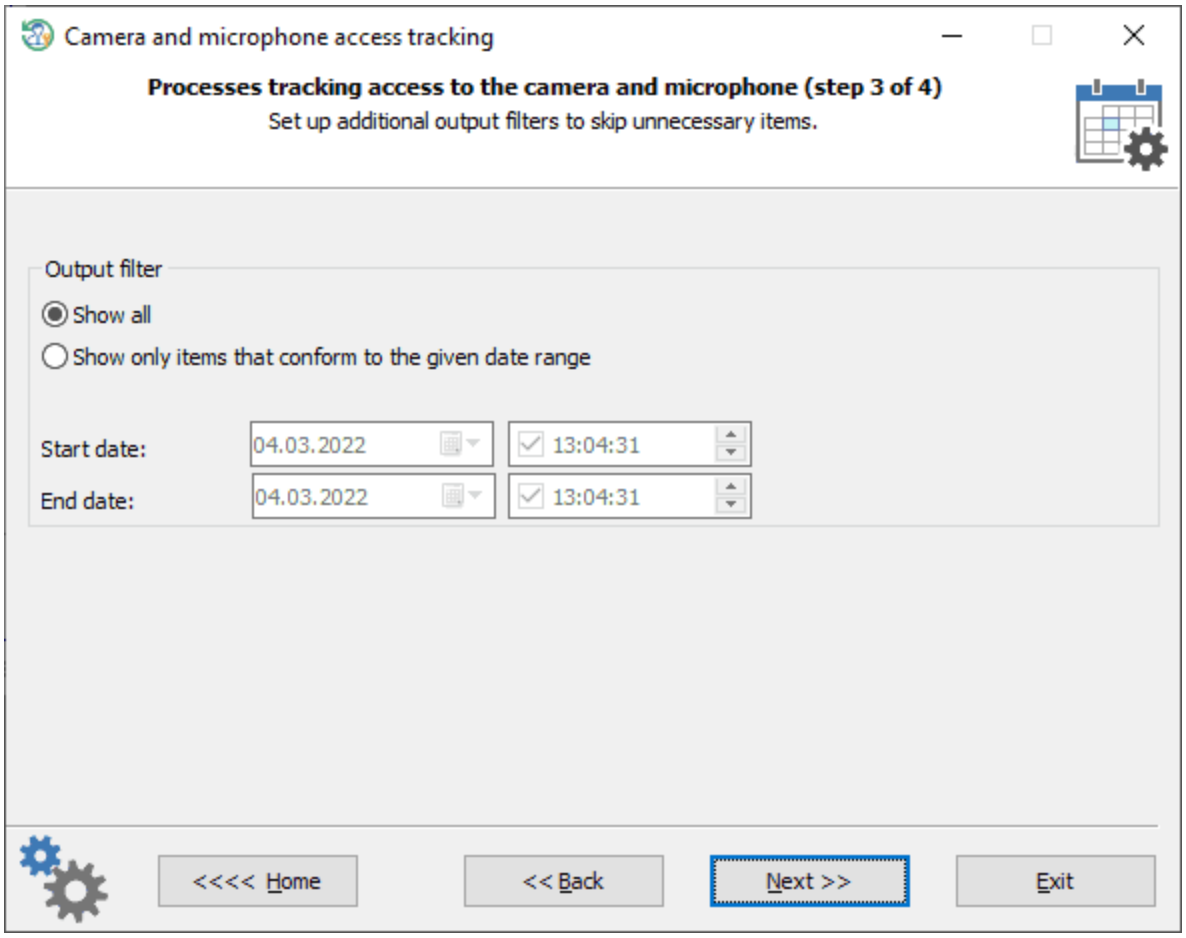
Данный инструмент можно также использовать для обнаружения вредоносных процессов и программ, ведущих скрытую слежку за пользователями.

Выбор пользователя



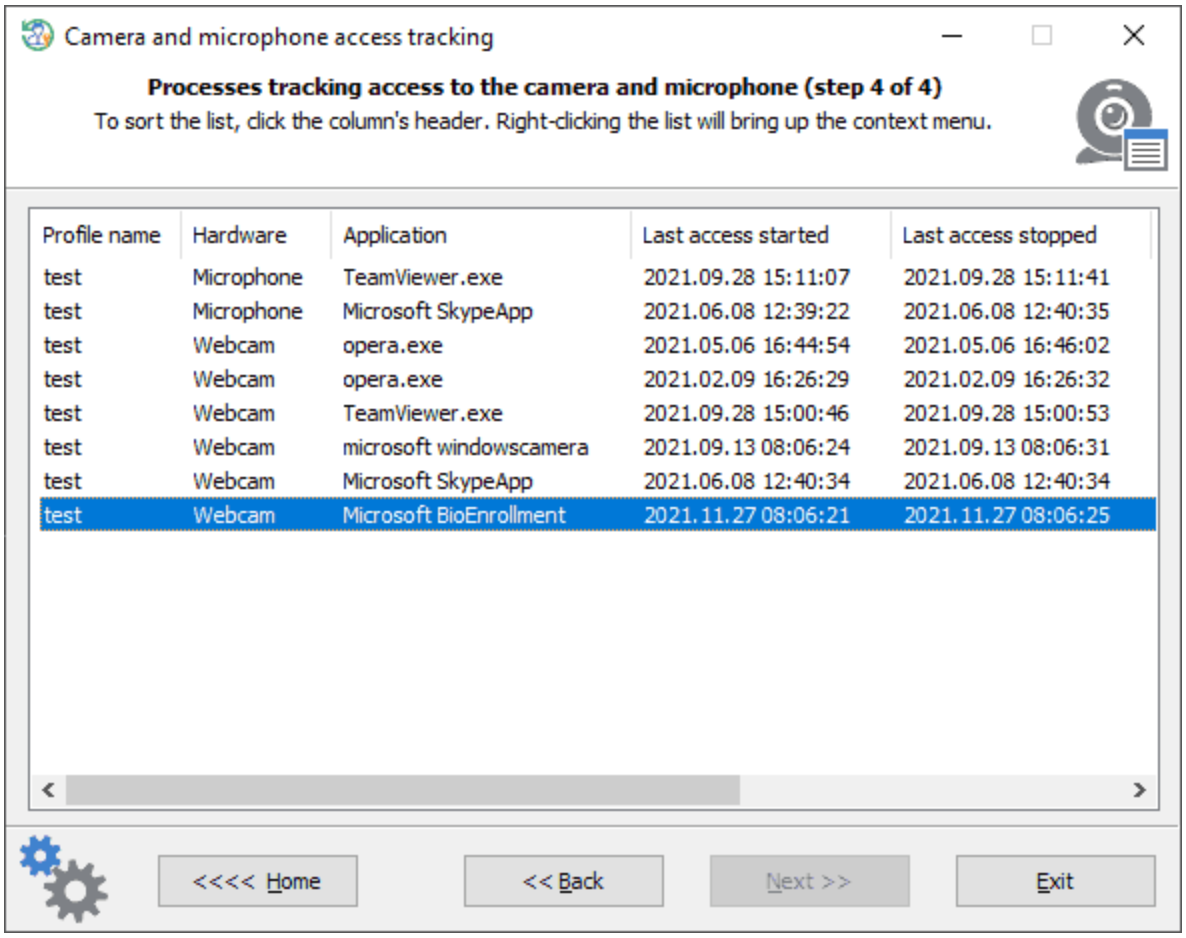
Для поиска информации о последнем доступе к камере и микрофону, сначала необходимо выбрать учетную запись пользователя.

Установка фильтров отображения



Для удобства можно также выставить опцию отображения за конкретный период.

Доступ к камере и микрофону

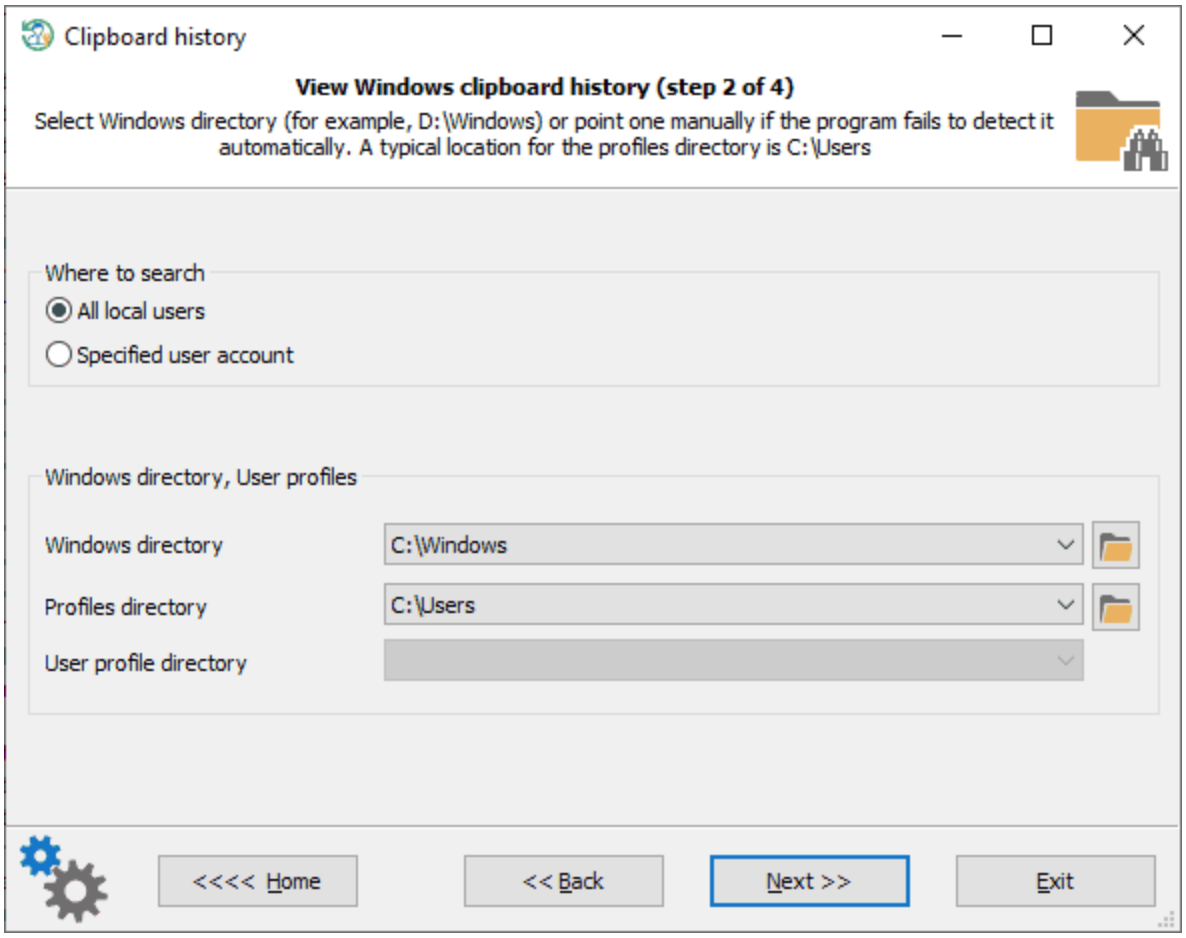


Программа также производит поиск информации о последнем доступе программ и к другим устройствам, не только к камере и микрофону. Например, к устройствам Bluetooth.

3.7.6 История буфера обмена

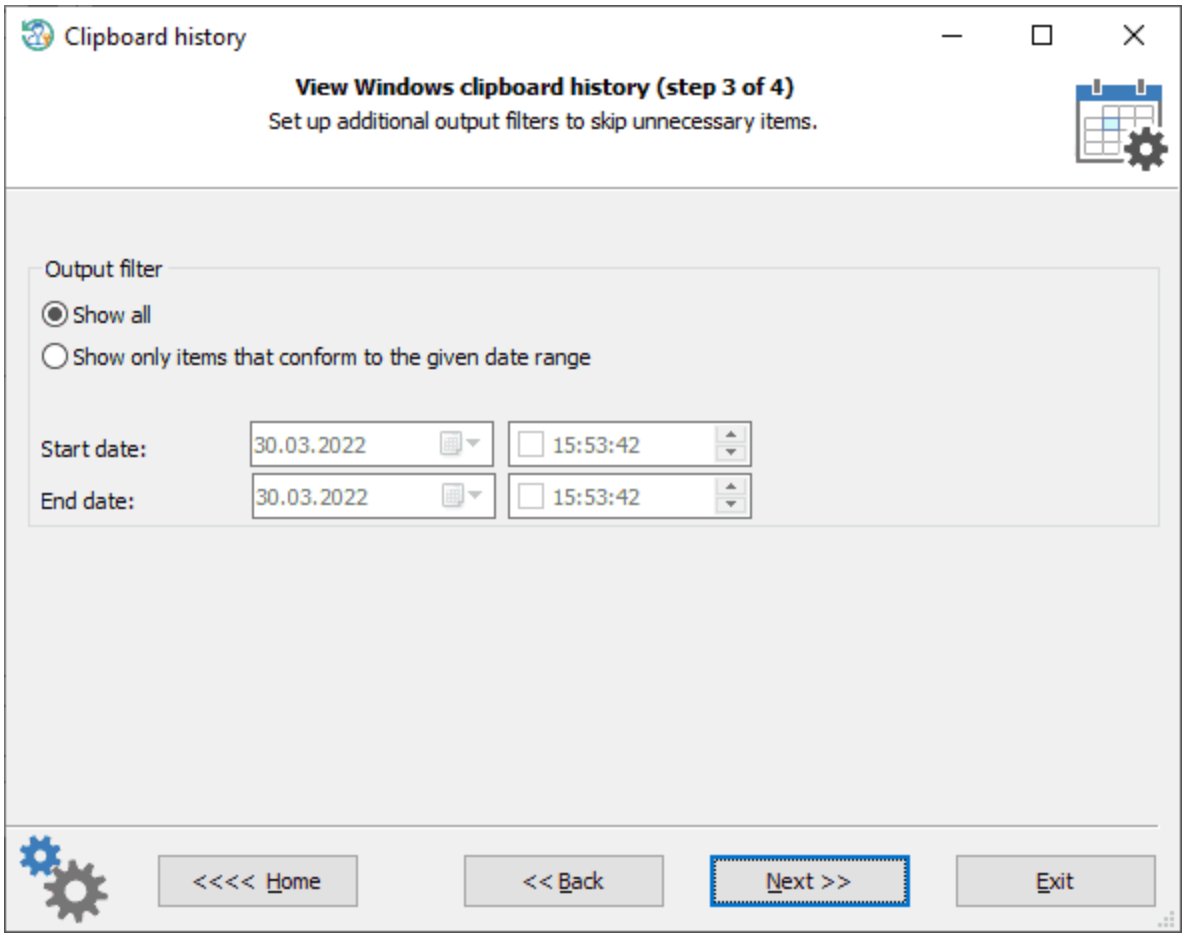
Инструмент для извлечения **истории буфера обмена** позволяет расшифровывает текст, изображения, а также другую информацию, хранящуюся в буфере обмена Windows. Буфер обмена Windows очищается каждый раз, когда пользователь выходит из системы. Однако, если включена опция *'История буфера обмена'*, система сохраняет информацию из буфера обмена. Таким образом, данные могут быть извлечены и расшифрованы даже после завершения работы операционной системы. Именно для для этого и предназначен новый инструмент.

Выбор учетной записи буфера обмена



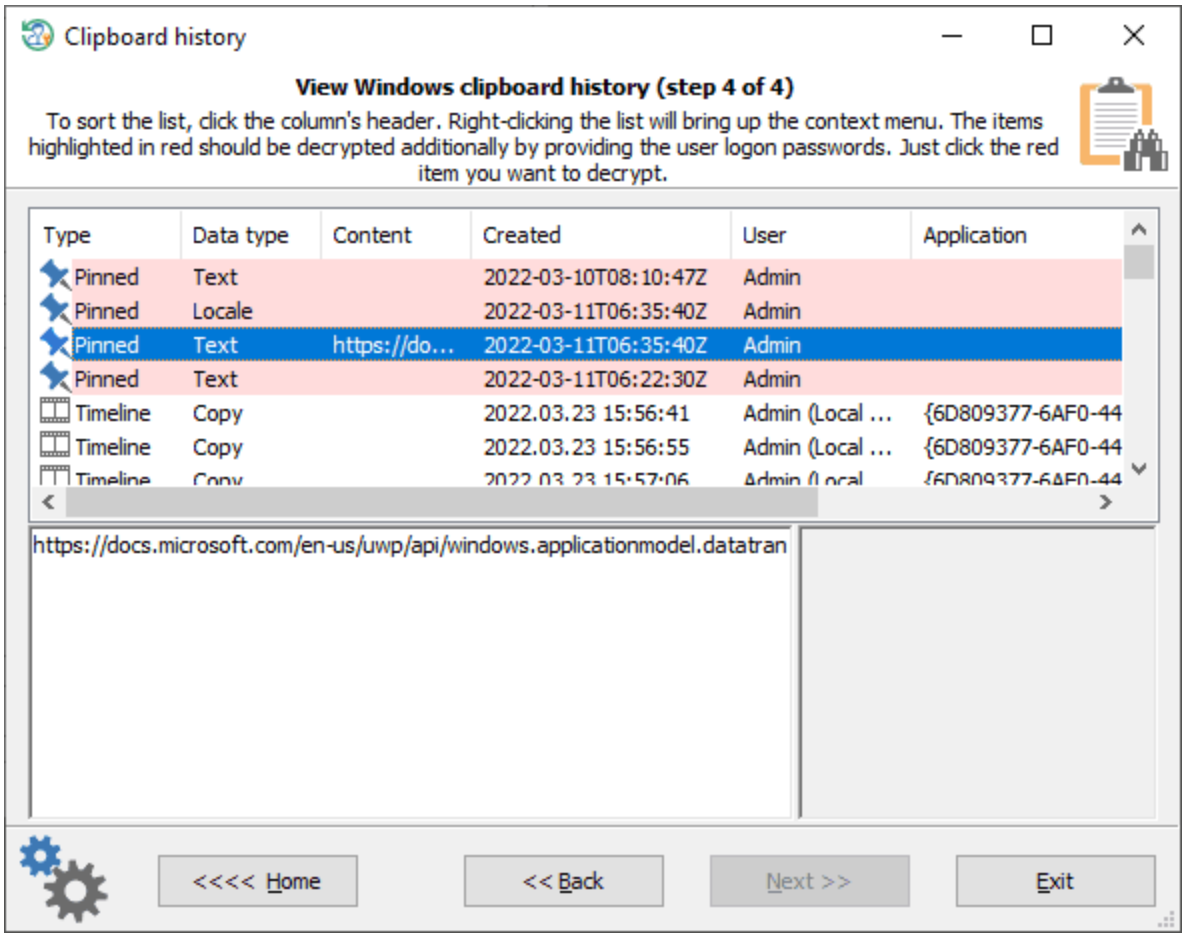
Выберите учетную запись, из которой вам нужно извлечь историю буфера обмена. По умолчанию заданы все локальные пользователи.

Настройка временных фильтров буфера обмена



Настройте временные фильтры, чтобы пропустить отображение ненужных записей буфера обмена.

История буфера обмена Windows



Программа поддерживает 3 типа буфера обмена Windows, данные из которых можно расшифровать после перезагрузки системы:

1. Элементы буфера обмена, хранящиеся в базе данных временной шкалы Windows.
2. Закрепленная история буфера обмена (требуется дополнительная расшифровка). Чтобы закрепить (сохранить) элемент буфера обмена, вызовите историю буфера, нажав клавишу с логотипом **Windows + V**, затем в контекстном меню элемента выберите '*Закрепить*'.
3.

Типы данных **Copy/Paste** в столбце *'Тип данных'* означают, что фактических данные не сохранены (столбец **Содержимое** всегда пуст), а присутствует только запись об операции с буфером. Расшифрованные список с историей буфера обмена содержит некоторую дополнительную полезную информацию, такую как название приложения и документа, где выполнялась операция с буфером, когда была выполнена операция и т.д.

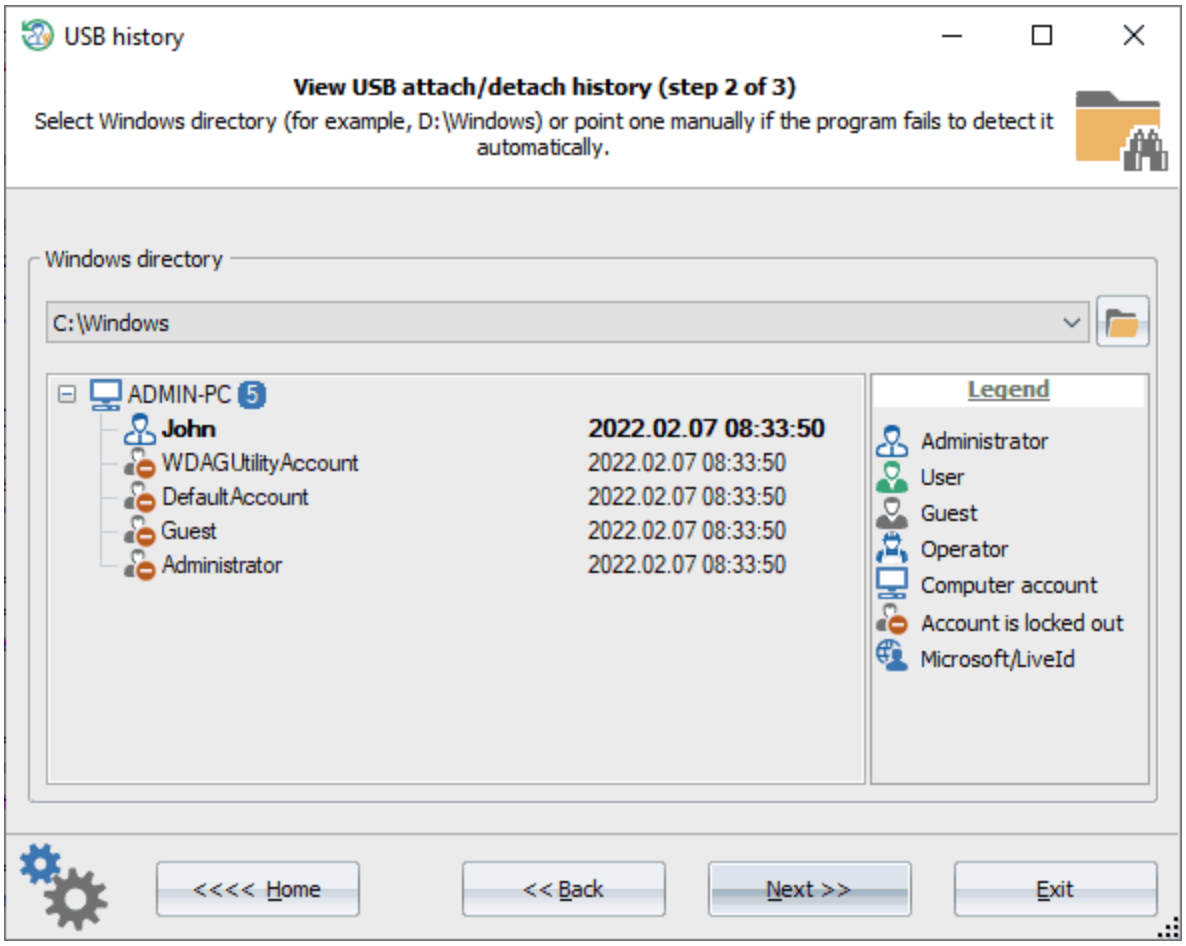
Для расшифровки некоторых данных может потребоваться пароль пользователя на вход. Однако в этом нет необходимости, если это был последний залогиненный в систему пользователь.

3.7.7 История USB

В криминалистической экспертизе часто требуется узнать какие USB устройства были подключены к компьютеру и когда. Поскольку Windows хранит следы всех подключаемых или отключаемых USB устройств, то сделать это довольно просто.

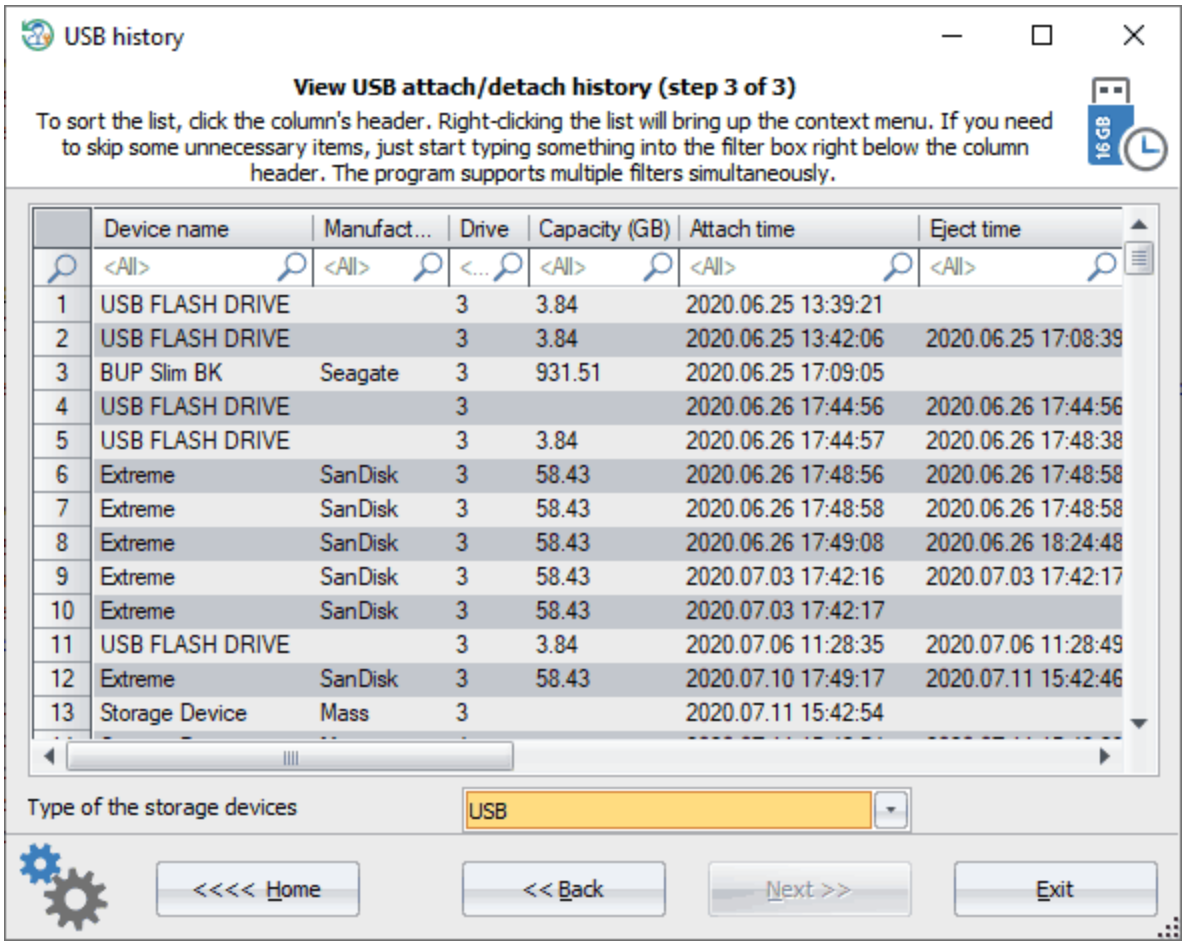
Инструмент для просмотра истории подключаемых накопителей позволяет узнать какие устройства были подключены к компьютеру и когда, их размер, серийный номер, а также другую техническую информацию, например, таблицу разделов и главную загрузочную запись во время подключения.

Выбор каталога Операционной Системы



Выберите каталог Windows для поиска информации о накопителях.

История USB



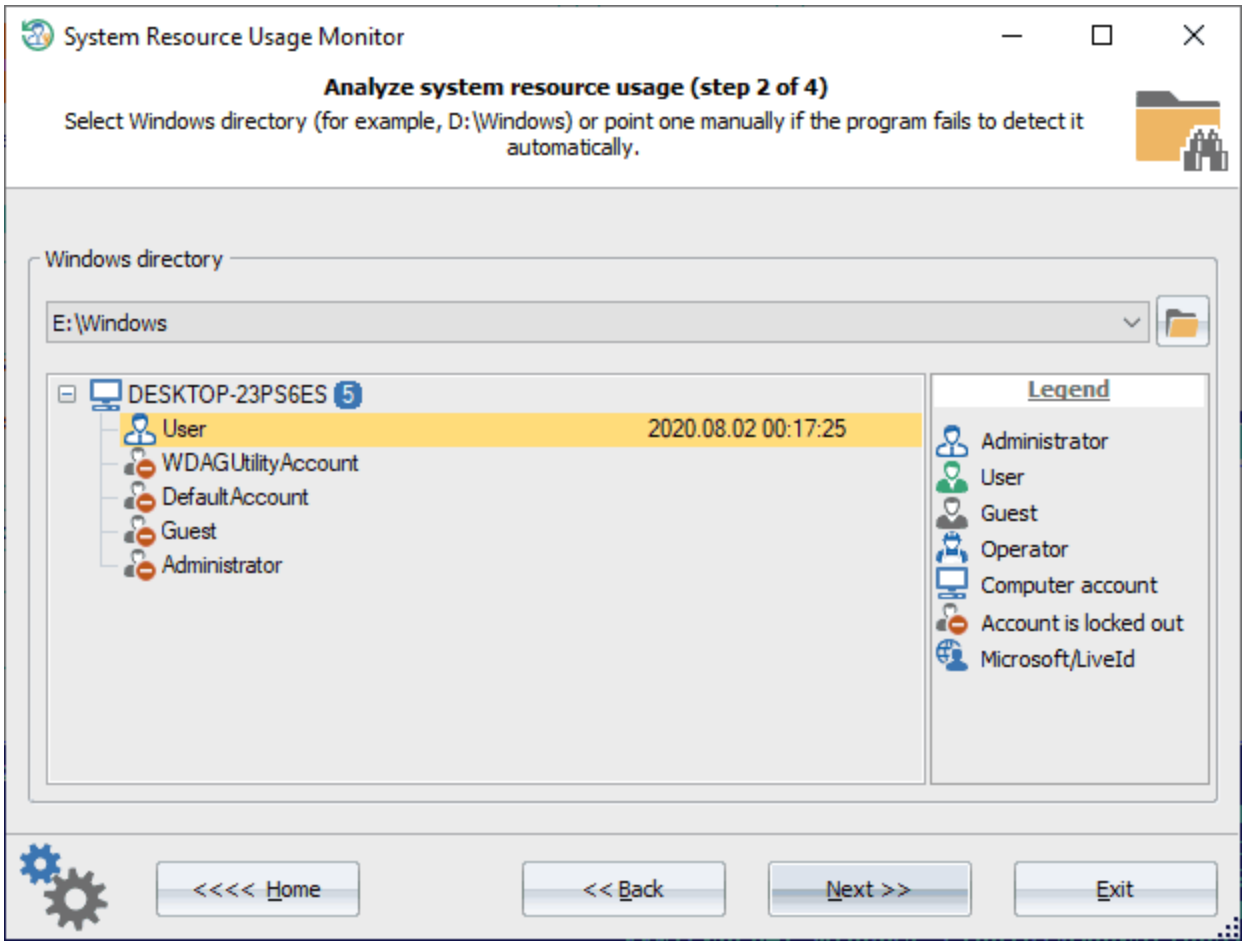
По-умолчанию, программа отображает историю подключений USB, но поддерживаются и другие типы накопителей: 1394, ATA, ATAPI, FIBRE, Virtual File Backup Storages, ISCSI, MMC, RAID, SAS, SATA, SCSI, SD, SSA, Storage Spaces, Virtual Storages.

3.7.8 Монитор использования системных ресурсов

Монитор использования системных ресурсов (SRUM) является недооцененным, но от этого отнюдь не бесполезным артефактом криминалистического расследования, который может рассказать, что происходило на компьютере в определенный момент времени. SRUM хранит (как правило, за последние два месяца) следы активности пользователей и процессов, статистику по отправленным и полученным сетевым данным, расширенную поминутную информацию об использовании процессорного времени, клавиатуры мыши, диска и т.д.

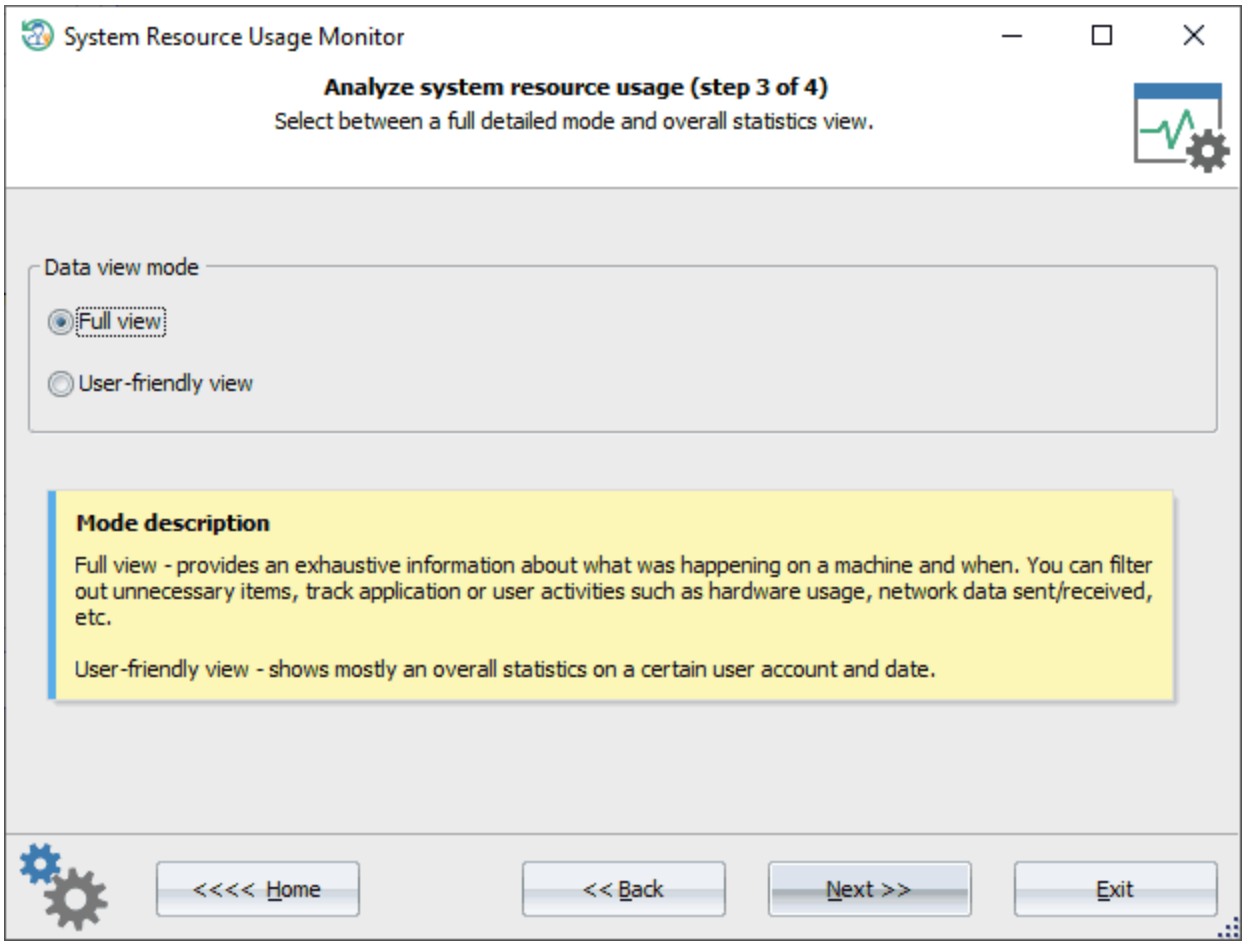
Монитор использования системных ресурсов впервые увидел свет с выходом Windows 8. Физически, все данные SRUM хранятся в файле **SRUMDB.DAT**, который находится в каталоге **%WINDIR%\System32\sru** и представляет собой базу данных в формате **E**xtensible **S**torage **E**ngine.

Выбор каталога Операционной Системы



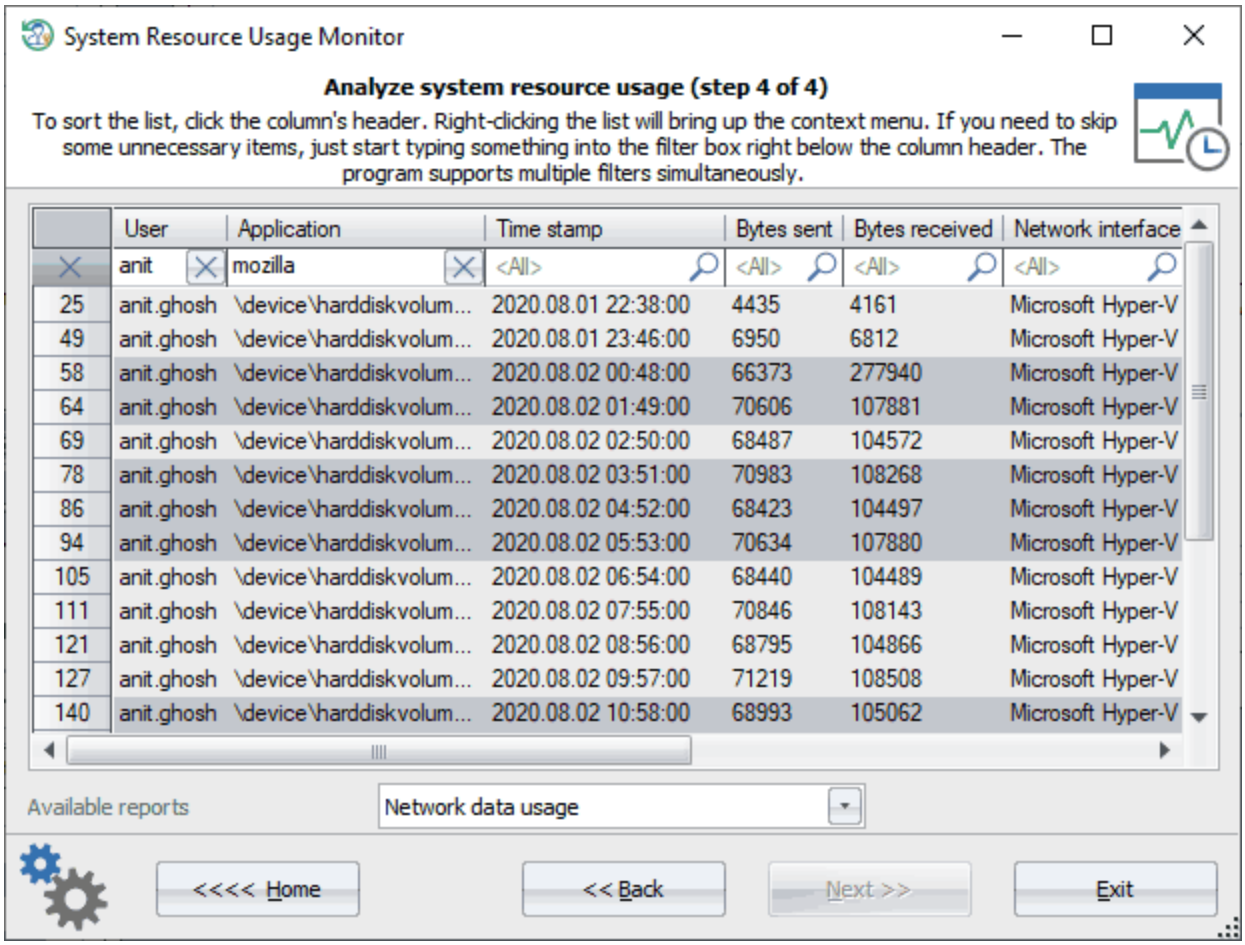
Для просмотра и анализа SRUM программе в первую очередь необходимо указать путь к каталогу Windows.

Выбор режима отображения



В программе предусмотрено два режима для отображения данных: полный, для вывода всей доступной информации, и краткий, который прячет избыточную информацию и показывает общую статистику по пользователям и датам.

SRUM - полная информация



Интересующую вас информацию можно просмотреть выбрав одну из доступных таблиц:
- Временная шкала приложений
- Использование ресурсов
- Сетевые соединения
- Сетевые данные

Задача. Узнать когда и сколько было прочитано и отправлено сетевых данных в браузере Firefox пользователем anit.ghosh.
Решение. Напишем в фильтр и именем пользователя 'anit.ghosh', а в поле с приложением - 'Mozilla' или 'Firefox'. В результате получим статистику по пользователю, как показано на картинке выше.

Общая информация для всех таблиц: имя пользователя, приложение, дата, когда информация была занесена в базу данных.

Доступная информация для таблицы *'Временная шкала приложений*': CPU timeline, CPU cycles, cycles breakdown, cycles attribute, cycles attribute breakdown, cycles WOB, cycles WOB breakdown, disk timeline, disk raw, network timeline, network tail raw, network bytes raw, metered network timeline, metered network tail raw, metered network bytes raw, rendered timeline, rendered, dirtied timeline, dirtied, propagated timeline, propagated, display required timeline, display required, in focus, user input timeline, user input, keyboard input timeline, keyboard input, mouse input, audio in timeline, audio in, audio out timeline, audio out, PSM foreground, flags, end time, timeline end, duration, span.

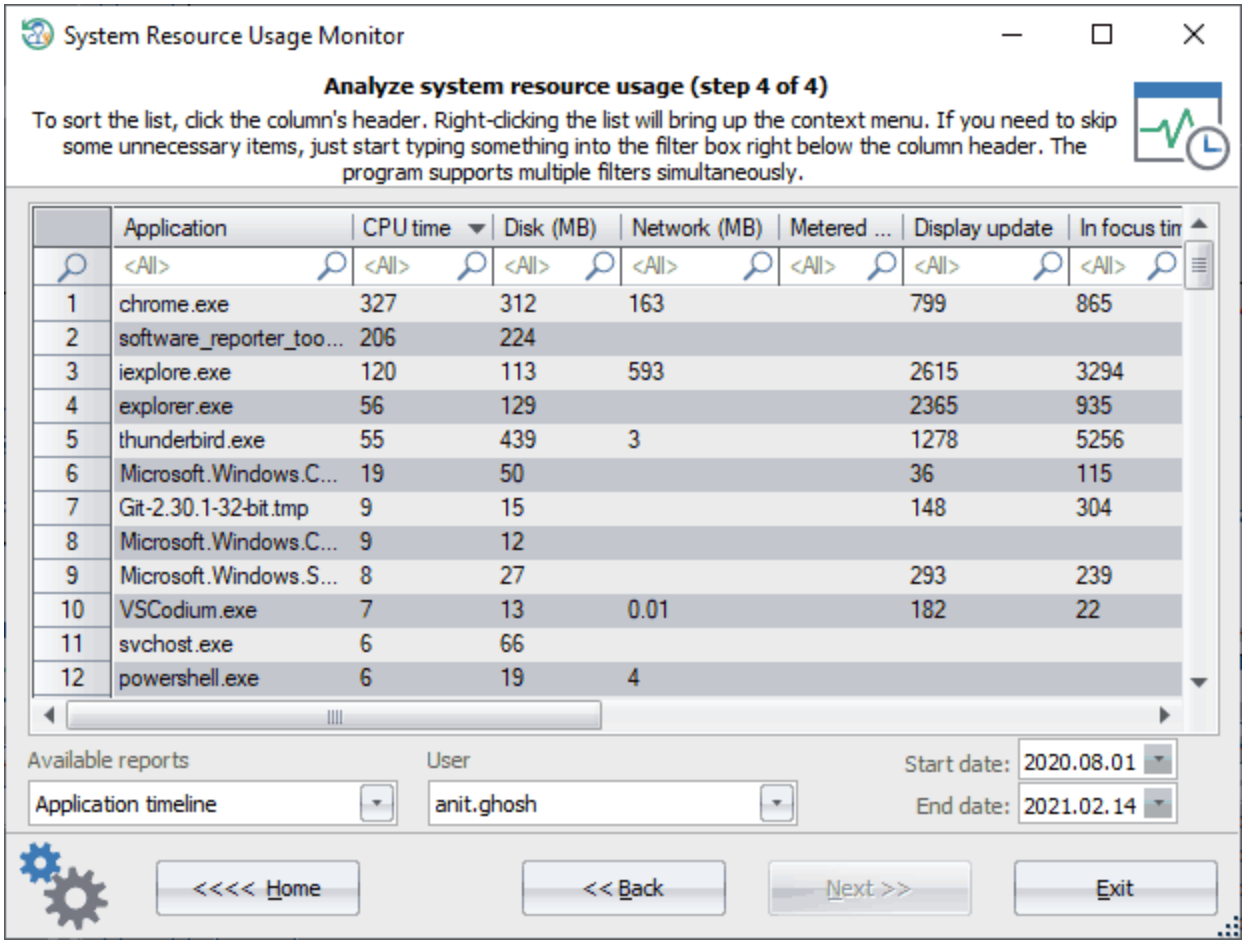
Доступная информация для таблицы *'Использование ресурсов'*: face time, foreground cycle time, foreground bytes read, foreground bytes write, foreground context switches, foreground number of flushes, foreground read operations, foreground write operations, background cycle time, background bytes read, background bytes write, background context switches, background number of flushes, background read operations, background write operations.

Доступная информация для таблицы *'Push-уведомления Windows'*: notification type, network type, payload size.

Доступная информация для таблицы *'Сетевые соединения'*: connection started, connection time, network interface, interface type, profile ID, profile flags.

Доступная информация для таблицы *'Сетевые данные'*: bytes sent, bytes received, network interface, interface type, profile ID, profile flags.

SRUM - общая статистика



Общая статистика по определенному пользователю за выбранный период.

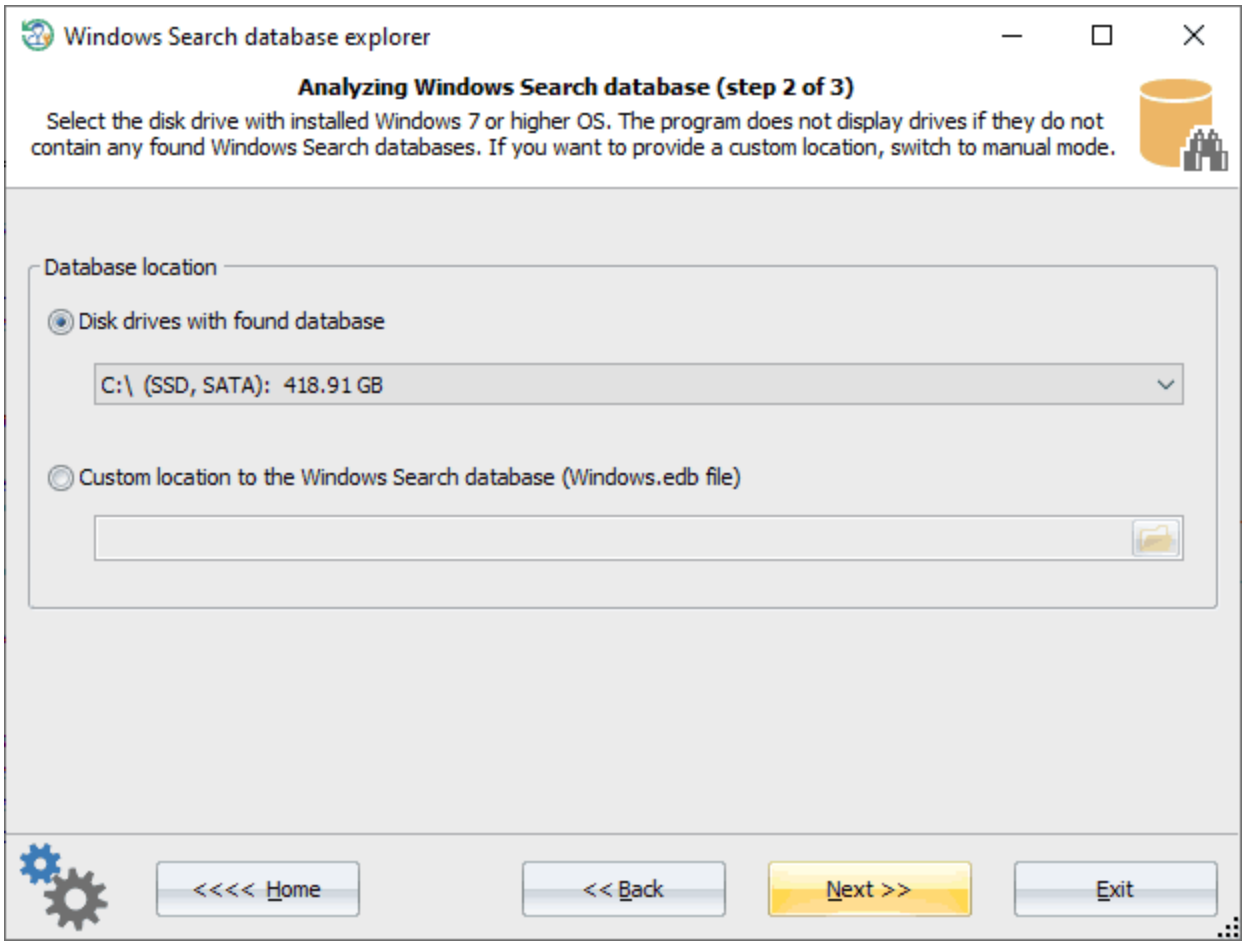
3.7.9 Обозреватель баз данных Windows Search

Windows Search - это десктопная поисковая платформа для индексации контента, разработанная корпорацией Майкрософт. Windows Search создает индекс файлов, документов, электронных писем, папок, программ, заметок, фотографий, истории Интернета и т.п., а также содержимого файлов. Цель индексации состоит в том, чтобы предложить пользователям быстрый инкрементный поиск на основе содержимого и метаданных, таких как авторы, даты, люди, имена и типы файлов, их размер и др.

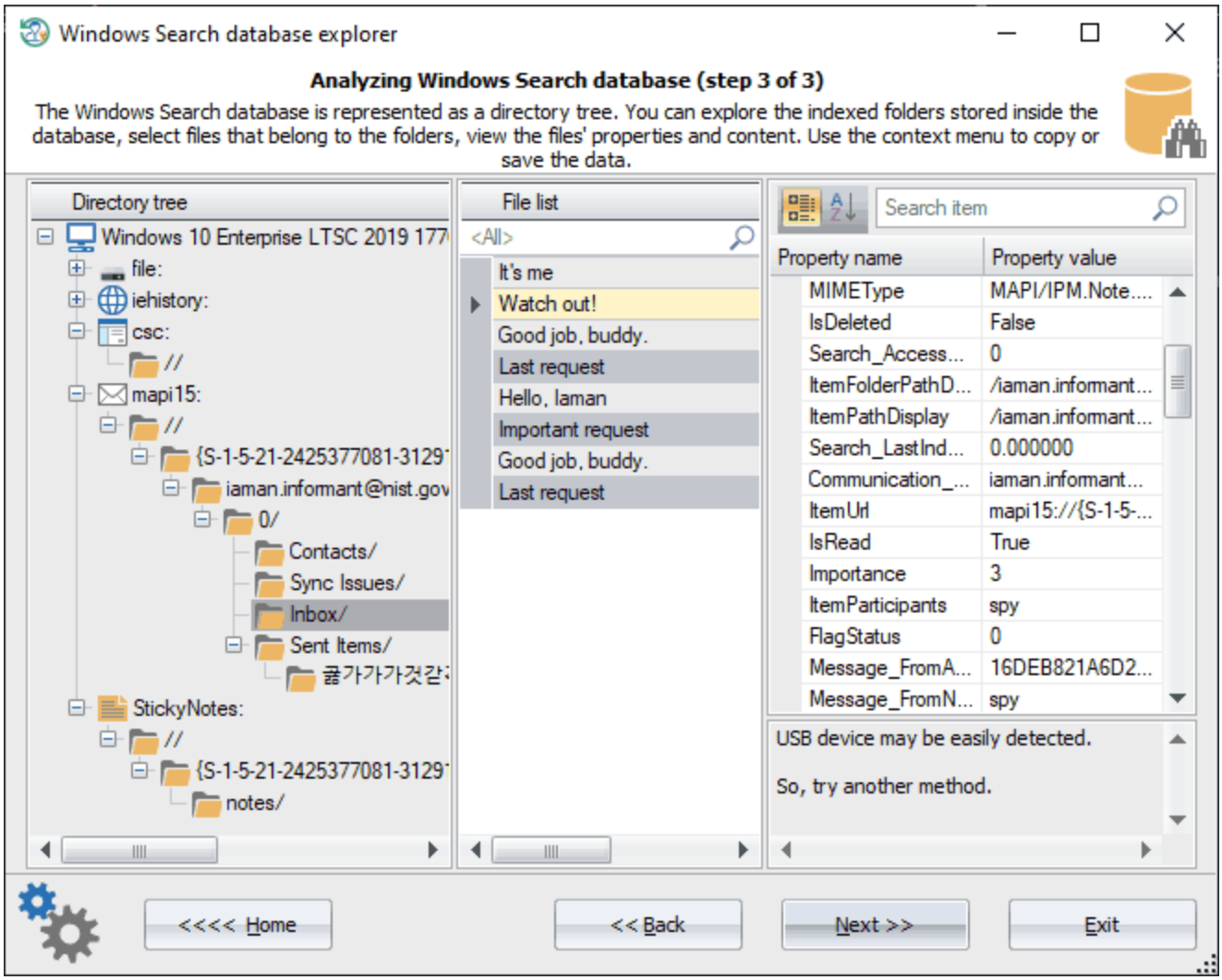
База данных Windows Search предоставляет ценный источник информации для судебного следователя. Данные хранятся внутри одного файла в формате **Extensible Storage Engine** в следующем каталоге: *%SYSTEMDRIVE%\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb*

Windows 11 хранит данные и индекс поиска в базе данных SQLite с именем Windows.db и имеет аналогичную Windows 10 структуру.

Обозреватель Windows Search - это инструмент для анализа базы данных и отображения собранной в результате индексации информации в удобочитаемом виде.



В первую очередь, необходимо указать путь к базе данных. Можно сделать это либо выбрав диск (программа отображает только те диски, на которых была обнаружена база данных), либо указав полный путь к базе данных вручную.



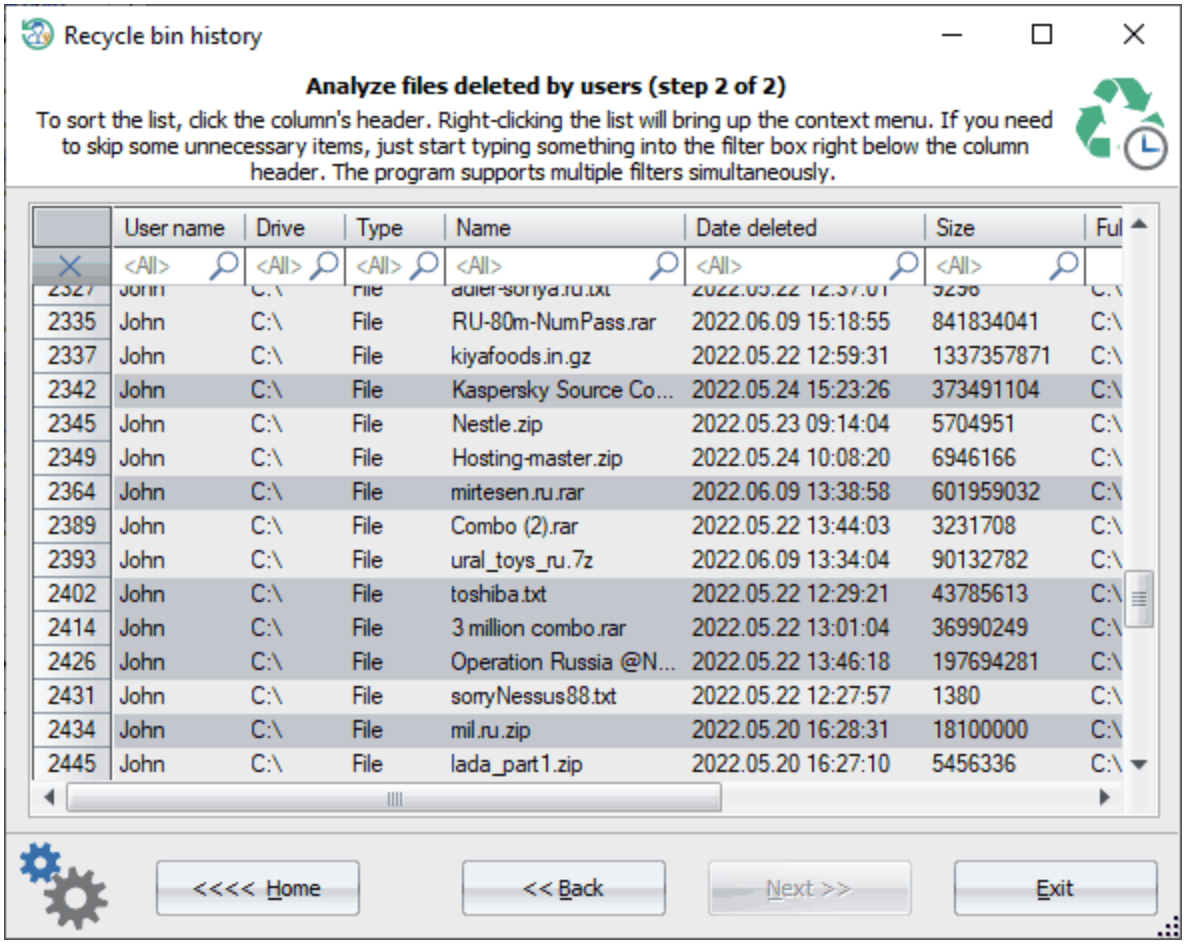
Программа создает список всех найденных элементов и отображает его на левой панели под в виде дерева каталогов. Таким образом, дерево каталогов является родителем для диска, электронной почты, истории Интернета, активности пользователей и других папок. Как только выбрана какая-либо папка в панели дерева каталогов, программа заполняет среднюю панель со списком файлов, отображая там элементы, принадлежащие выбранной папке. Чтобы просмотреть доступные свойства (правая панель), просто выделите соответствующий файл или элемент.

Опытные пользователи могут воспользоваться дополнительной опцией для создания списков слов, содержащих все проиндексированные слова из базы данных поиска. Эти словари можно будет использовать позже для дальнейшего анализа системы или в любом программном обеспечении для восстановления паролей.

3.7.10 История корзины

Корзина Windows это элемент графического интерфейса, предназначенный для удаления ярлыков, файлов и папок, о котором все знают, но который все забывают чистить периодически. Корзина может использоваться для восстановления удаленных данных, например, в следствие ошибки.

Часто пользователи забывают, что неочищенная корзина в Windows хранит их улики, пароли, историю, исходные коды и т.д. Поэтому для экспертов корзина - наиболее простой способ анализа последних действий пользователя и удаленных им файлов.

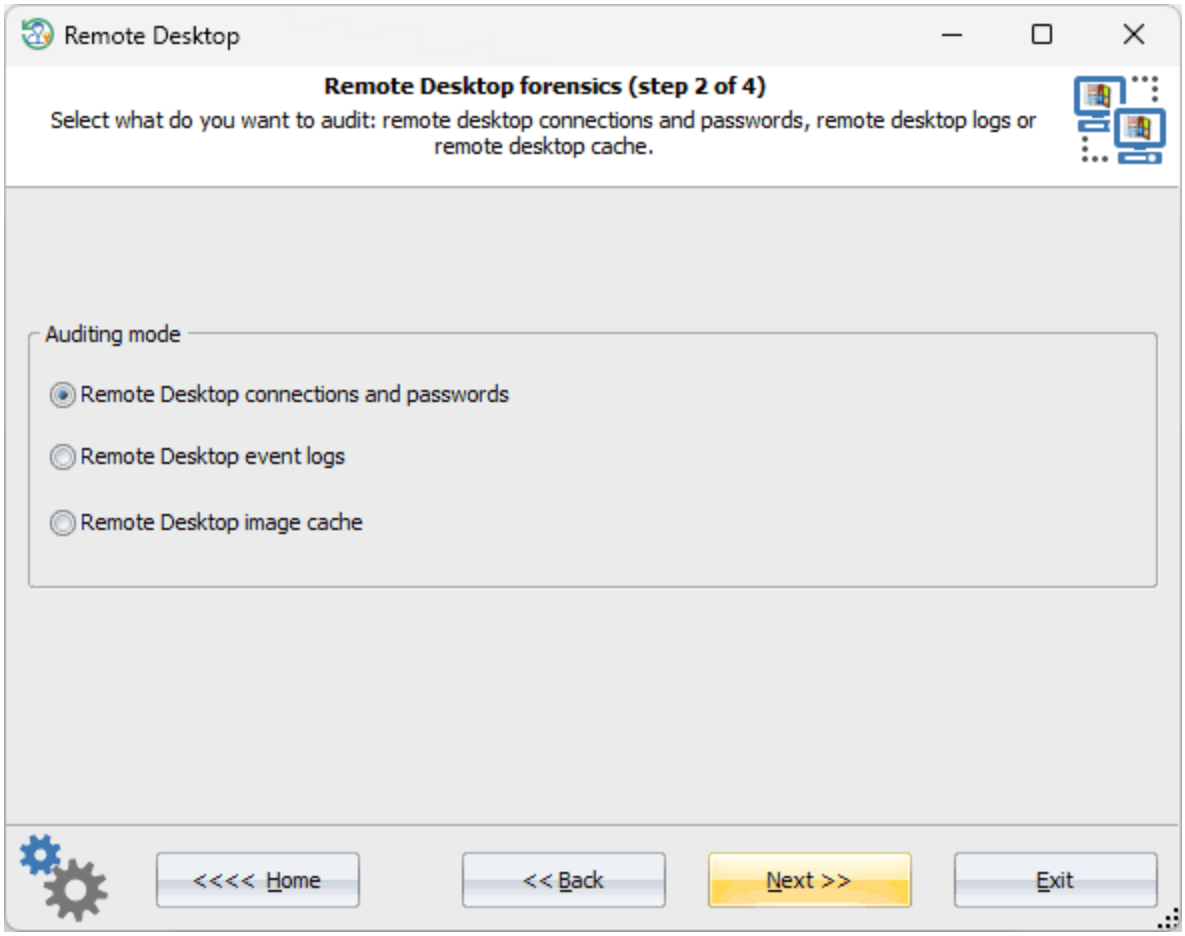


При запуске инструмента **'История корзины'**, программа сканирует жесткие диски, производит поиск корзин всех установленных ОС Windows для всех учетных записей и сводит найденные данные в одну таблицу. Для быстрого поиска нужного элемента в таблице можно использовать фильтры. Например, чтобы найти все удаленные ярлыки, введите '.lnk' (без кавычек) в фильтр с именем файла. Выбранные элементы можно сохранить в *.zip архив.

3.7.11 Удаленный рабочий стол

Эта функция программы предоставляет криминилистическую информацию об удаленных подключениях по протоколу удаленного рабочего стола в Windows.

Протокол удаленного рабочего стола (RDP) - это проприетарный протокол, разработанный компанией Microsoft. Он позволяет пользователям удаленно подключаться к компьютеру на базе Windows по сетевому соединению и получать доступ к удаленному рабочему столу, приложениям и файлам удаленного ПК. После подключения пользователь может взаимодействовать с удаленным рабочим столом, запускать приложения и передавать файлы между локальным и удаленным компьютерами. RDP поддерживает различные функции, включая перенаправление аудио и видео, обмен принтерами и буфером обмена, а также удаленную помощь.



В судебных расследованиях крайне важно собирать каждый возможный фрагмент доказательств, связанных с удаленными подключениями, включая сохраненную информацию о входе, записи действий и любые изображения удаленного рабочего стола, которые могут быть кэшированы. Этот конкретный раздел программы предназначен именно для этого.

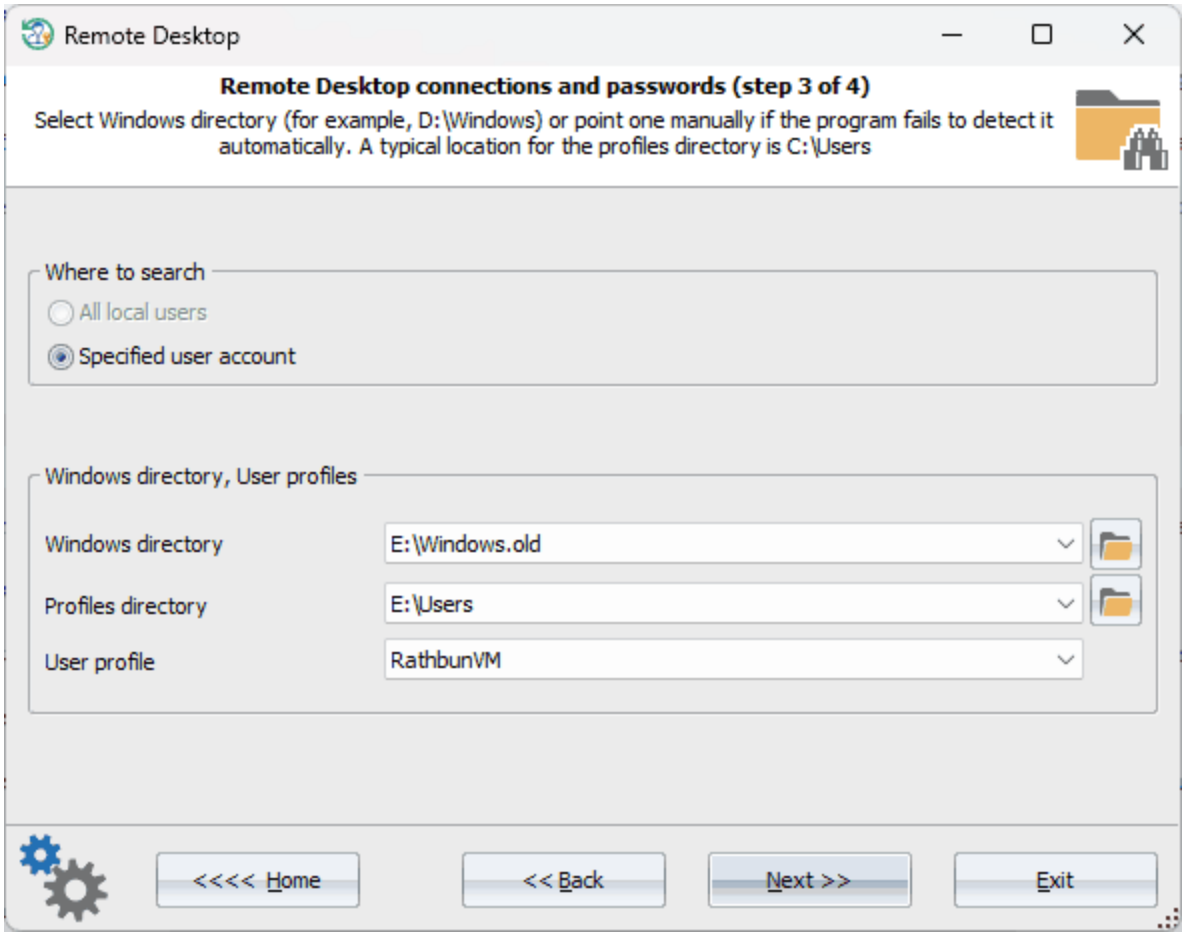
3.7.11.1 Соединения и пароли удаленного рабочего стола

Во время подключения пользователя к удаленному компьютеру через протокол удаленного рабочего стола, учетные данные удаленного компьютера кэшируются локально (если пользователь установил соответствующий параметр) для обеспечения последующей автоматической аутентификации.

Кэшированные учетные данные хранятся в менеджере учетных данных Windows, который является защищенной областью для хранения приватной информации. Например, секретов, токенов, паролей и другой информации для аутентификации. Это позволяет пользователю подключаться к удаленному компьютеру, не вводя каждый раз имя и пароль учетной записи.

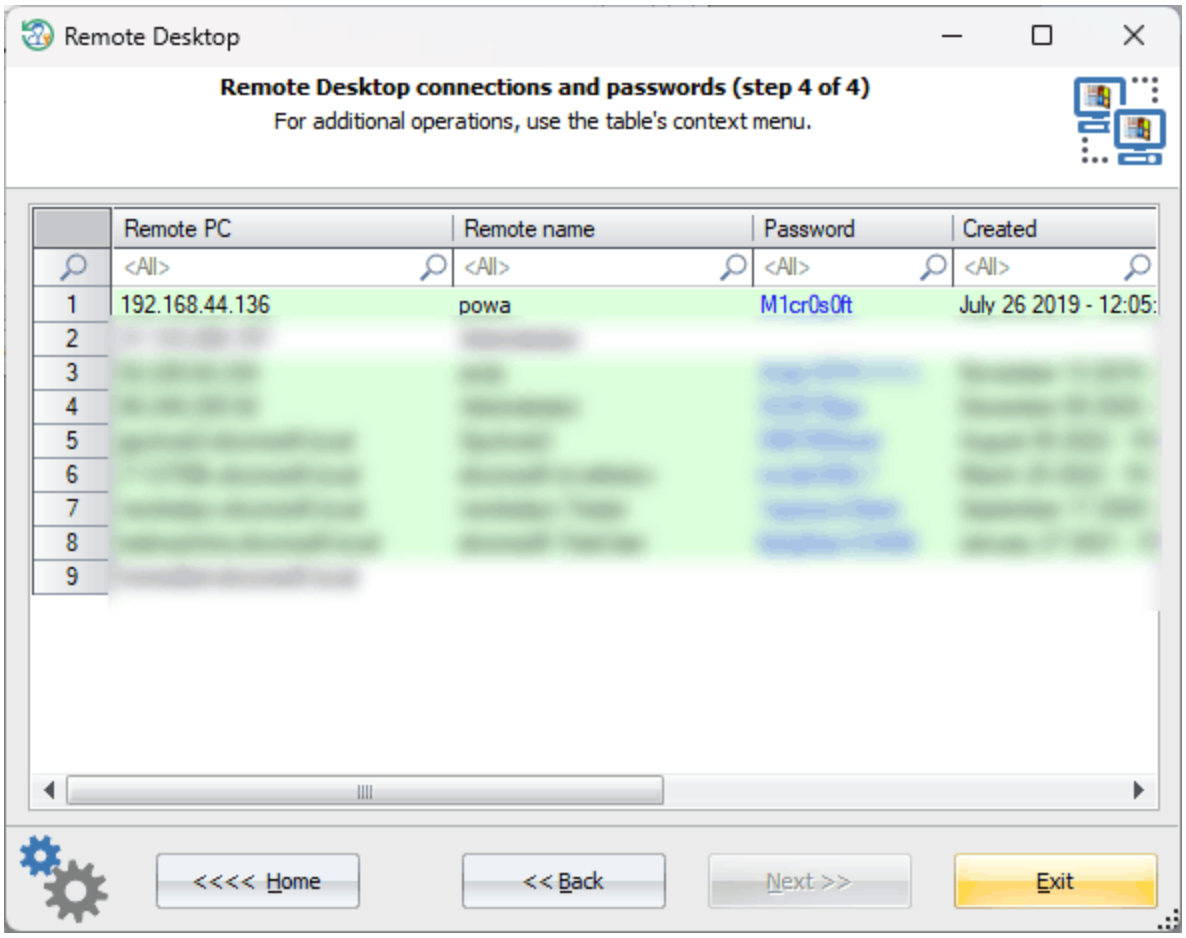
Reset Windows Password может извлекать и расшифровывать учетные данные RDP, хранящиеся в менеджере учетных данных Windows, буквально за два простых шага.

Выбор учетной записи



Сначала введите каталог Windows и учетную запись пользователя, для которой нужно сканировать сохраненные учетные данные RDP.

Подключения и пароли удаленного рабочего стола



Если требуется, введите на запрос программы пароль на вход в учетную запись. После этого, программа расшифрует найденные учетные данные RDP, а также адреса удаленного компьютера, даты подключения и другую сопутствующую информацию.

Если вам нужно расшифровать другие пароли, хранящиеся в менеджере учетных данных Windows, переключитесь на инструмент восстановления сетевых паролей.

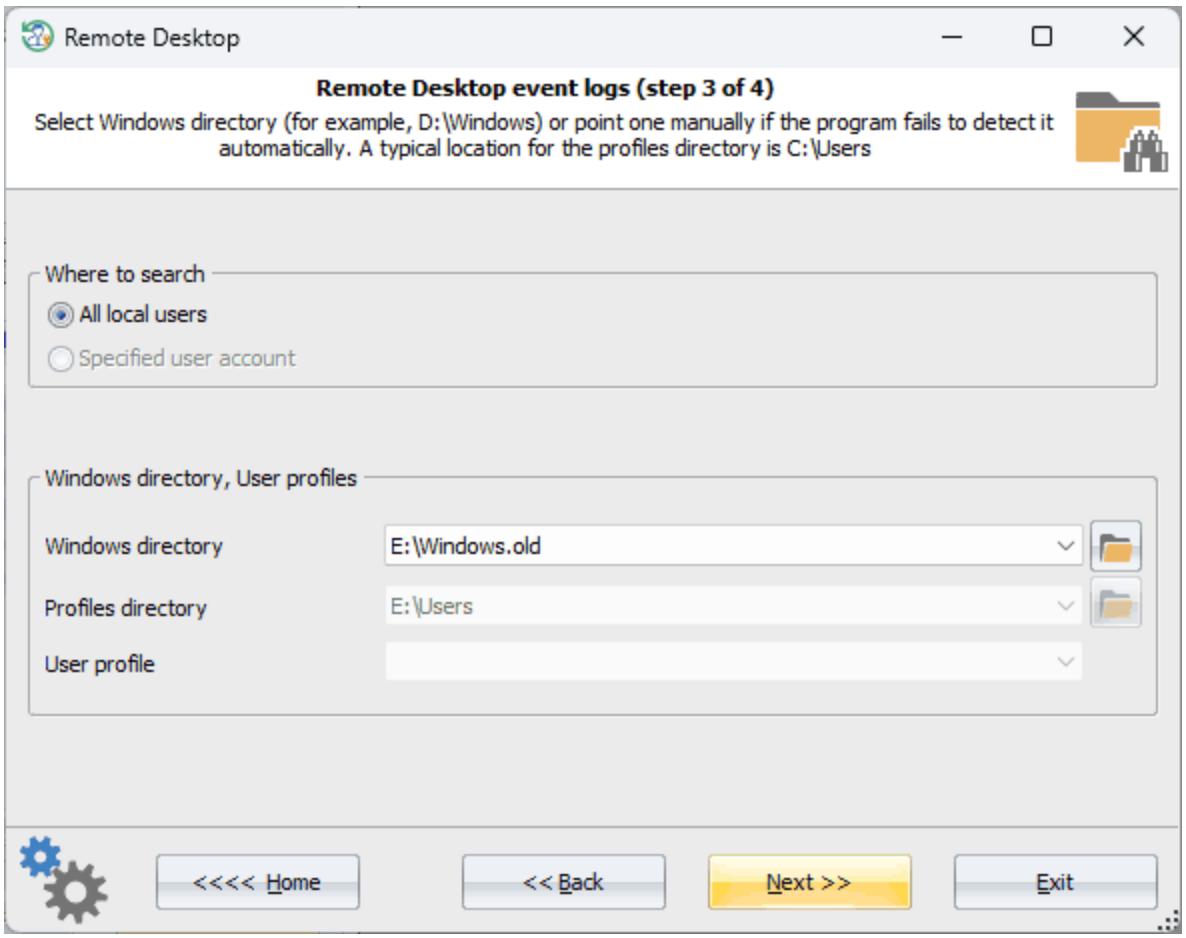
3.7.11.2 Просмотр событий удаленного рабочего стола

При использовании клиента службы терминалов (также известного как подключение к удаленному рабочему столу) в Windows различные события, связанные с клиентом, сохраняются и могут быть просмотрены позже с помощью Просмотрщика событий (Event Viewer). Для просмотра событий, связанных с клиентом службы терминалов, откройте Просмотрщик событий, перейдите в раздел "Журналы приложений и служб", разверните папку "Microsoft" и выберите журнал "TerminalServices-ClientActiveXCore".

Просмотрщик событий - это инструмент в Windows, который позволяет пользователям просматривать и управлять системными и приложенческими журналами. Однако он может быть доступен только после входа в учетную запись. Еще одной проблемой является то, что события, связанные с удаленным рабочим столом, разбросаны по разным журналам и не ограничены только одним журналом "TerminalServices-ClientActiveXCore".

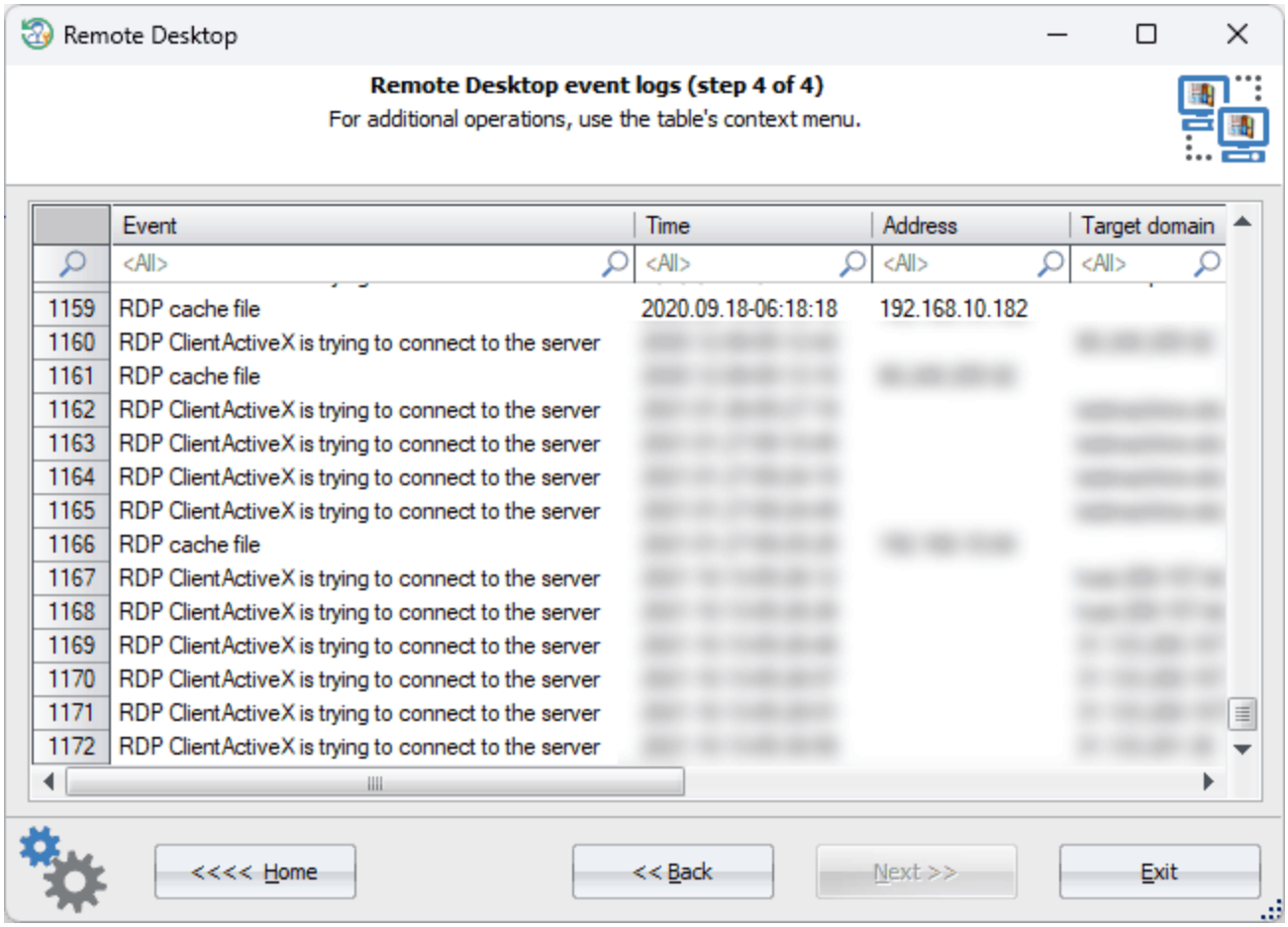
Данная функция программы решает обе проблемы, собирая как можно больше событий, связанных с подключениями RDP и извлекая дополнительные данные из журналов "TerminalServices-RemoteConnectionManager", "RemoteDesktopServices-RdpCoreTS", "TerminalServices-LocalSessionManager", "System" и "Security".

Выбор каталога Windows



Для этого укажите каталог, в котором установлена Windows.

Просмотр журналов удаленного рабочего стола



При просмотре журналов RDP вы можете использовать контекстное меню для сохранения списка в виде отчета HTML.

Обратите внимание, поиска и анализ всех элементов журнала может занять некоторое время.

3.7.11.3 Кэш удаленного рабочего стола

Кэширование изображений, передающихся по протоколу удаленного рабочего стола в Windows, позволяет улучшить производительность удаленных подключений, сохраняя при этом копию экрана удаленного рабочего стола на клиентском устройстве. Это позволяет клиенту RDP быстро выполнять перерисовку, не передавая по сети весь экран удаленного рабочего стола при обновлении, а только измененную его часть.

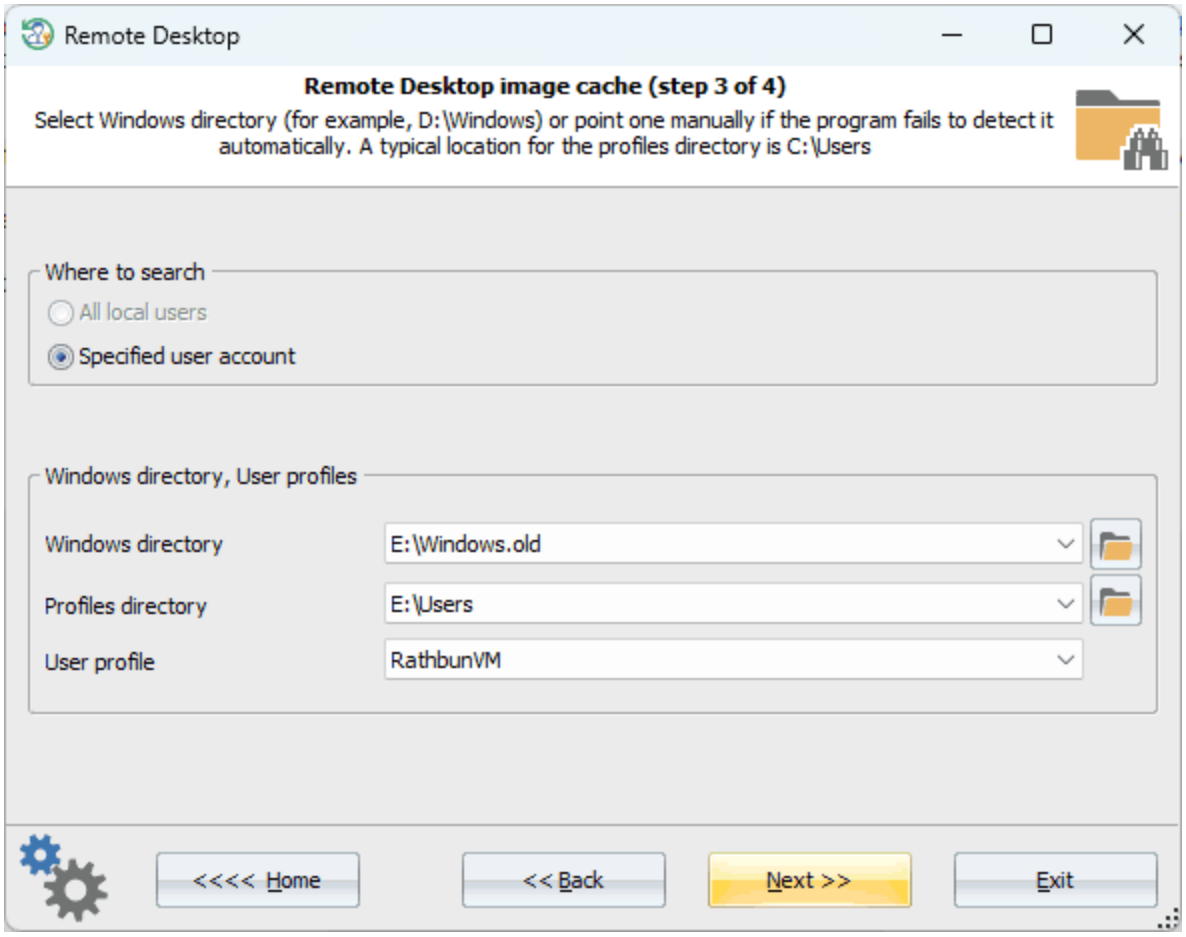
Когда устанавливается удаленная сессия, клиент RDP изначально получает полную карту экрана от сервера и сохраняет его в кэше в памяти. Все последующие обновления удаленного рабочего стола приходят в виде дельта-смещений, которые описывают изменения, внесенные в экран с момента последнего обновления. Эта техника значительно улучшает отзывчивость и прорисовки, особенно в случаях, когда сетевое соединение имеет ограниченную пропускную способность или высокую задержку.

Содержимое кэша памяти затем сохраняется в файлах ".bmc" и ".bin" в папке "c:\Users\<user>\AppData\Local\Microsoft\Terminal Server Client\Cache". Бинарная структура файлов ".bmc" и ".bin" не документирована компанией Microsoft.

Файлы кэша битовых карт состоят из фрагментов (плиток), обычно размером 64 на 64 пикселя, при этом каждая плитка представляет определенную часть удаленного экрана. Некоторые плитки кэша сохраняются затем из памяти в файлы ".bin" и доступны даже после завершения удаленной сессии.

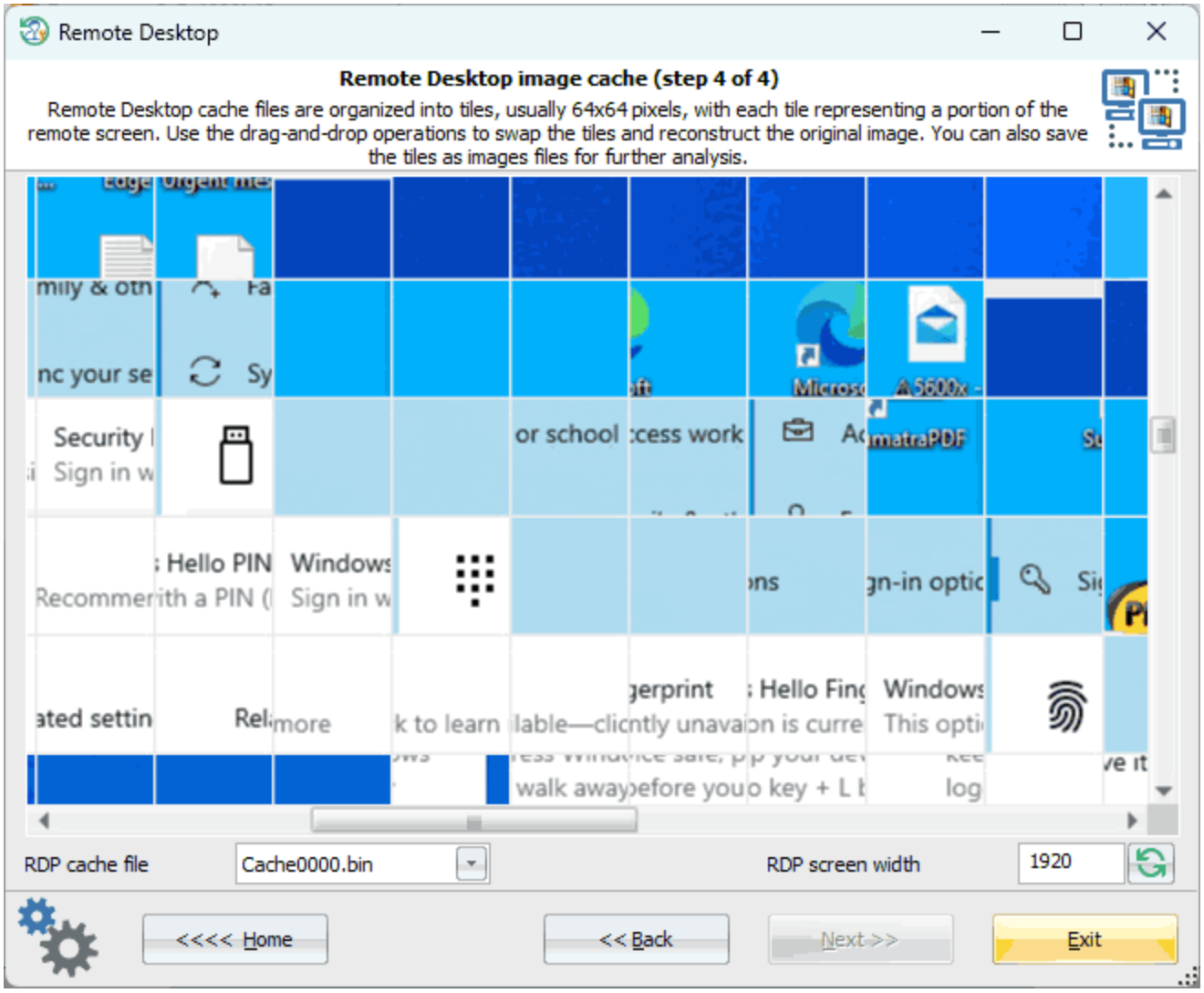
При помощи Reset Windows Password можно восстановить исходное изображение удаленного экрана или, по крайней мере, его часть, используя операции перетаскивания плиток. Однако, это может потребовать некоторых усилий и времени.

Выбор учетной записи, с который был вход в удаленный рабочий стол



Выберите учетную запись пользователя, для которой необходимо выполнить поиск кэша удаленного рабочего стола.

Просмотр кэша удаленного рабочего стола



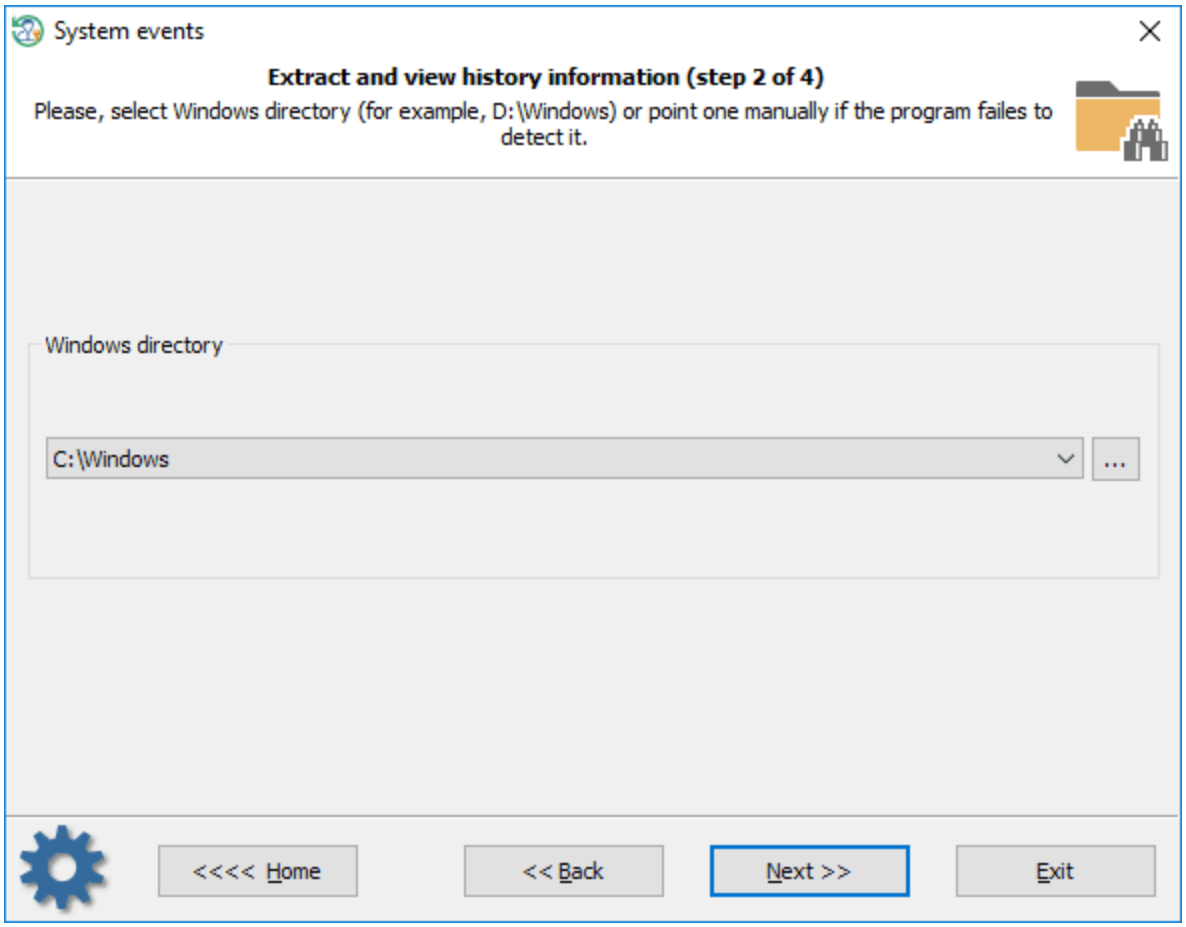
Просмотр и редактирование кэша RDP. Используйте операции перетаскивание для замены любых двух фрагментов. Если вы хотите сохранить всю битовую карту, отдельную плитку или все плитки сразу, выберите соответствующий пункт контекстного меню.

3.7.12 Системные события

Операционная система Windows постоянно ведет запись в журнал разных событий, которые возникают в системе. Например, это могут быть проблемы в установке устройств, ошибки в работе приложений, уведомления о критических событиях безопасности и т.д. События регистрируются в журналах Windows в хронологическом порядке и помогают устранять ошибки, выполнять диагностику и мониторинг системы, поддерживать ее безопасность. Журнал событий представляет собой *.evtx файл. Каждый evtx файл соответствует определенному источнику событий или компоненту операционной системы. Например, в system.evtx записываются системные события. В security.evtx сохраняются все события безопасности.

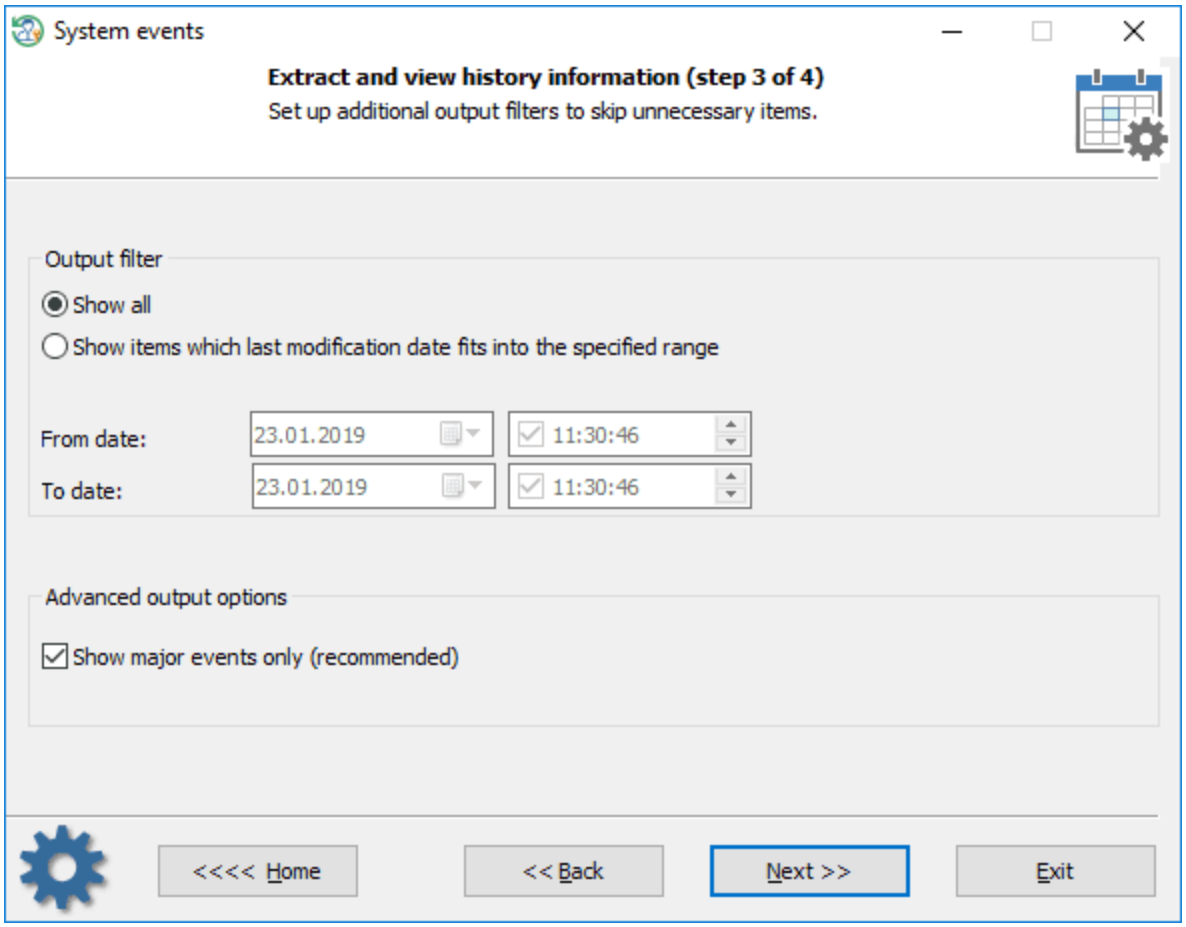
Утилита для просмотра событий представляет собой простейший компонент программы, который позволяет отображать основные события, происходящие в операционной системе Windows Vista и новее. Например, загрузка/выключение ОС, вход в/выход из учетной записи, установка драйвера и т.д.

Выбор каталога Windows



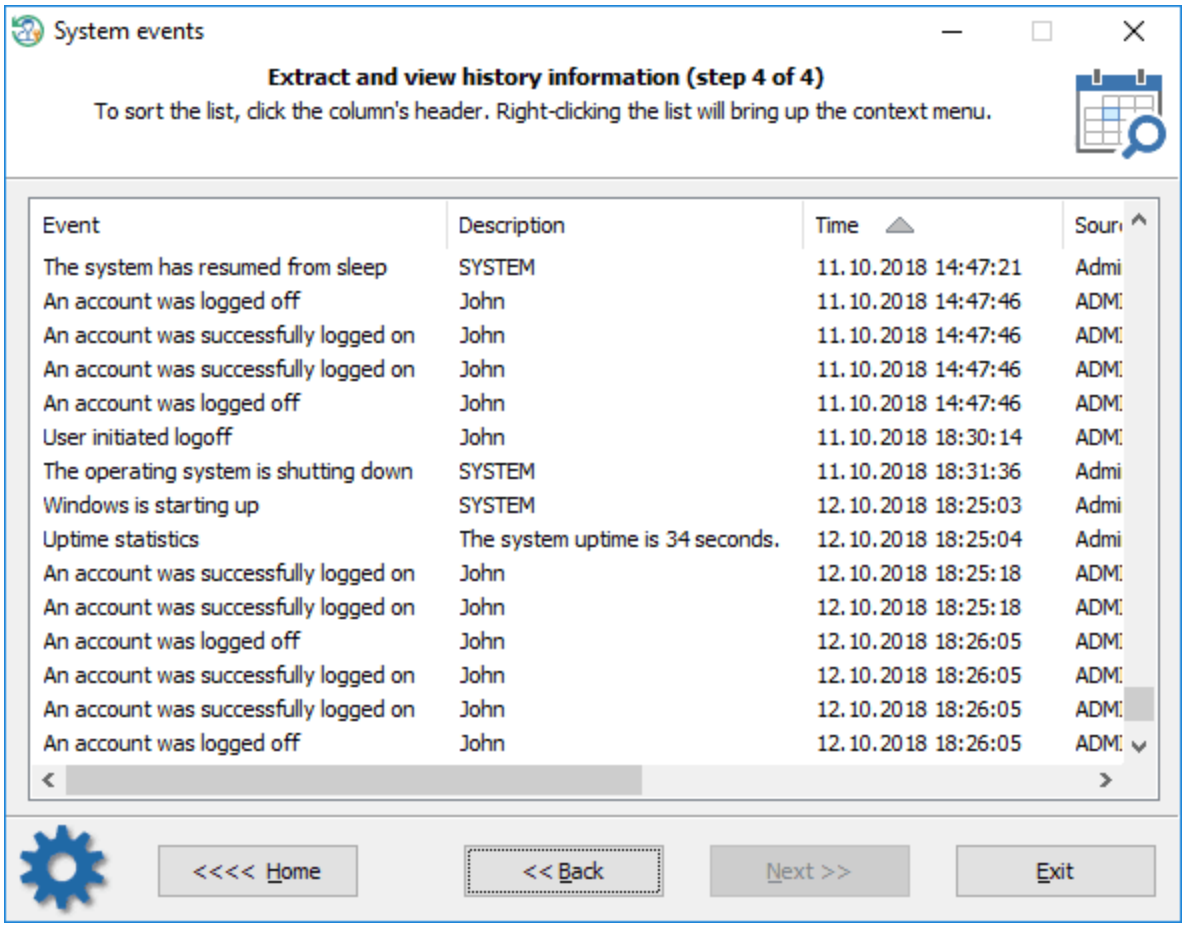
Сначала необходимо выбрать папку Windows, в которой находятся журналы событий.

Установка фильтров отображения



На следующем шаге можно настроить дополнительные фильтры вывода для отображения событий, которые происходили за определенный период. Дополнительная опция предназначена для поиска всех событий. Если она не установлена, то программа отображает только основные/известные события.

Системные события Windows



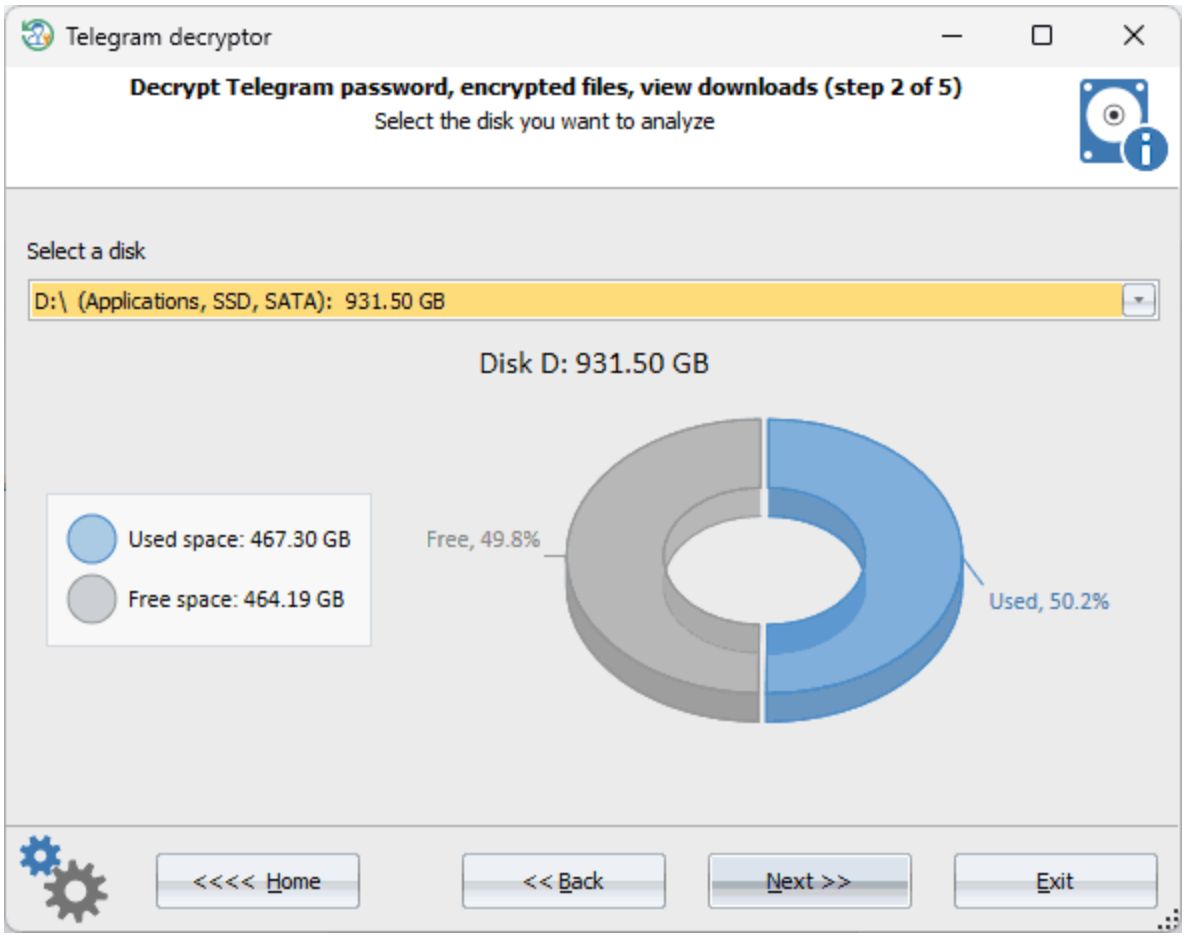
Сбор и обработка информации может занять значительное время, в зависимости от размера журналов событий. Для того, чтобы скрыть определенные, не интересующие вас записи, щелкните правой кнопкой мыши на списке событий и выберите один из пунктов для удаления ненужной информации. Для сортировки событий, щелкните по заголовку соответствующего столбца.

3.7.13 Расшифровщик Telegram

Как известно, популярный кроссплатформенный мессенджер **Telegram** является одним из самых популярных систем для обмена мгновенными сообщениями. Его можно скачать и установить на операционную систему Windows, где он поставляется как приложение **Telegram Desktop**. Telegram имеет надежную встроенную защиту. Все локальные файлы, которые используются приложением - настройки, кэш, картинки и т.д. - надежно зашифрованы.

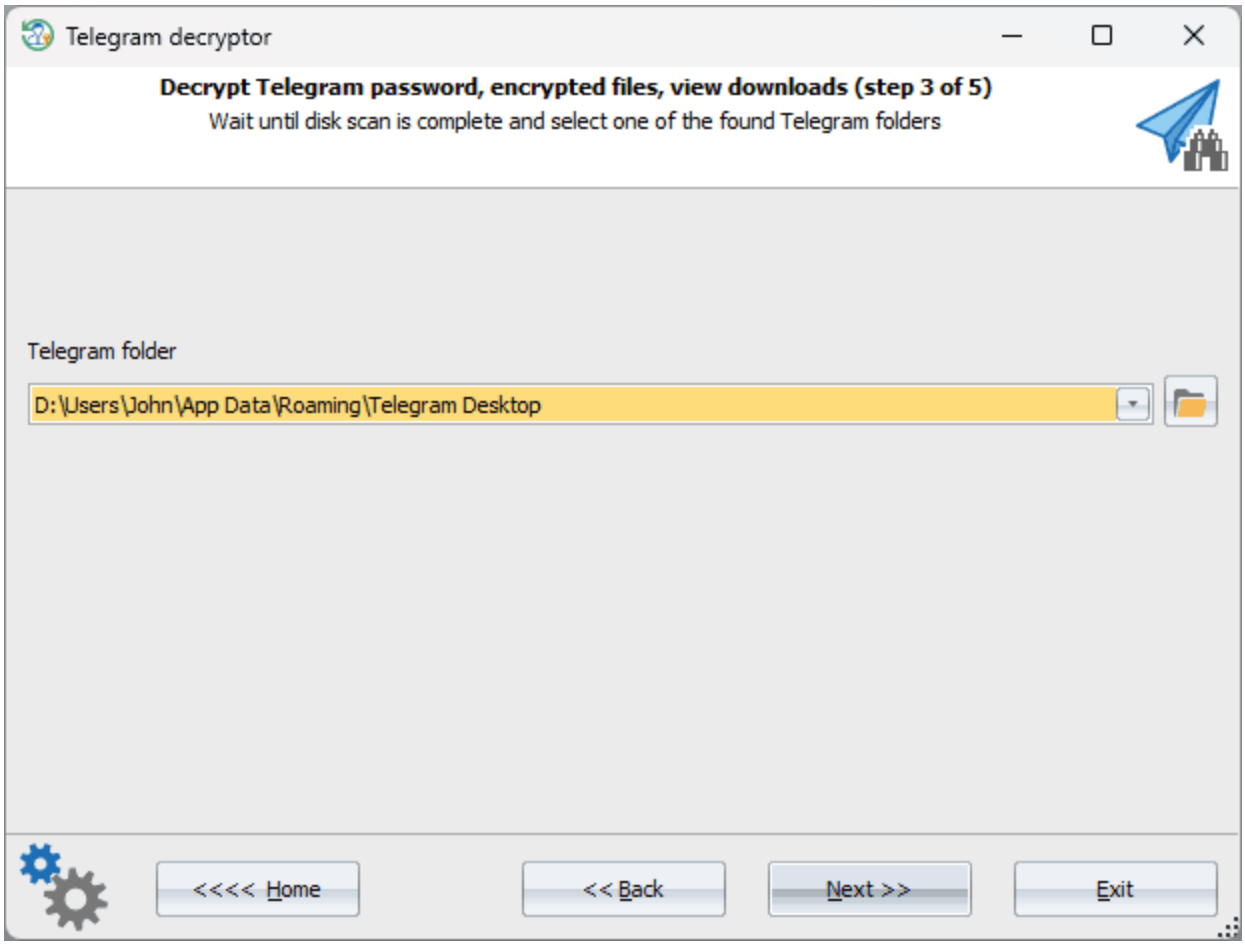
Данная функция Reset Windows Password предназначена для поиска основного пароля, расшифровки файлов и просмотра закачек приложения Telegram Desktop.

Выбор диска для поиска



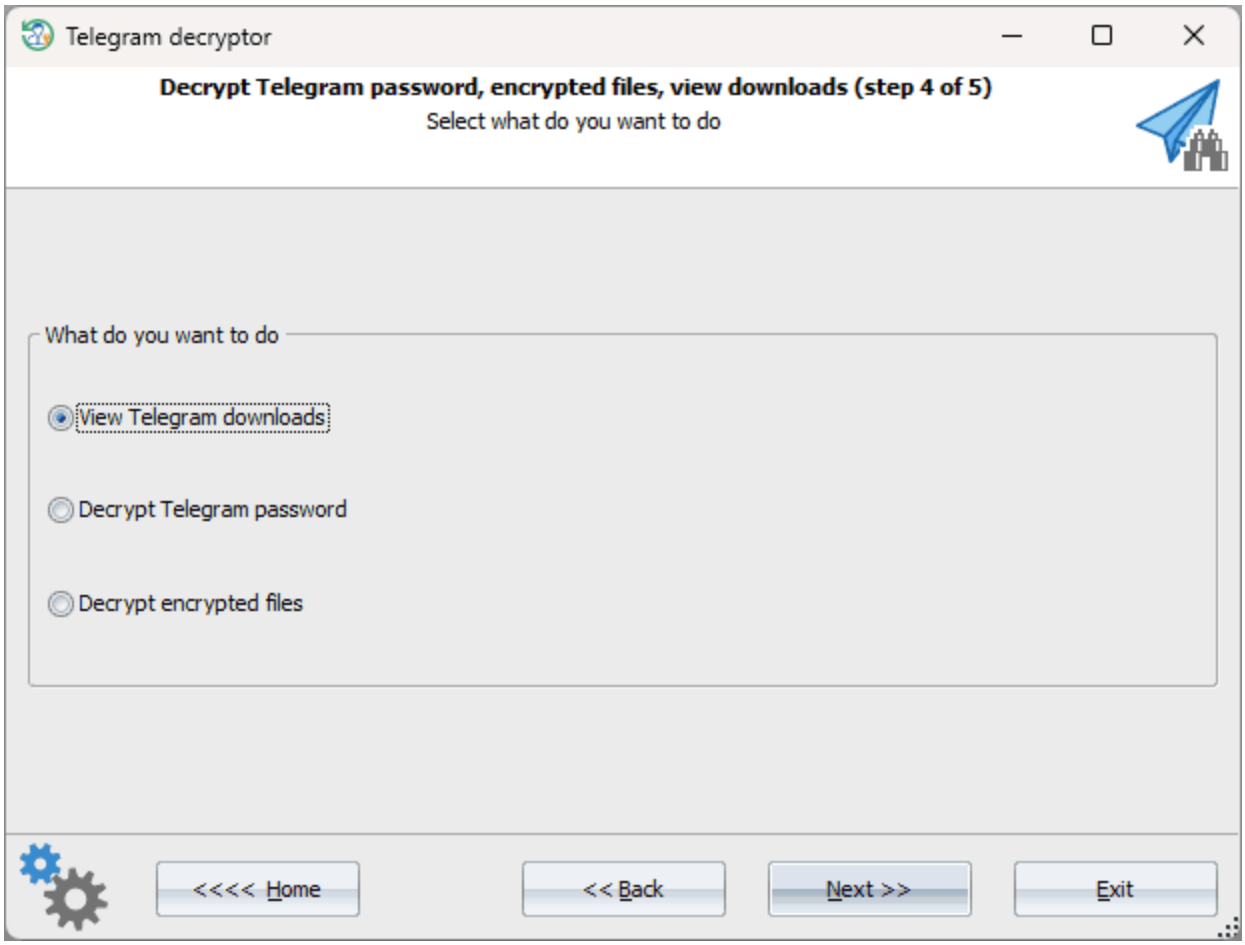
Выберите диск, на котором необходимо выполнить поиск каталогов Telegram Desktop.

Выбор каталога Telegram



После того, как диск выбран, программа начнет немедленный поиск каталогов Telegram на диске. Имейте в виду, первое сканирование, если этот диск еще не был кэширован, может занять несколько минут. В дальнейшем поиск, как правило, занимает секунды. Программа гарантирует успешное нахождение всех каталогов Telegram Desktop на выбранном диске, где бы они не находились.
Найденные каталоги Telegram можно выбрать из выпадающего списка. Выберите нужный вам каталог, если их несколько, чтобы продолжить.

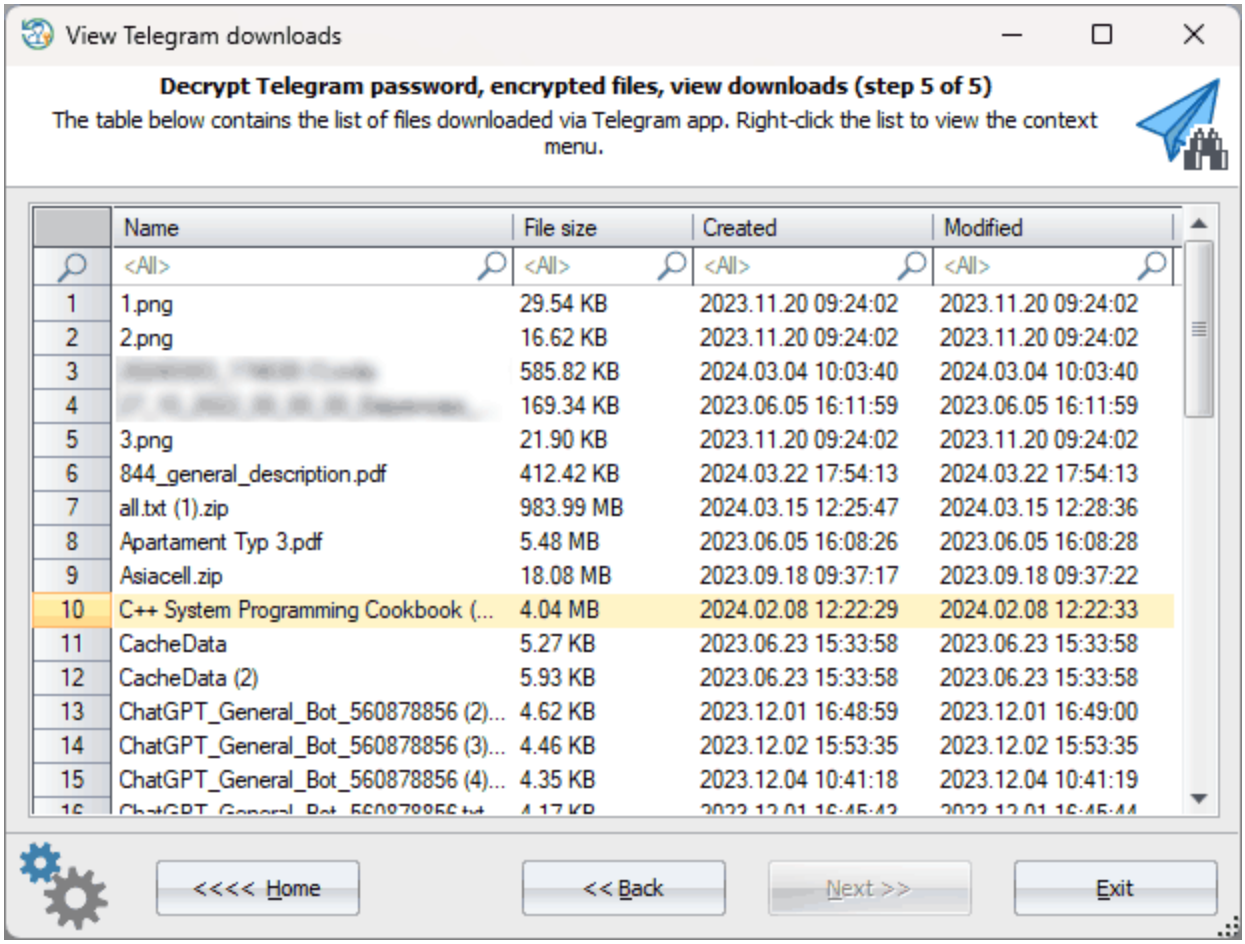
Дальнейшие действия



Выберите дальнейшие действия, доступные для найденного каталога:

- Просмотр файлов, которые были скачаны на компьютер через Telegram
- Расшифровка начального пароля Telegram
- Расшифровка локальных файлов Telegram

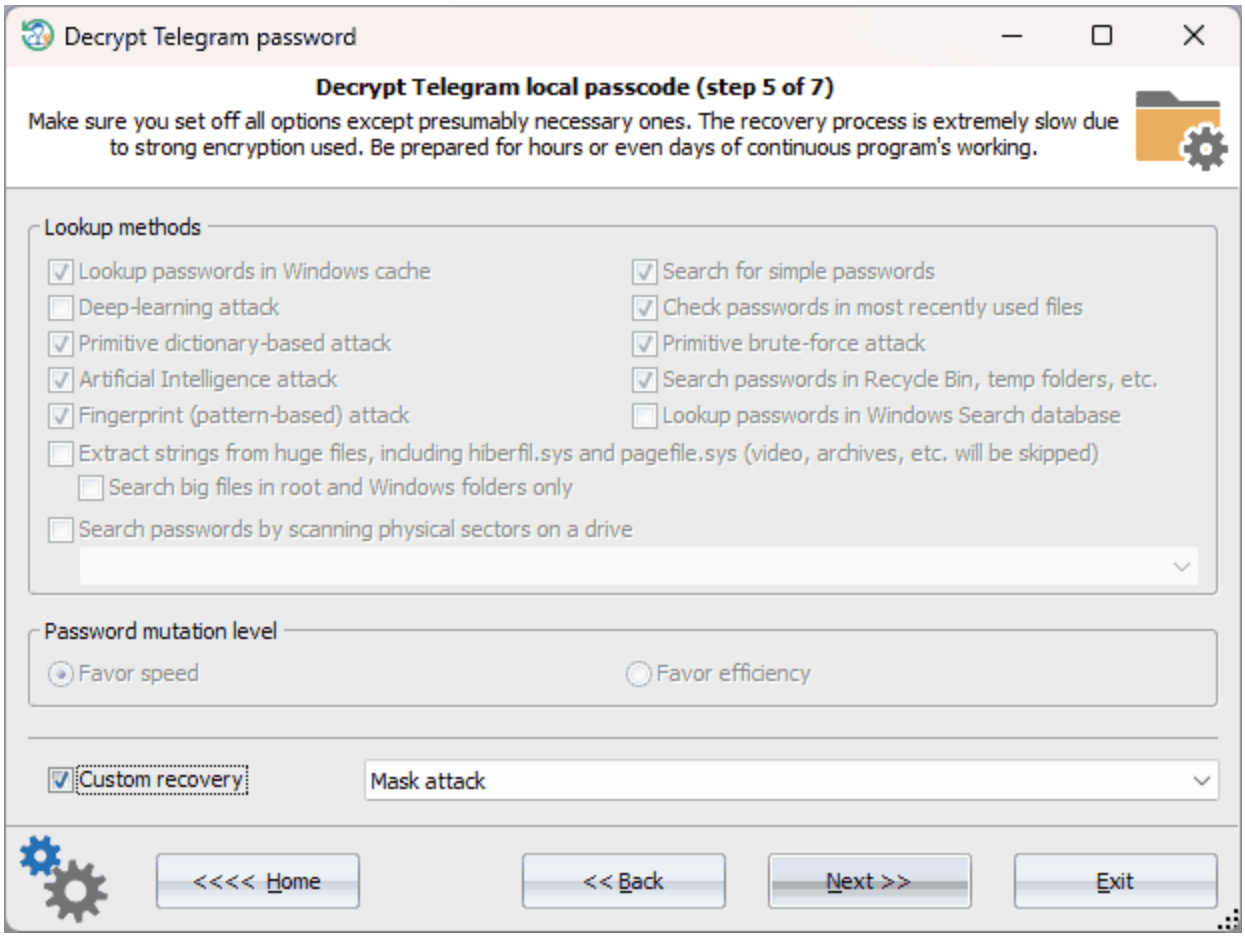
3.7.13.1 Скачанные файлы Telegram



Скачанные через Telegram файлы представлены в виде списка. Вы можете открыть папку с этими файлами, создать текстовый или HTML отчет или сделать бэкап одного или нескольких файлов.

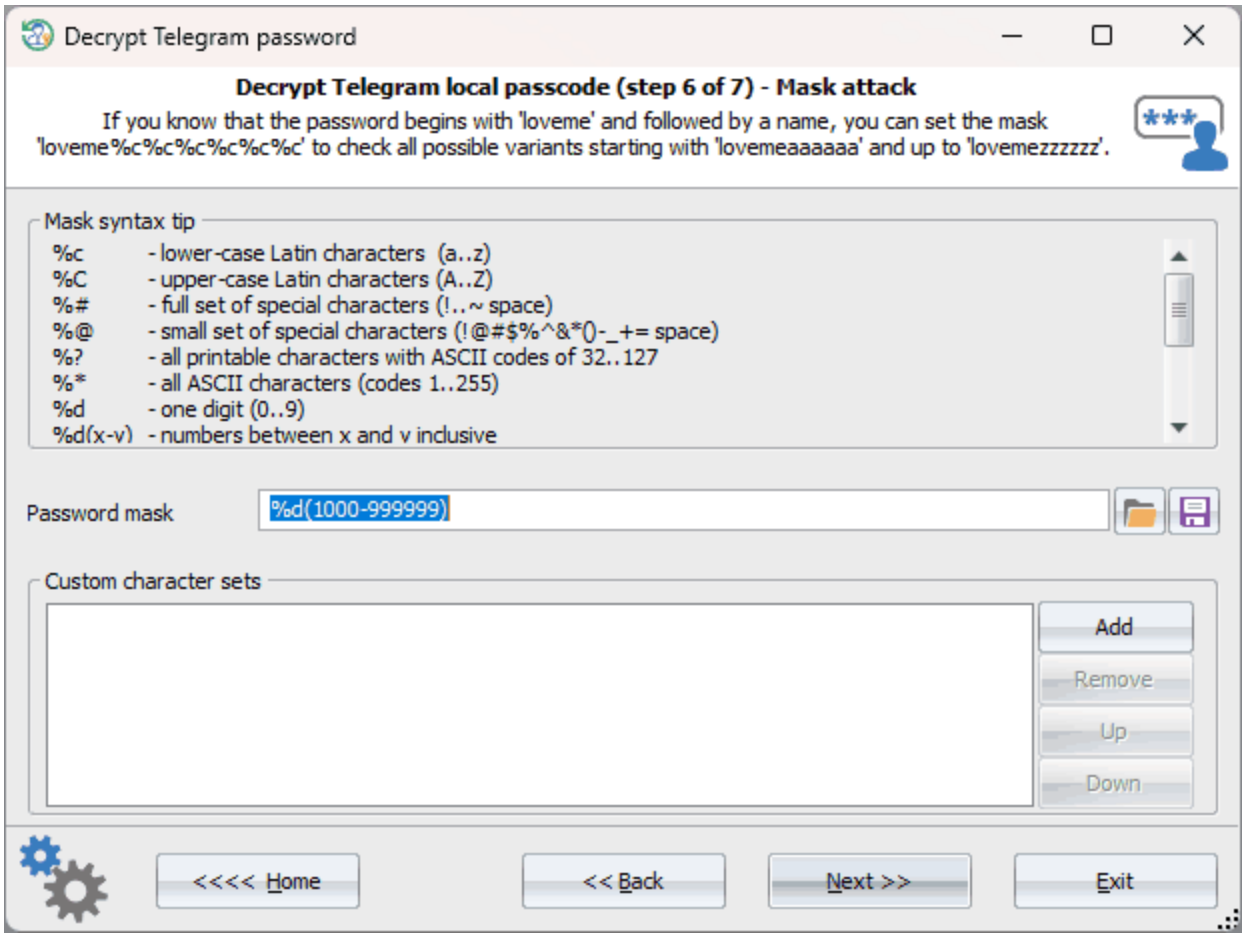
3.7.13.2 Расшифровка пароля Telegram

Выбор и настройка методов восстановления пароля



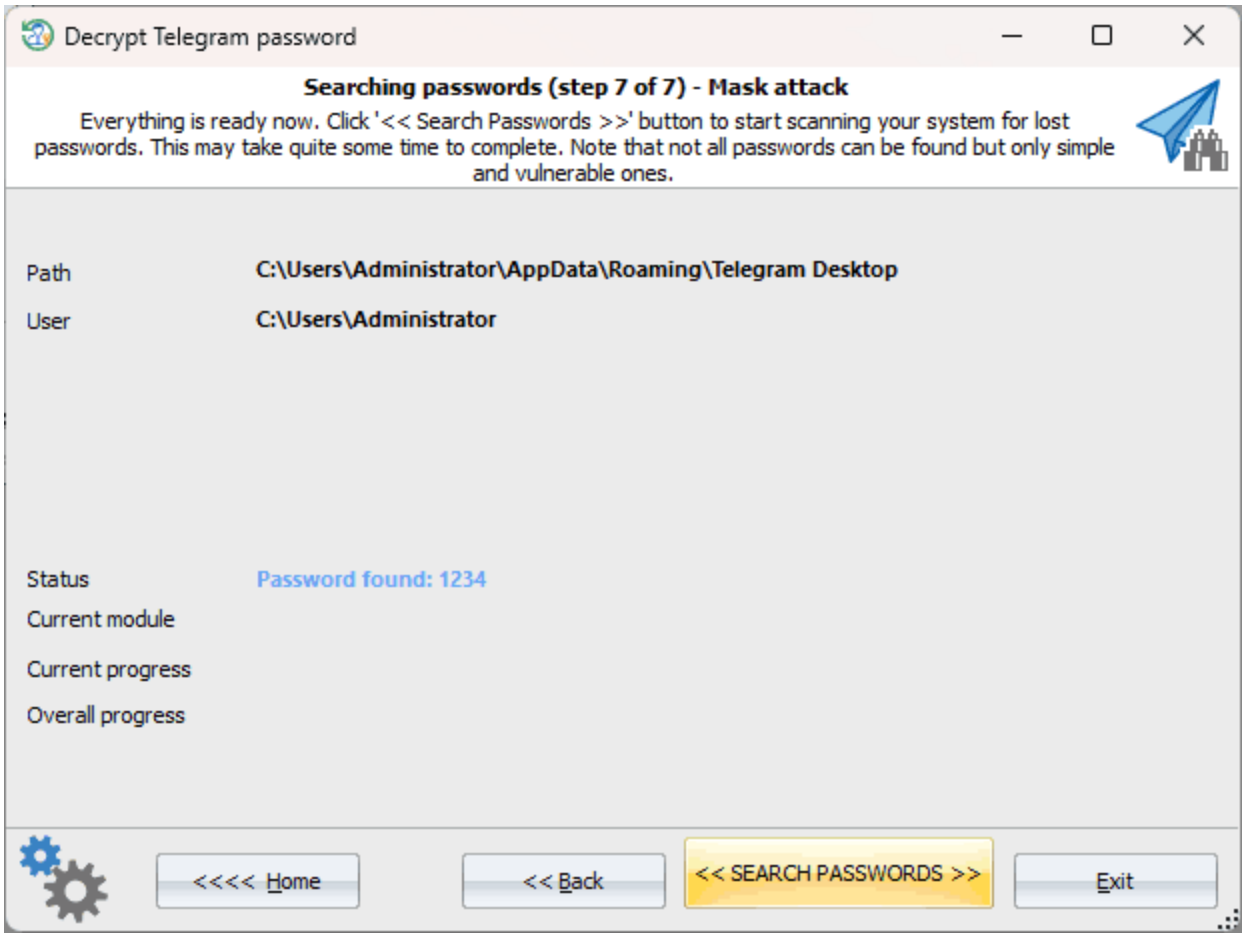
Пароль Telegram имеет сильную встроенную защиту. Перебор таких паролей происходит со скоростью всего несколько штук в секунду. Поэтому в самом начале необходимо выбрать правильный метод восстановления. В противном случае, поиск займет неопределенно долгое время. Рекомендуется использовать пользовательские атаки, если известно что-либо о паролей. Если нет, можно переключиться на стандартный поиск, отключив при этом самые затратные по времени опции, оставив как минимум две важные: поиск паролей в кэше Windows и Интеллектуальную атаку.

Настройка каталогов или пользовательских атак



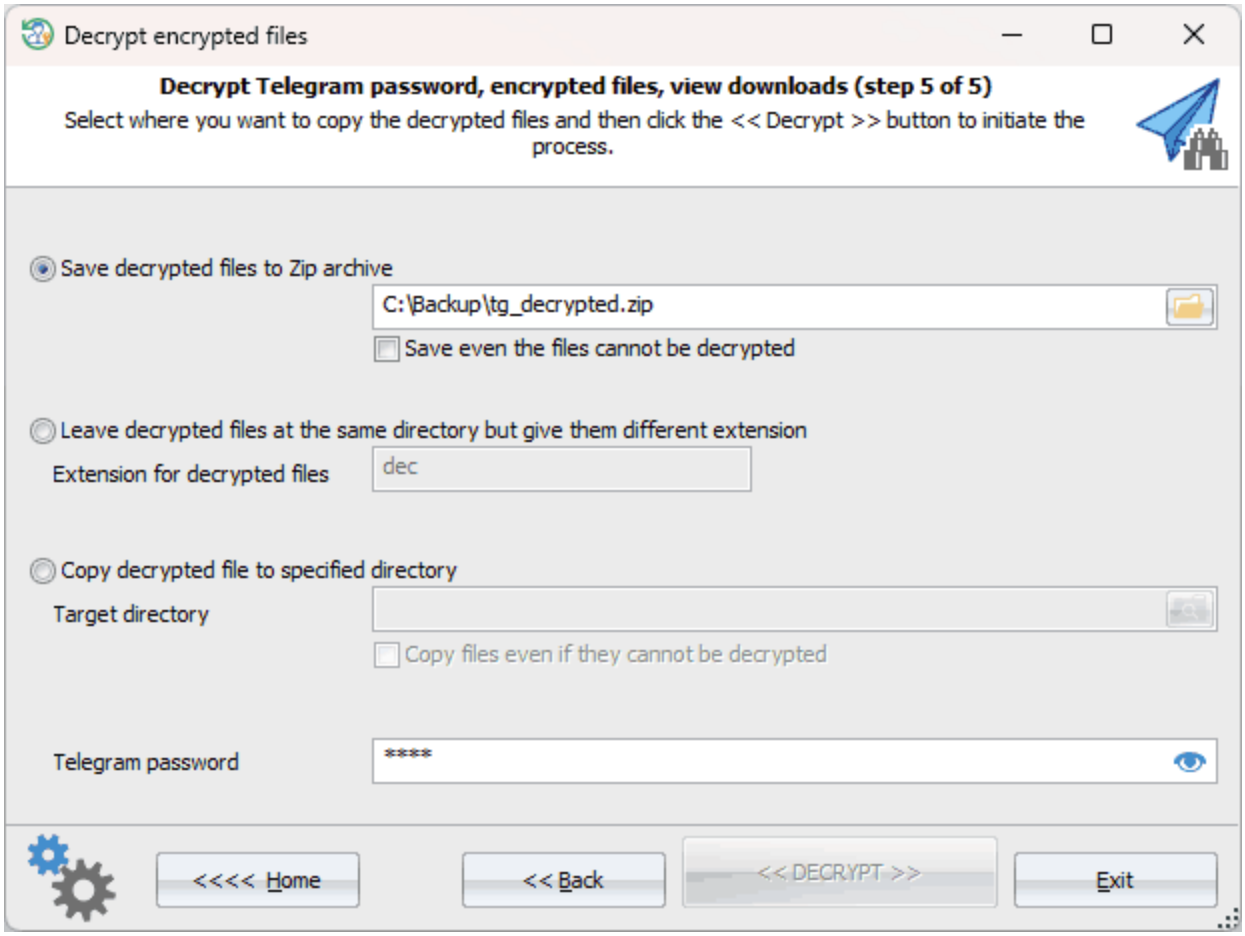
Если выбрана одна из пользовательских атак, необходимо выполнить ее предварительную настройку. Например, на приведенной выше картинке задана атака по маске, которая будет перебирать цифровые пароли от 4 до 6 символов. Т.е. от '1000' до '999999'.

Поиск пароля Telegram



Несмотря на то, что алгоритмы, которые используются в шифровании пароля Telegram, максимально оптимизированы, будьте готовы к тому, что любой перебор паролей, даже самых простых, может занять очень много времени. Любопытно, что программа работает намного быстрее, чем популярная утилита Hashcat. Однако, к сожалению, загрузочная среда имеет ограничения на использование только центрального процессора, в то время как нет возможности использовать более производительные видеокарты.

3.7.13.3 Расшифровка файлов Telegram



Если пароль Telegram известен или не задан, то расшифровка локальных файлов представляется довольно тривиальной задачей. В противном случае, необходимо сначала расшифровать начальный пароль Telegram.

Вы можете выбрать один из трех способов расшифровки, более удобный для вас:
- Создать ZIP архив и скопировать в него все локальные файлы, которые будут расшифрованы
- Оставлять расшифрованные файлы в исходном каталоге, но под другим расширением. Например, если задать расширение DEC, то расшифрованные файлы будут иметь вид XXXXXX.DEC, YYYYYY.DEC и т.д.
- Копировать расшифрованные файлы в выбранный каталог

Полученные таким образом файлы можно использовать для дальнейшего анализа. Например, расшифрованный файл **maps** содержит имя и телефон пользователя Telegram.

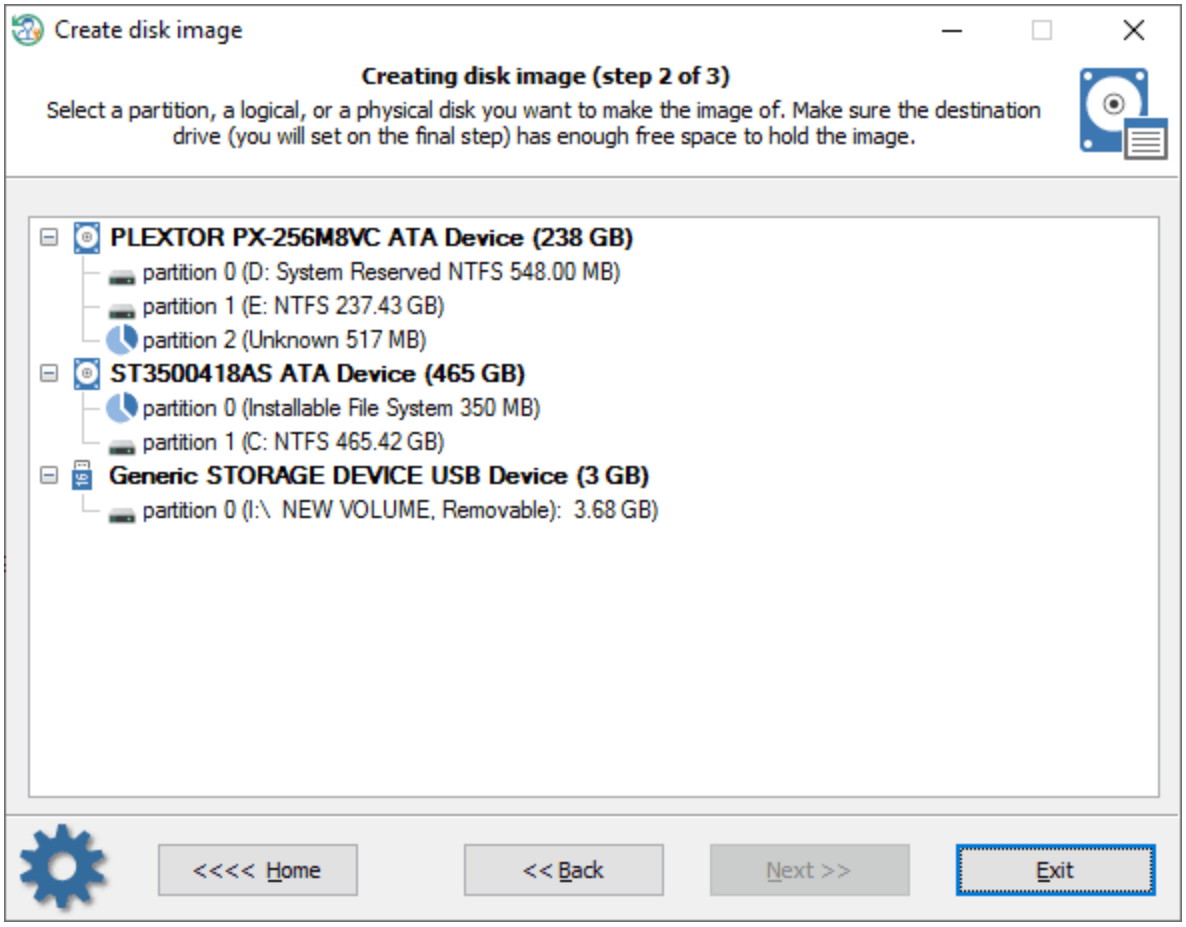
3.8 Файлы и диски

3.8.1 Создание образа диска

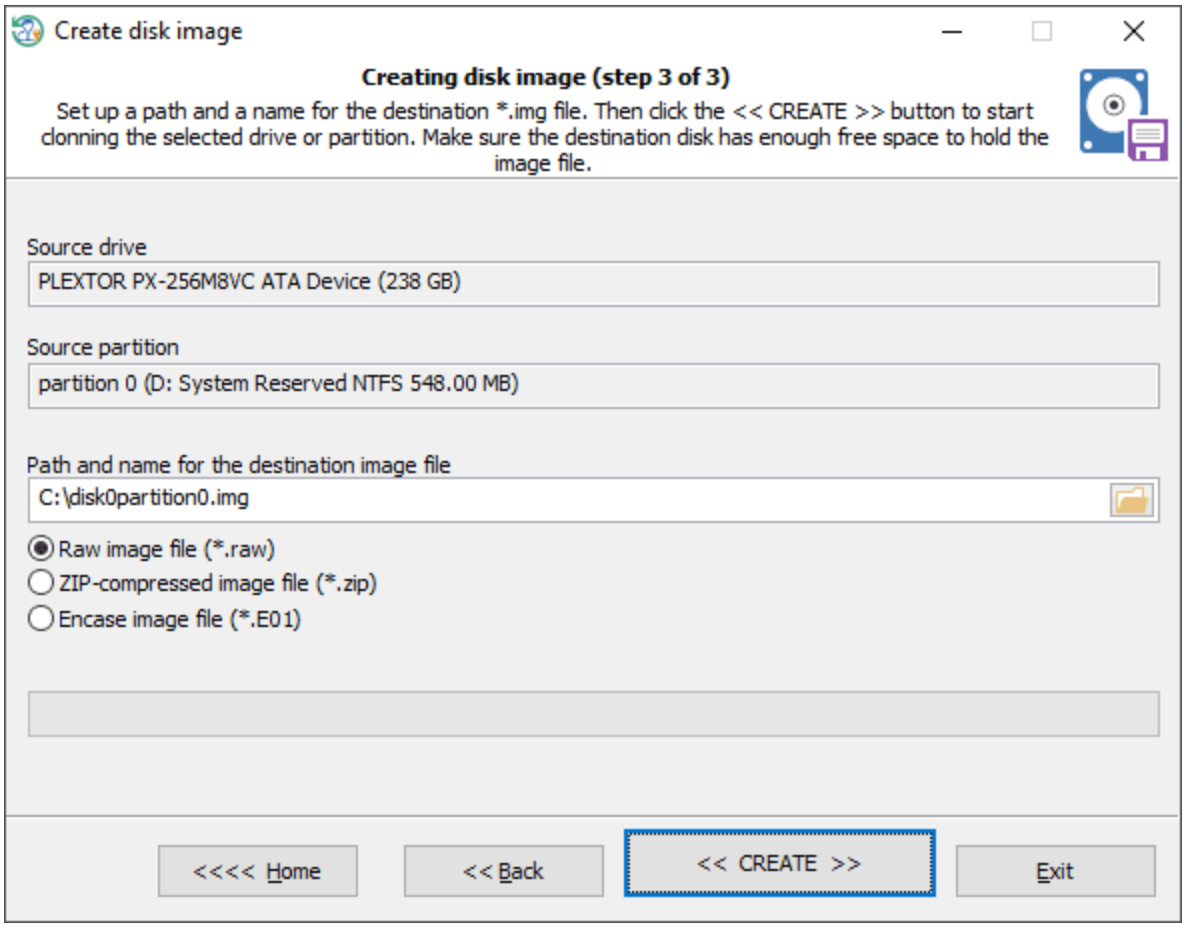
Когда повреждена и не загружается ОС Windows или вышел из строя жесткий диск, крайне важно вовремя создать резервную копию всего содержимого вашего диска, включая шифрование, состояние Операционной Системы, ее настройки, пароли, установленные приложения, драйверы, всю личную информацию и т.д. Один из самых простых способов сделать это - создать образ всего жесткого диска.

В криминалистике образ диска является обязательным и позволяет как сэкономить время во время начального расследования, так и гарантировать, что при дальнейшем углубленном анализе не будет упущено никакой важной информации.

Создание образа диска в RWP чрезвычайно просто.



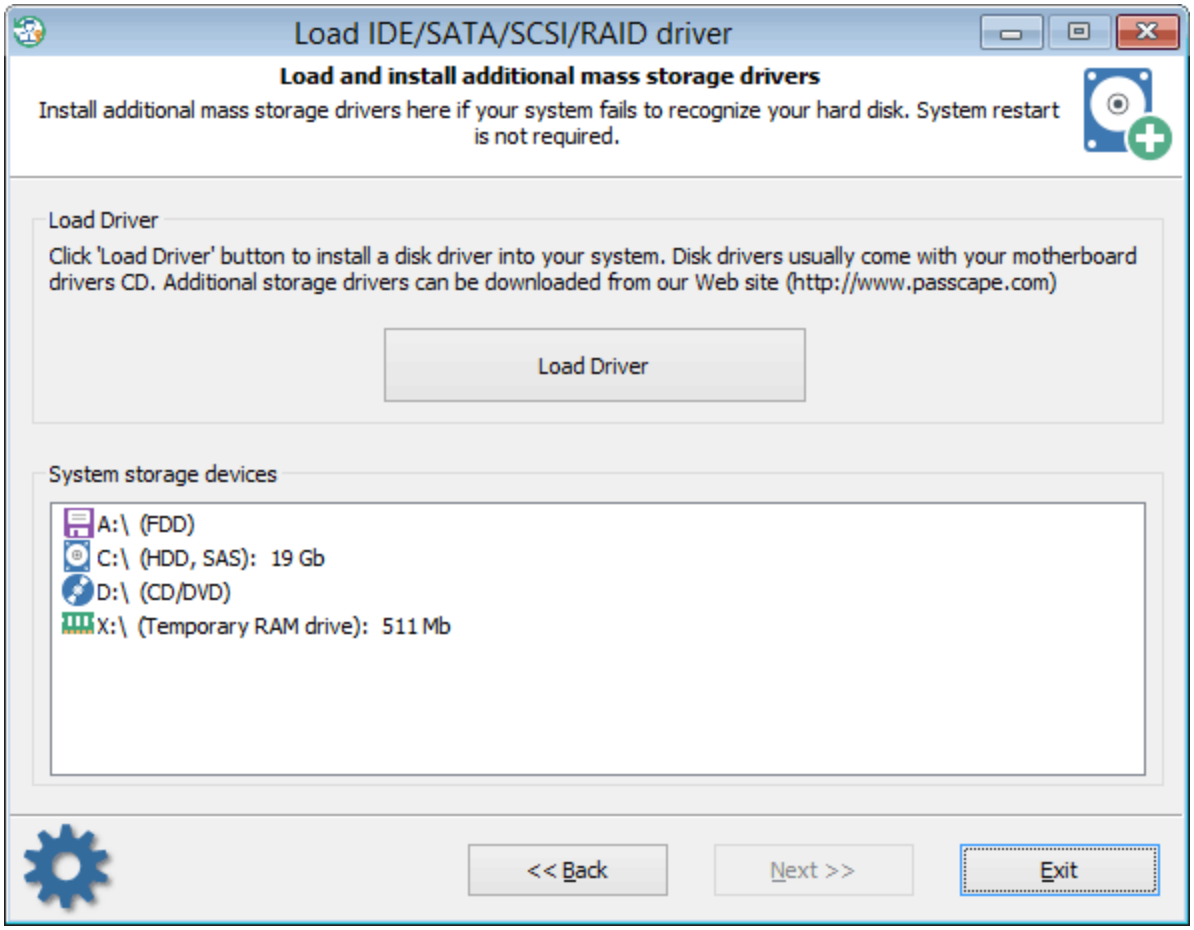
В первом диалоговом окне программа отображает список найденных дисков и принадлежащих им разделов. Выберите раздел или диск, образ которого вы хотите создать.



В заключительном диалоговом окне задайте имя образа и путь, по которому будет сохранен этот файл. Обратите внимание, что целевой путь должен быть расположен на другом физическом диске. Также убедитесь, что на целевом диске достаточно свободного места для хранения образа. Нажмите кнопку *"<< Создать >>"* , чтобы запустить процесс создания образа диска. Будьте терпеливы, это может занять некоторое время и зависит от скорости как исходного, так и целевого диска.

Дополнительно доступна опция сжатие образа. После ее установки файл с образом будет сжат в zip-архив.

3.8.2 Загрузка драйверов жесткого диска



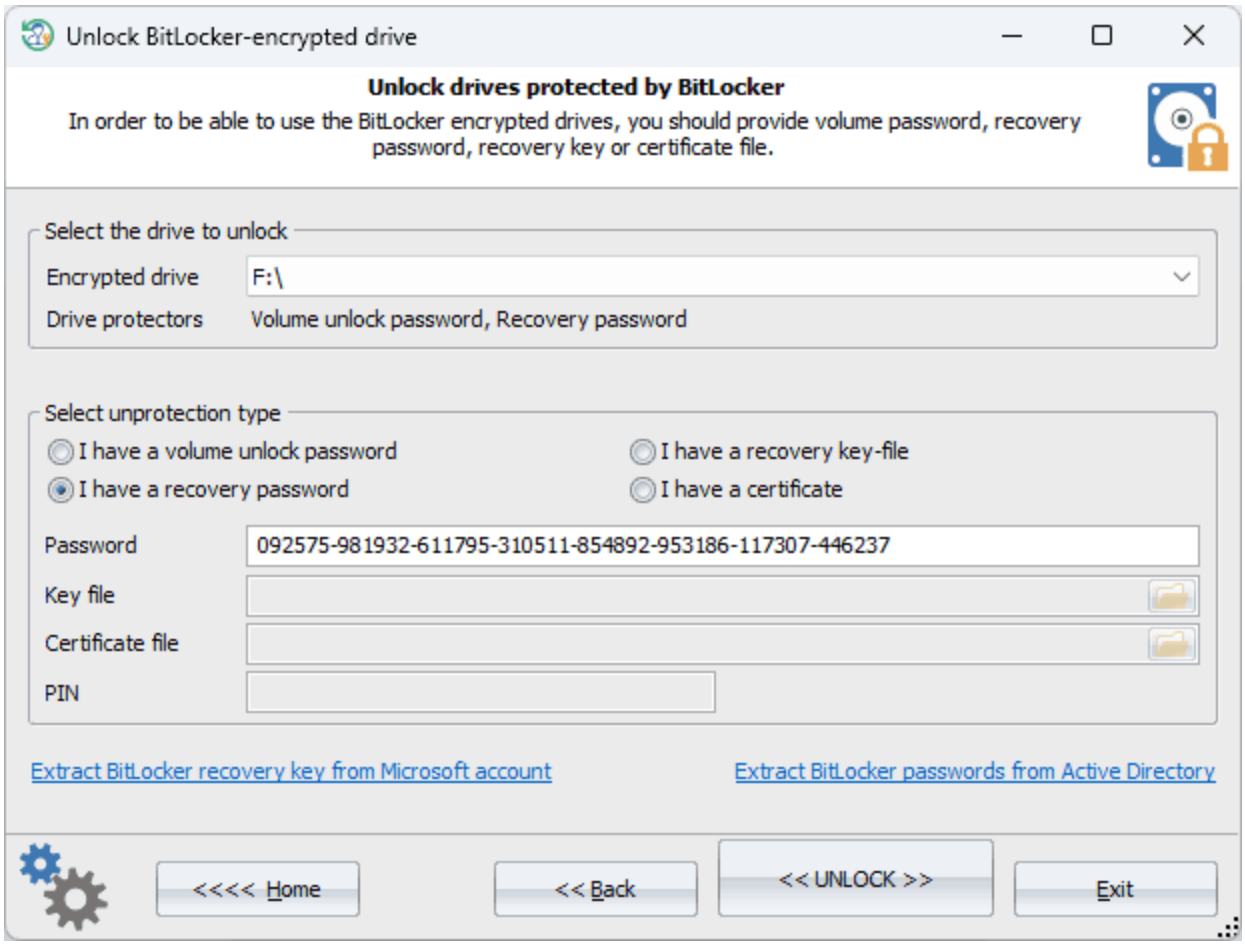
Если при запуске программа не смогла определить один или несколько жестких дисков, то вам, скорее всего, потребуется установить драйвер для этого устройства. В главном окне в списке задач выберите '*Загрузка IDE/SATA/SCSI/RAID/NVME драйвера*' и перейдите на страницу установки драйвера.

С программой поставляются несколько популярных драйверов контроллеров жестких дисков: ATI, Highpoint, Intel, Jmicron, Marvell, Nvidia, Silicion Image, Sis, Uli, Via, Vmware. Все они находятся в папке **X:\Apps\Drivers**. Например, если контроллер вашего HDD построен на базе чипсета Nvidia, загрузите соответствующий *.INF файл из папки X:\Apps\Drivers\Nvidia.

Обычно при покупке нового PC 'в нагрузку' выдают компакт диск с драйверами материнской платы и жесткого диска. Можно, и даже желательно, воспользоваться этим диском для установки драйверов отсутствующих устройств. Будьте внимательны! Программе требуются драйвера для операционной системы Windows 11 x64. Ознакомьтесь, пожалуйста, с руководством вашей материнской платы для более подробной информации по установке драйверов.

Установка драйвера в Reset Windows Password осуществляется 'на лету', поэтому перезагрузка системы не требуется. При этом в списке устройств хранения информации должны появиться новые найденные устройства. После того, как будет установлен соответствующий драйвер и найден жесткий диск, можно приступать к дальнейшей работе.

3.8.3 Расшифровка Bitlocker дисков



Если один из дисков зашифрован при помощи Bitlocker, то его содержимое изначально недоступно. Разблокировать и получить доступ к диску можно одним из четырех способов: предоставив пароль тома, цифровой пароль восстановления, ключ восстановления или сертификат.

Выберите доступный для вас метод и нажмите кнопку << *UNLOCK* >> для расшифровки диска.

Для извлечения паролей Bitlocker в домене, перейдите по ссылке Extract BitLocker passwords from Active Directory и следуйте указаниям программы.

Очень часто ключ восстановления BitLocker хранится в учетной записи Майкрософт. В этом случае, для получения ключа восстановления BitLocker, необходимо воспользоваться следующей простой инструкцией:

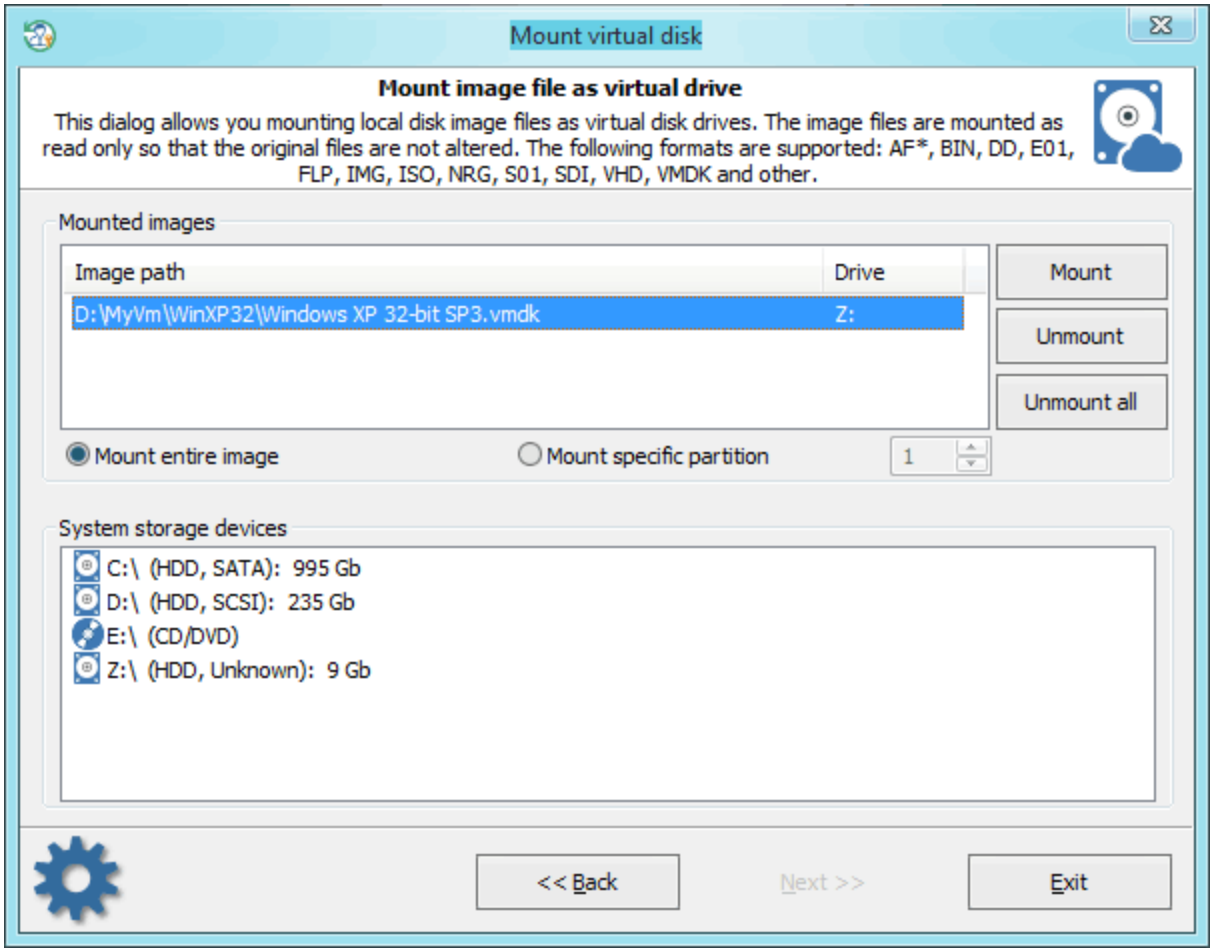
- Убедитесь, вы подключены к Интернет при помощи проводного соединения.
- Убедитесь, что вы помните логин (адрес электронной почты) своей учетной записи Майкрософт и пароль. Если нет, сначала восстановите пароль.
- Нажмите на ссылку *'Извлечь ключ восстановления BitLocker из учетной записи Microsoft'* в левом нижнем углу окна. После установки сетевых драйверов и подключения к Интернету программа откроет

страницу вашей учетной записи Майкрософт, где следует ввести адрес электронной почты вашей учетной записи Microsoft и пароль.
- Следуйте инструкциям на экране, чтобы войти в свою учетную запись. Вас могут попросить пройти второй фактор аутентификации. Например, предоставить ключ безопасности, отправленный на ваш адрес электронной почты. Будьте готовы к этому.
- После входа в учетную запись, идентифицируйте свое устройство и найдите там 48-значный ключ восстановления BitLocker. Скопируйте этот ключ в буфер обмена.
- Теперь вернитесь в диалоговое окно RWP, выберите *'У меня есть пароль восстановления'* и вставьте туда ключ из буфера обмена.
- Нажмите кнопку *<<РАЗБЛОКИРОВАТЬ>>*, чтобы разблокировать и расшифровать накопитель.

Вы можете использовать эту инструкцию, чтобы получить доступ к вашему зашифрованному BitLocker диску, даже если Windows запрашивает ключ восстановления BitLocker и не удается загрузить ОС. Например, после смены оборудования (таких как добавление или удаление видео или сетевой карты), обновления BIOS или изменения некоторых параметров BIOS, таких как TPM или безопасной загрузки.

Точное местоположение вашего ключа восстановления зависит от метода, который вы использовали для его резервного копирования при включении шифрования BitLocker.

3.8.4 Монтирование виртуального диска



В этом диалоге вы можете создать виртуальный диск из файла с образом. В последствии, можно обращаться к новому виртуальному диску по соответствующей букве тома. Образы монтируются в режиме только-для-чтения чтобы избежать модификации файла. Таким образом, например, можно создать виртуальный привод из файла-образа виртуальной системы VMWare и обращаться к нему как к обычному диску: искать пароли, делать дамп хэшей и т.д. Однако сброс паролей на таком диске не пройдет т.к. он будет доступен только для чтения.

Если начальный образ содержит два или более файловых раздела, необходимо установить соответствующую опцию и указать номер раздела, который нужно монтировать. В противном случае, монтируется весь образ целиком.

Поддерживаются следующие форматы образов: AF*, BIN, DD, E01, FLP, IMG, ISO, NRG, S01, SDI, VHD, VMDK и некоторые другие.

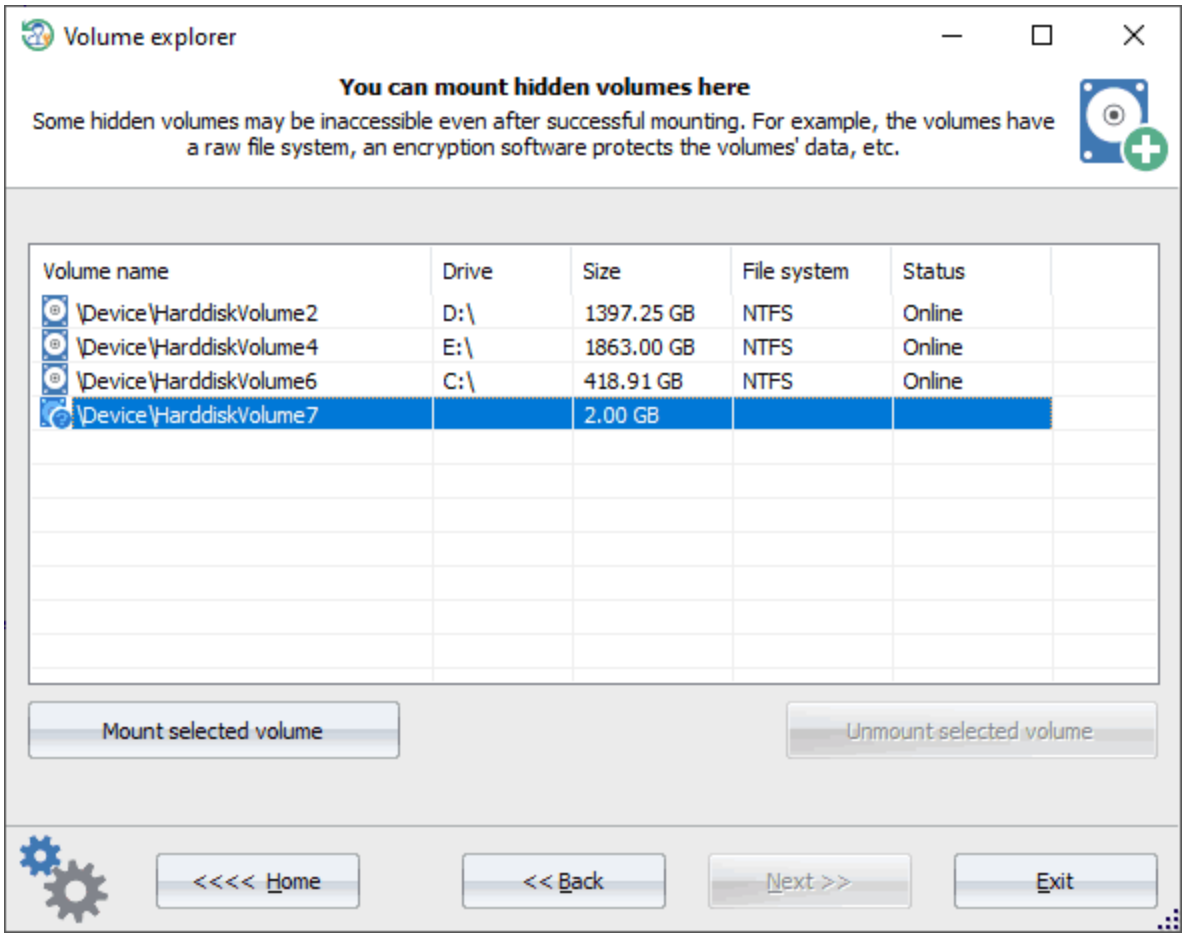
Чтобы закончить работу с виртуальным диском, просто выделите его в списке и нажмите кнопку 'Unmount'. При выходе из программы, все монтированные виртуальные диски будут автоматически отключены.

Для работы с зашифрованными BitLocker образами, сначала смонтируйте BitLocker образ, затем расшифруйте его при помощи пароля или ключа.

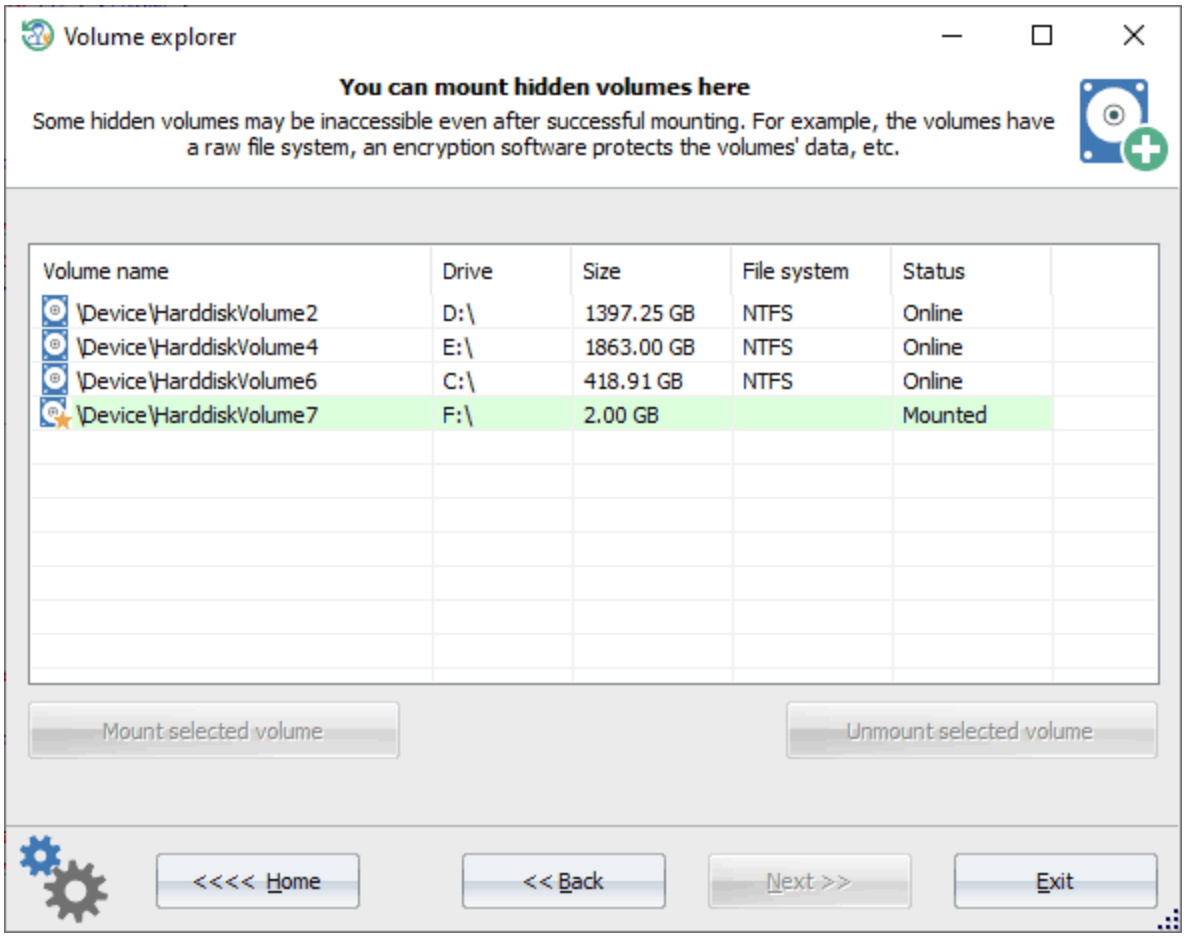
Будьте терпеливы, подключение некоторых форматов может занять несколько минут!

3.8.5 Скрытые тома и разделы

Большинству современных систем Windows для успешного функционирования требуется по крайней мере один скрытый раздел. Такие невидимые для пользователей разделы используются операционной системой во время запуска, восстановления или обновления системы. Некоторые продвинутые пользователи даже могут создавать свои собственные скрытые разделы для предотвращения доступа к личным файлам и персональной информации.



Данный инструмент предназначен для временного монтирования скрытых разделов и использования их в качестве обычных логических дисков.
Чтобы подключить скрытый раздел, выберите его из списка найденных томов и нажмите кнопку '*Смонтировать выбранный том*'.



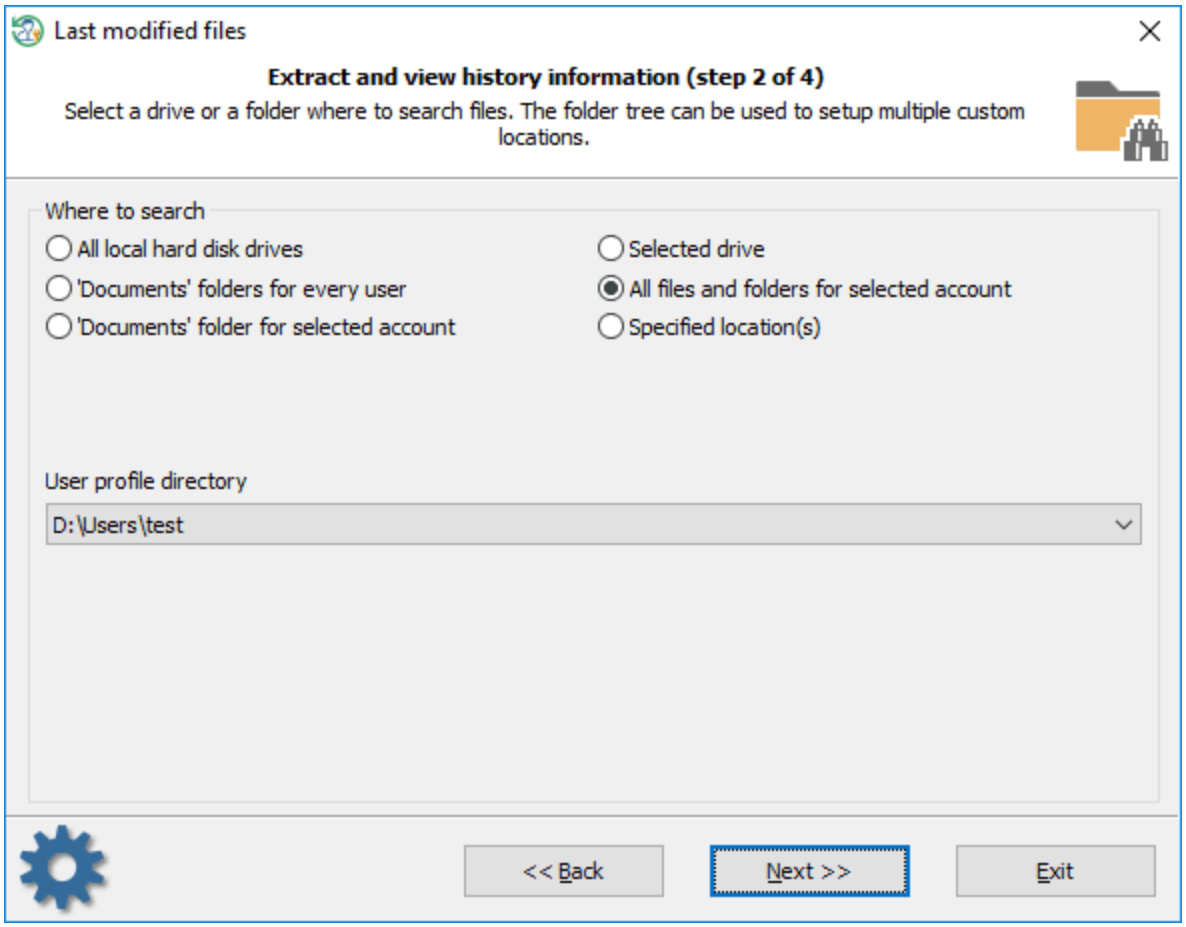
Не забудьте отключить его, если он вам больше не нужен.

Имейте в виду, некоторые разделы могут быть непригодны для использования даже после успешного монтирования. Например, если раздел имеет файловую систему raw, зашифрован при помощи ПО для шифрования дисков (кроме BitLocker) и так далее.

3.8.6 Последние измененные файлы

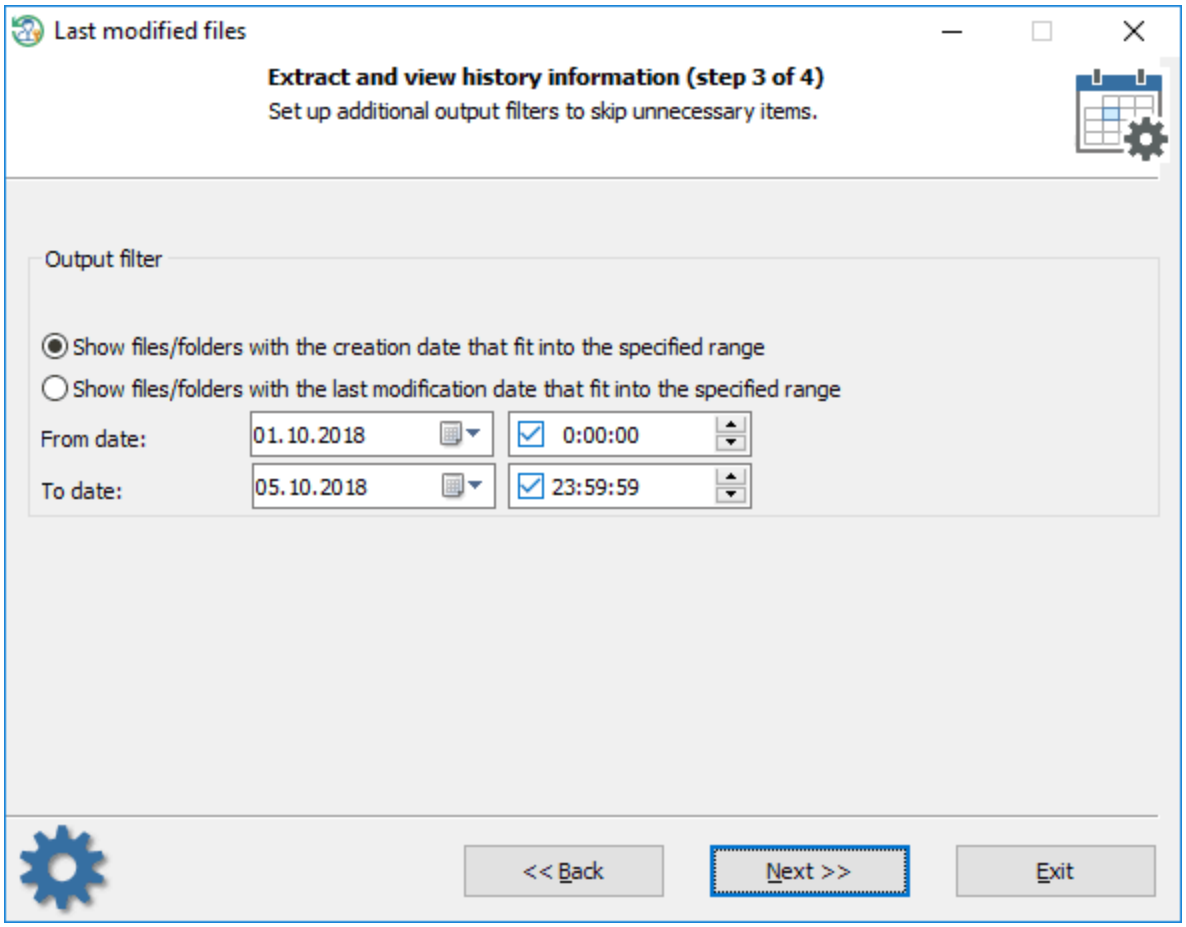
Иногда требуется выяснить, какие файлы или папки были созданы или изменены в определенный промежуток времени. Удивительно, но в Интернете не так много удобных утилит для этого. Мы постарались сделать такой инструмент, при этом максимально упростив его в использовании. Все, что вам нужно, это указать место поиска и временной диапазон для искомых файлов/папок.

Задание начальной точки поиска



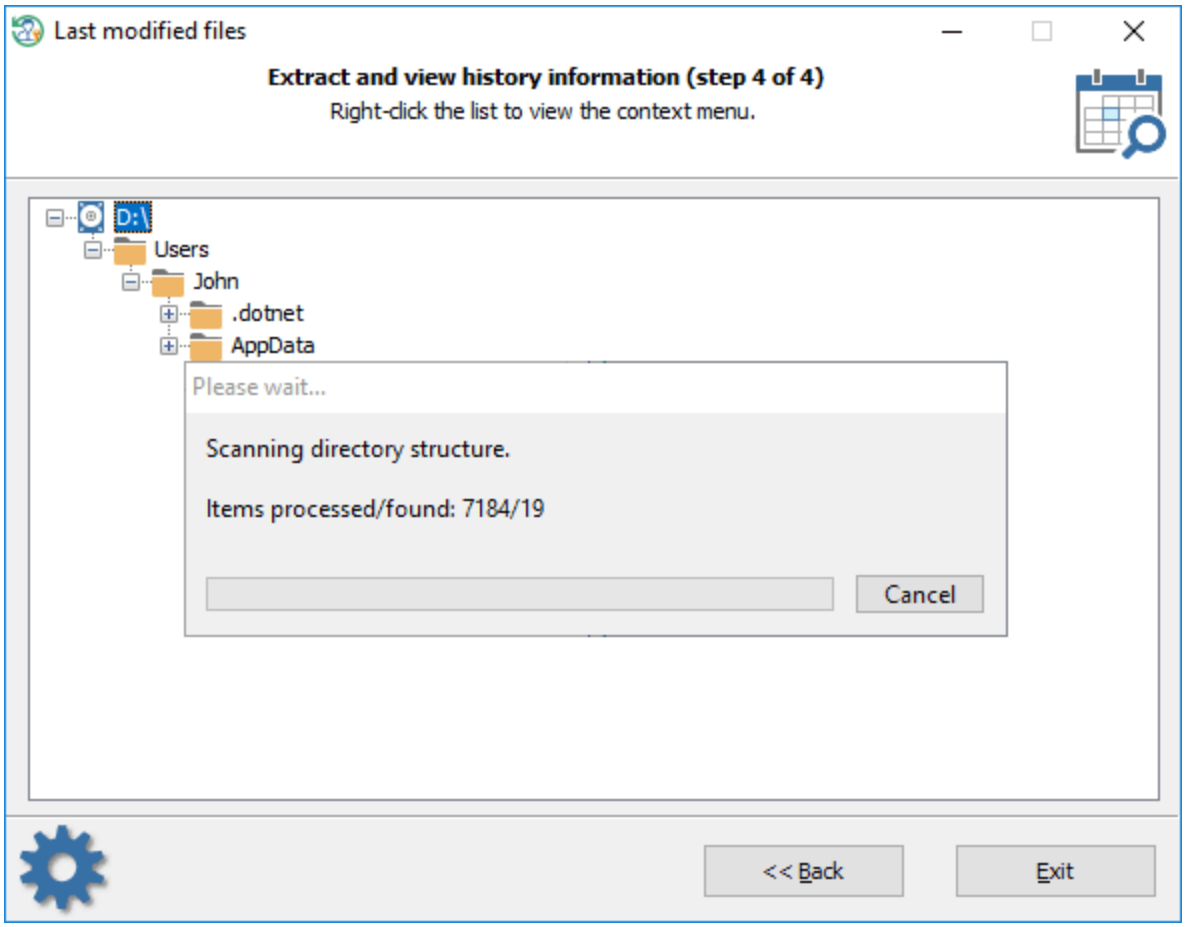
Чтобы задать программе начальную точку для поиска файлов, выберите одно из предопределенных значений. Например, папку документов определенного пользователя, весь его профиль и т.д. Кроме того, можно указать собственный путь или весь жесткий диск.

Временной диапазон для искомых файлов



В этом диалоге выберите, что нужно искать: файлы/папки с определенной датой создания или датой изменения. Можно настроить время вплоть до нескольких секунд или полностью отключить секунды. В последнем случае программа будет производить поиск по дням.

Поиск последних измененных файлов



После того, как все настройки заданы, программа начнет поиск всех файлов, включая вложенные папки и фалы, за указанную дату.
Будьте терпеливы, поиск может занять довольно много времени.

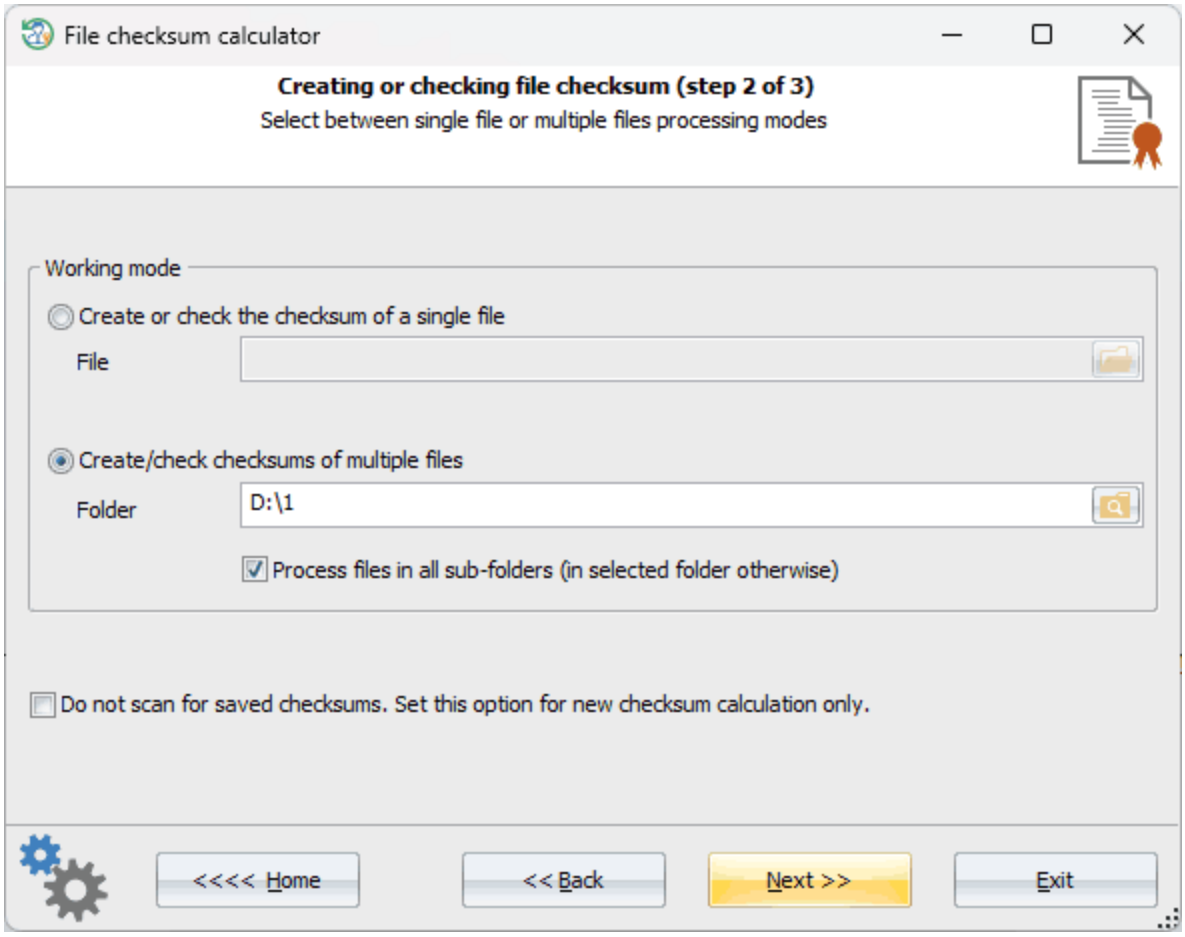
3.8.7 Последние измененные папки

Этот инструмент ведет себя точно так же, как предыдущий, за исключением того, что ищет папки вместо файлов. Пожалуйста, обратитесь к инструменту поиска файлов для получения дополнительной информации.

3.8.8 Калькулятор контрольной суммы или хэша

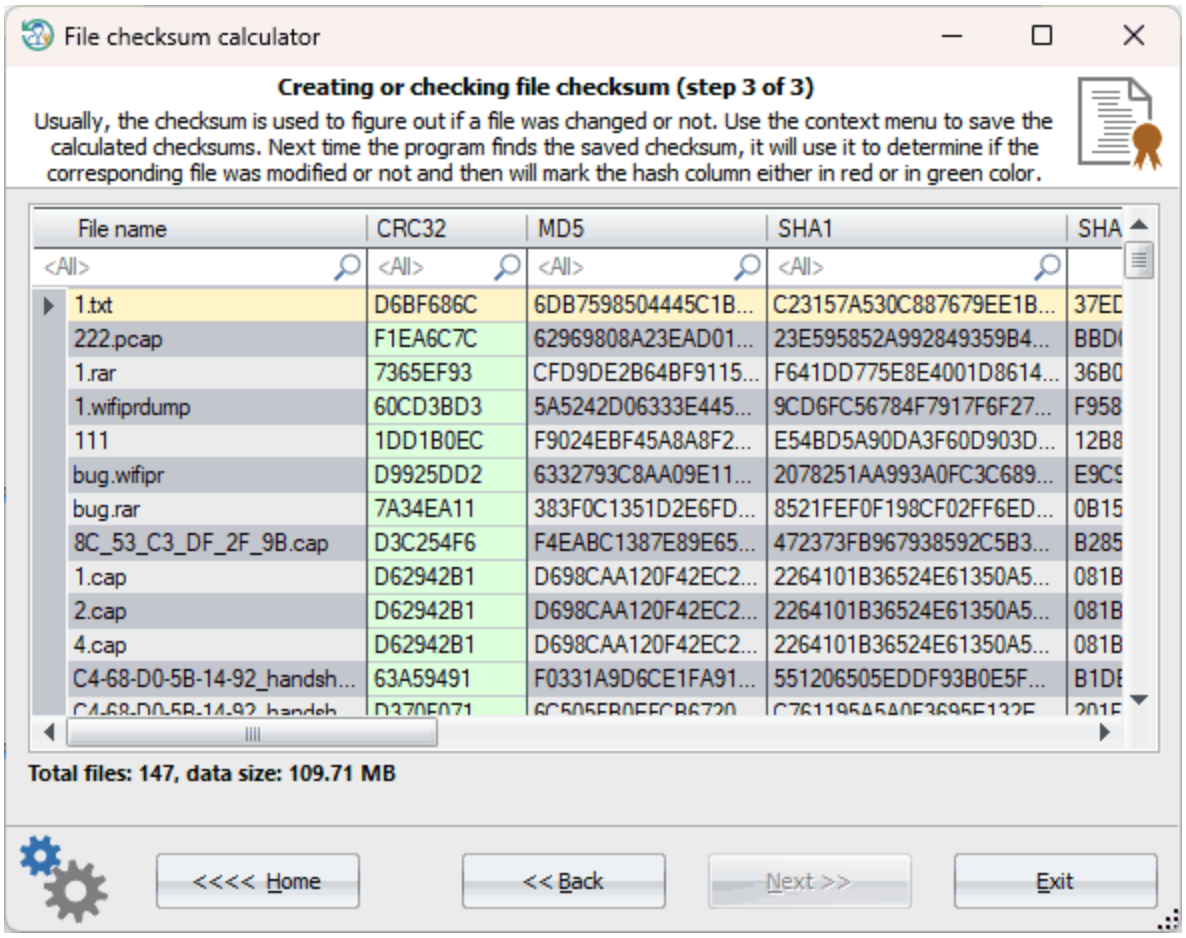
Это инструмент предназначен для обеспечения проверки целостности данных путем создания контрольных сумм и хэширования файлов. Утилита использует различные алгоритмы хеширования, такие как CRC32, MD5, SHA1, SHA-256 и SHA-512. Она может работать в пакетном режиме, одновременно вычисляя и проверяя контрольные суммы нескольких файлов из любого заданного каталога.

Выбор файла или каталога



Программа может работать в двух режимах, обрабатывая либо один, либо несколько файлов одновременно. Выберите тот, который вам более подходит. При использовании режима работы с несколькими файлами будьте осторожны. Несмотря на то, что вычисление контрольных сумм тысяч файлов не займет много времени, вывод результата работы может привести к ступору на некоторое время.
По умолчанию программа и вычисляет, и проверяет контрольные суммы одновременно. Вы можете отключить проверку контрольных сумм, установив соответствующую опцию.

Вывод результатов создания/проверки хэшей



Алгоритм проверки контрольных сумм довольно прост. Как только программа обнаружит файл с соответствующим расширением (*.crc, *.md5, *.sha, *.sha256 или *.sha512), она будет использовать его для сравнения с вычисленным хэшем.

Например, когда программа находит файл с именем readme.txt, она сначала вычисляет CRC32, MD5, SHA1, SHA256 или SHA512 хэш этого файла. Затем сканирует текущий каталог на наличие readme.txt.crc, readme.txt.md5... readme.txt.sha512 файлов и, если таковой найден, считывает хэш из этого файла и сравнивает его с вычисленным хэшем. Если хэши совпадают, инструмент помечает соответствующий столбец таблицы зеленым, в противном случае - красным цветом (что означает, что файл был изменен с момента сохранения хэша).

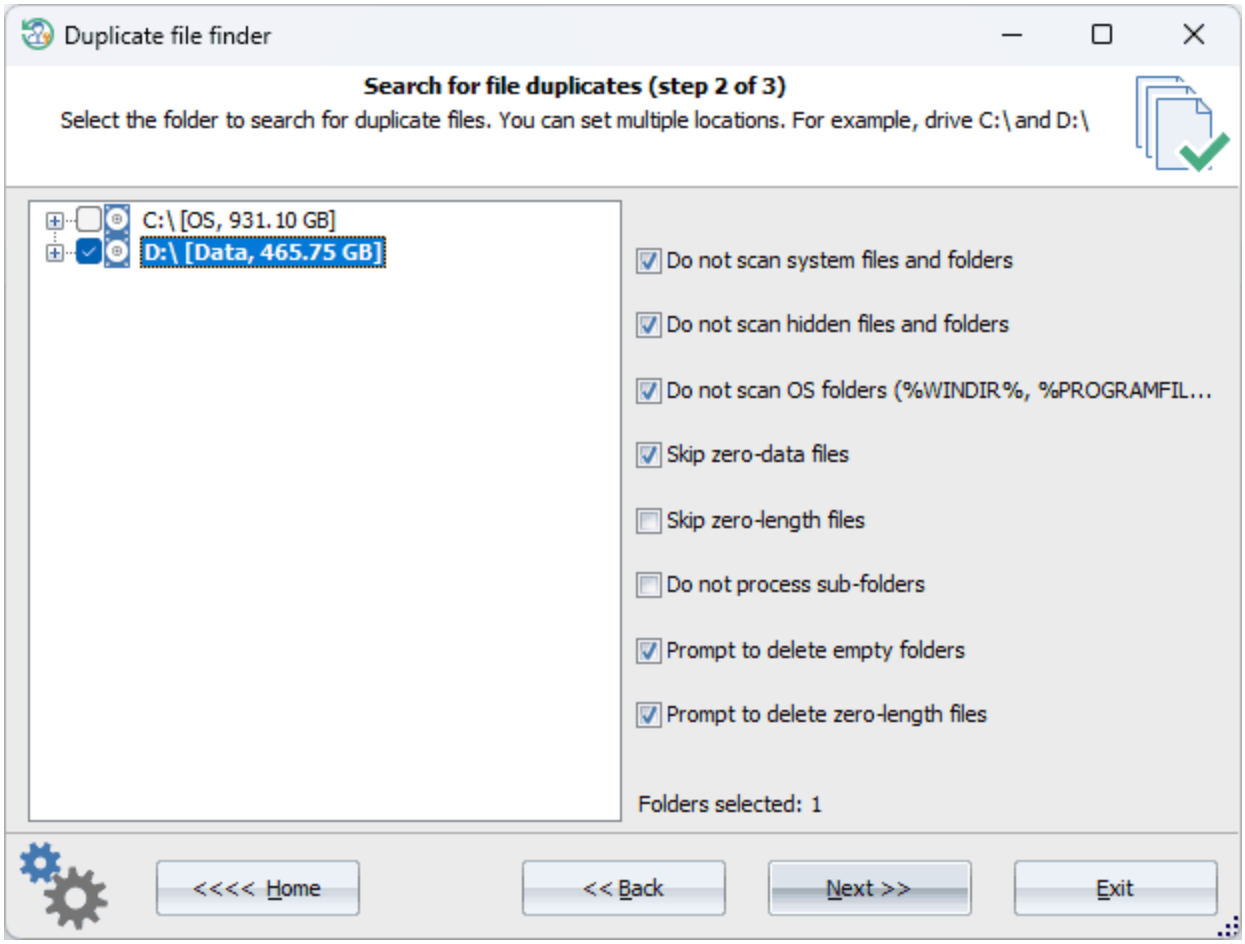
Чтобы сохранить вычисленный хэш(ы), щелкните правой кнопкой мыши таблицу, откройте контекстное меню и выберите *'Сохранить'*.

3.8.9 Поиск дубликатов файлов

Если у вас есть тысячи музыкальных файлов, документов, фотографий или видео и вам не хватает места на диске, этот инструмент именно для вас. Он поможет найти и удалить ненужные дубликаты файлов, а также пустые файлы и папки буквально за пару щелчков мыши. Мы постарались сделать этот инструмент

максимально быстрым и оптимизировали скорость алгоритма поиска дубликатов для работы с современными твердотельными накопителями и многоядерными процессорами.

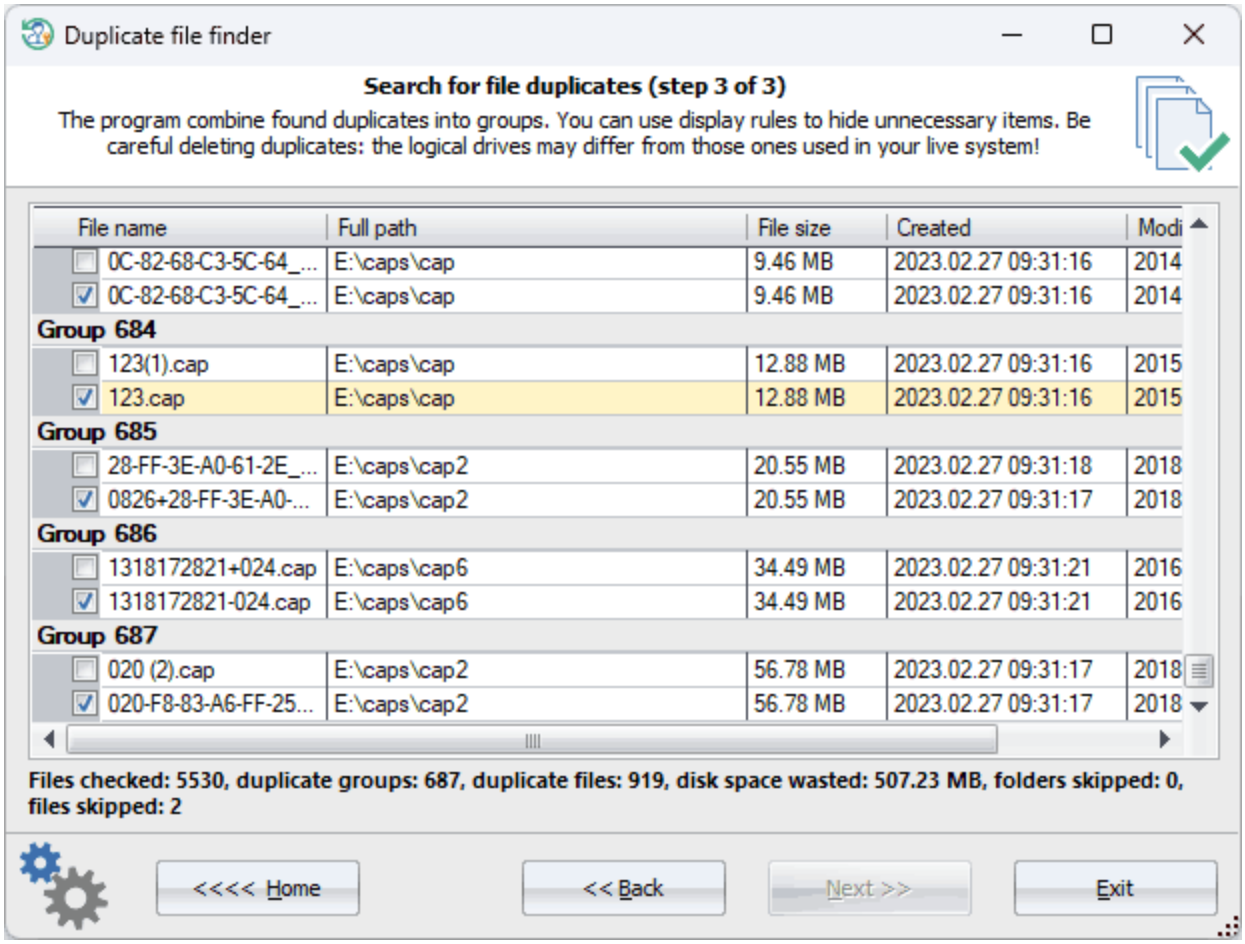
Выбор каталога(ов) для поиска файловых дубликатов



Выберите исходный диск, папку или несколько папок, где будет происходить поиск дубликатов. Программа предлагает небольшой набор дополнительных опций:

- **Do not scan system files or folders.** Не сканировать (пропускать) файлы и папки, у которых установлен атрибут SYSTEM.
- **Do not scan hidden files or folders.** Не сканировать (пропускать) файлы и папки, у которых установлен атрибут HIDDEN.
- **Do not scan OS folders.** Не сканировать системные папки Windows, такие как %WINDIR%, %PROGRAMFILES%, %PROGRAMDATA% и т.д.
- **Skip empty-data files.** Пропустите файлы заполненные одними нулями.
- **Skip zero-length files.** Не обрабатывайте файлы с нулевой длиной.
- **Do not process sub-folders.** Сканируйте только текущий каталог, не лезть во вложенные папки.
- **Prompt to delete empty folders.** Запрос на удаление пустых каталогов. Используйте с осторожностью. Windows использует некоторые пустые каталоги.
- **Prompt to delete zero-length files.** Запрос на удаление файлов с нулевой длиной.

Работа с найденными дубликатами



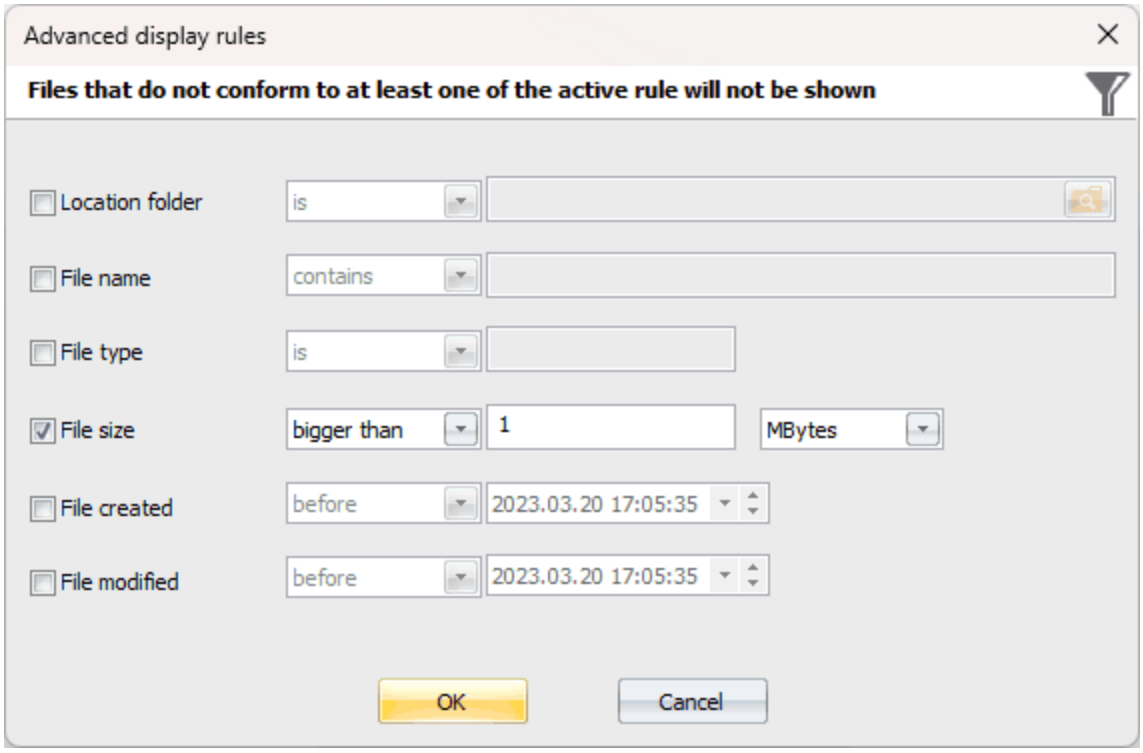
Как только процесс сканирования завершится, программа сначала попросит удалить все найденные пустые файлы и папки (если установлены соответствующие параметры). Будьте осторожны, некоторые пустые элементы могут использоваться операционной системой. Этот параметр часто используется для очистки структуры каталогов.

Например, как в Windows 10, так и в Windows 11 есть ошибка, из-за которой создаются тысячи пустых папок в каталоге
C:\Windows\System32\config\systemprofile\AppData\Local
Все пустые папки выглядят так: **tw-XXXXXXXXXXXXXXXX.tmp**, где **X** - шестнадцатеричное значение.
Вы можете использовать программу для удаления этих пустых вложенных папок из исходного каталога. Но сначала убедитесь, что были установлены по крайней мере два параметра:

- Не обрабатывать вложенные папки. Этот параметр гарантирует, что программа не будет обрабатывать пустые папки глубже вложенной папки первого уровня.
- Запрос на удаление пустых папок

RWP объединяет все найденные дубликаты файлов в группы. Группа состоит по крайней мере из двух идентичных файлов. По умолчанию программа автоматически выбирает для удаление все элементы после первого в каждой группе. Вы можете выбирать или отменять выбор любых необходимых элементов или

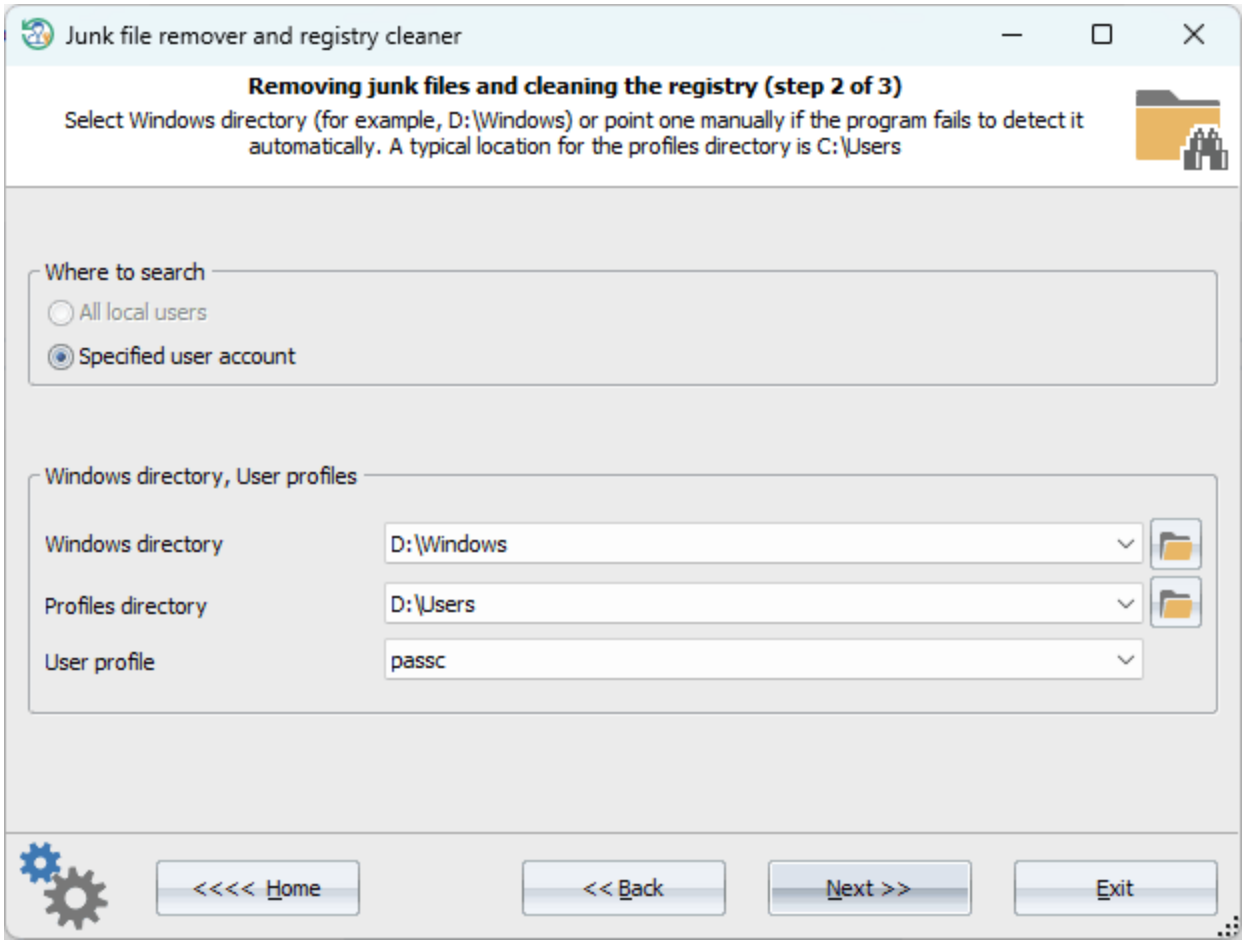
настраивать свои собственные правила отображения. Например, чтобы скрыть все файлы размером менее 1 МБ, используйте правило отображения, как показано ниже.



3.8.10 Удаление ненужных файлов и очистка реестра

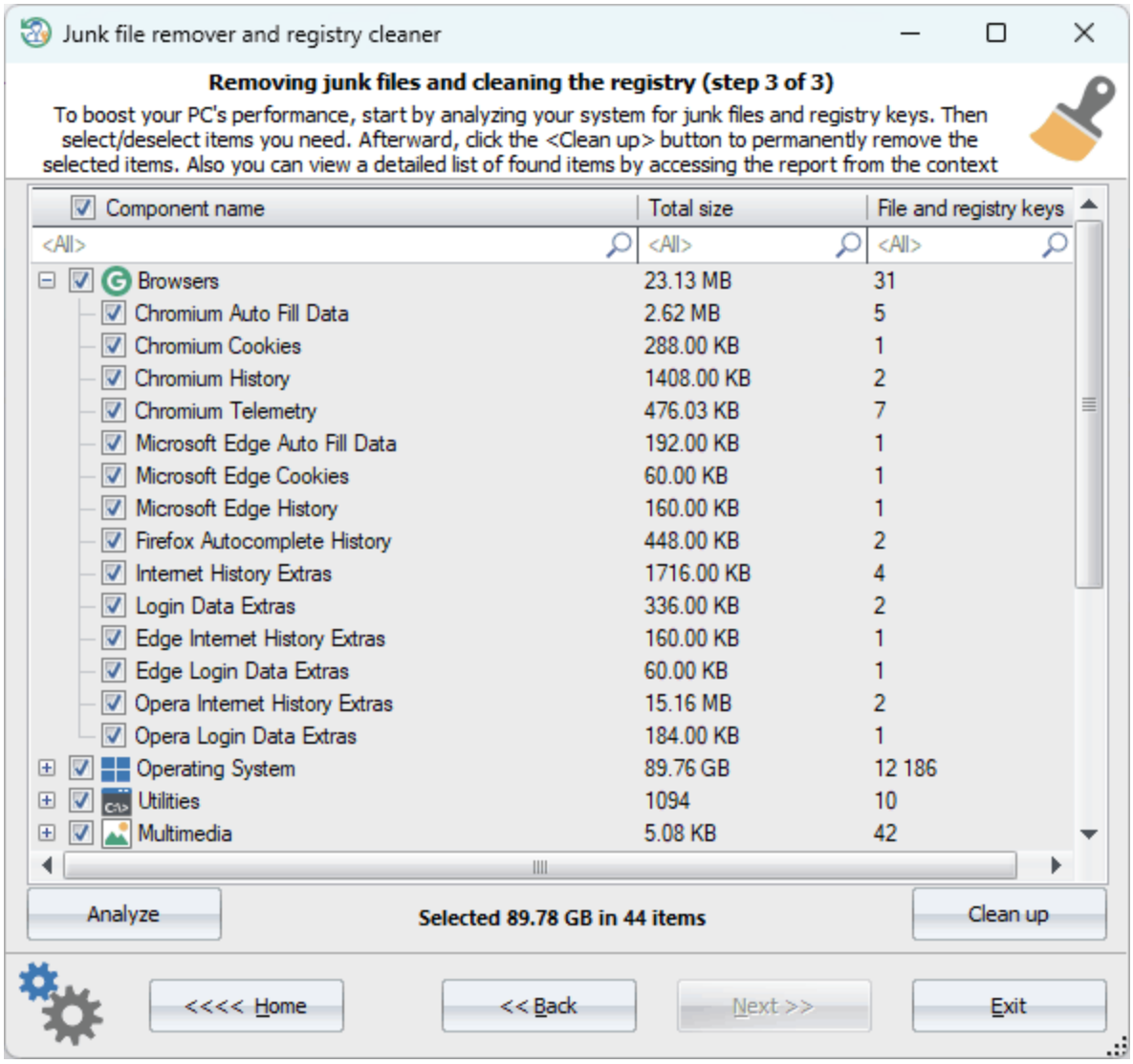
Эта функция программы позволяет избавиться от ненужных файлов и записей реестра вашего компьютера и устраняет проблемы производительности всей системы. Программа выполняет всестороннюю очистку диска, производя поиск мусорных файлов, которые накапливаются со временем. Сюда входят временные файлы, системные и браузерные кэши, старые загрузки, ненужные резервные копии и многое другое. Удаление этого цифрового мусора освобождает пространство на диске, что приводит к более быстрому запуску программ, увеличивая скорость загрузки Интернет страниц, улучшая отзывчивость и производительность системы.

Выбор системных каталогов и профиля пользователя



Благодаря простому и интуитивно понятному интерфейсу, программа обеспечивает оптимизацию без особых сложнойстей и сложных настроек, что подходит даже для тех, кто совсем не разбирается в компьютерах. Чтобы начать, выберите каталог Windows и целевого пользователя, профиль которого вы хотите отсканировать.

Удаление ненужных файлов и очистка реестра



В финальном диалоговом окне щелкните кнопку *'Анализ'*. Это запустит процесс сканирования, который заполнит таблицу списком найденных и потенциально ненужных файлов и ключей реестра. Вы можете выбрать или снять выбор с определенных элементов в таблице, прежде чем перейти к очистке. Чтобы окончательно удалить отмеченные элементы, нажмите кнопку *'Очистить'*.

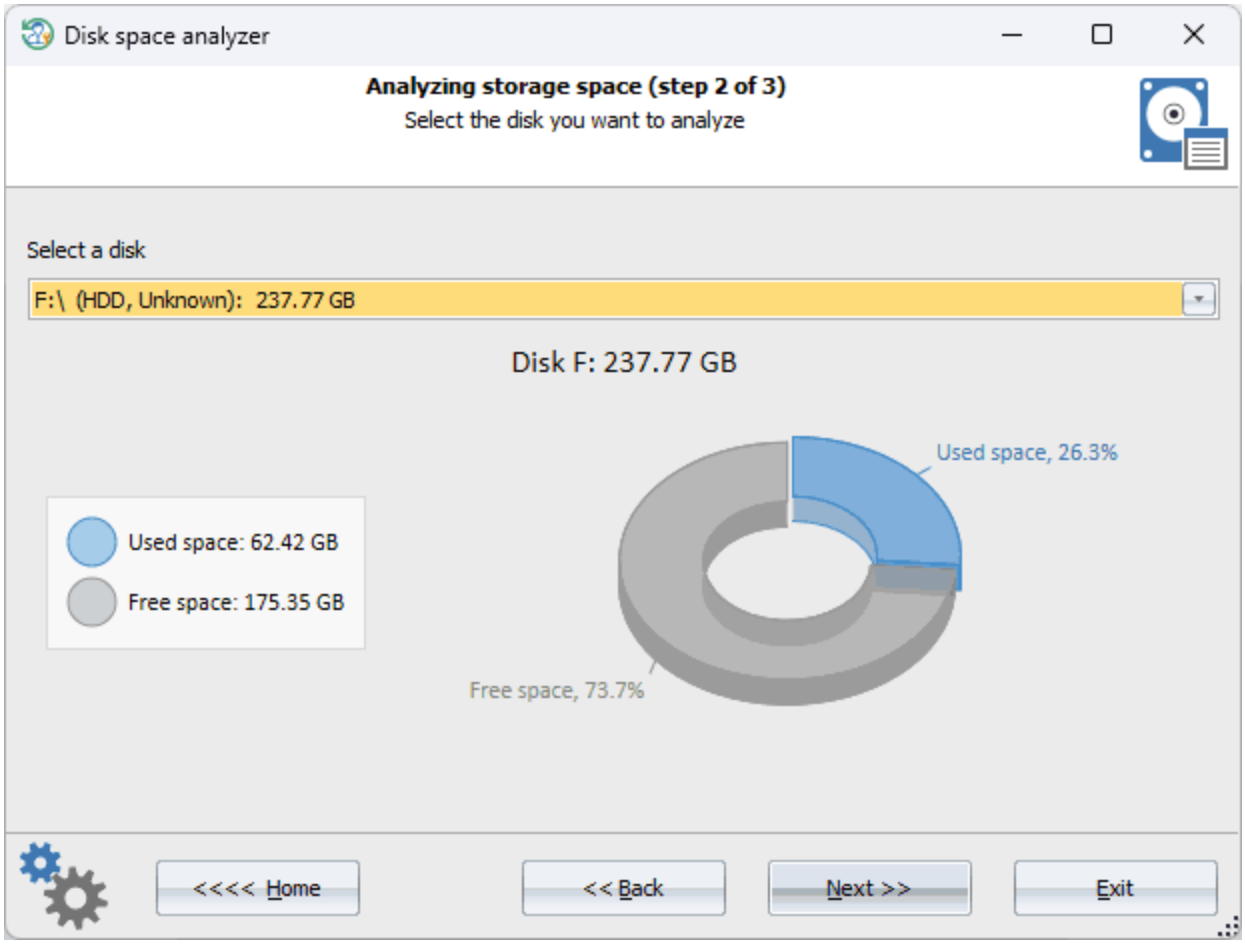
Перед очисткой системы рекомендуется создать резервную копию реестра и важных файлов, чтобы обеспечить возможность возврата. Эта предосторожность поможет защитить ваши данные на случай возникновения непредвиденных проблем.

3.8.11 Анализатор дискового пространства

Анализ свободного места на вашем компьютере может быть сложной задачей, но благодаря новой функции программы, это стало просто и невероятно быстро. Вам нужно лишь выбрать диск, и программа автоматически отсортирует все файлы и папки на нем в зависимости от занимаемого места, практически мгновенно. Фактически, это один из самых быстрых инструментов для анализа свободного места. После

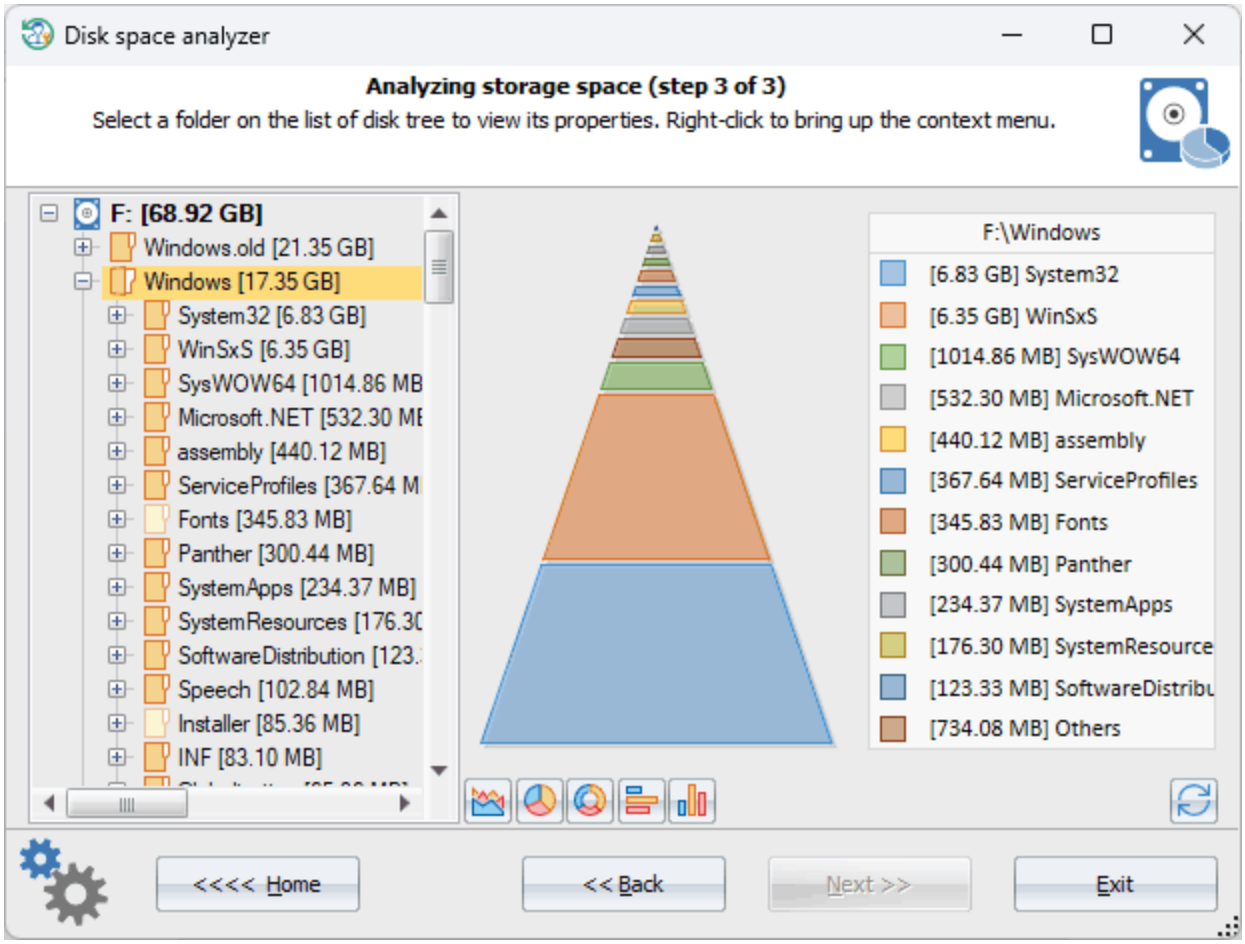
завершения анализа вы сможете создать и просмотреть отчёт о состоянии диска или удалить ненужные элементы, чтобы освободить дополнительное место.

Выбор логического диска



Выберите логический диск, который необходимо проанализировать. При первом доступе программы к диску происходит анализ его структуры и сохранение этой информации в файле кэша. Обычно этот процесс занимает менее минуты, но может сильно зависеть от количества файлов на диске и его скорости. После этого каждый последующий анализ диска происходит почти мгновенно.

Анализ свободного места



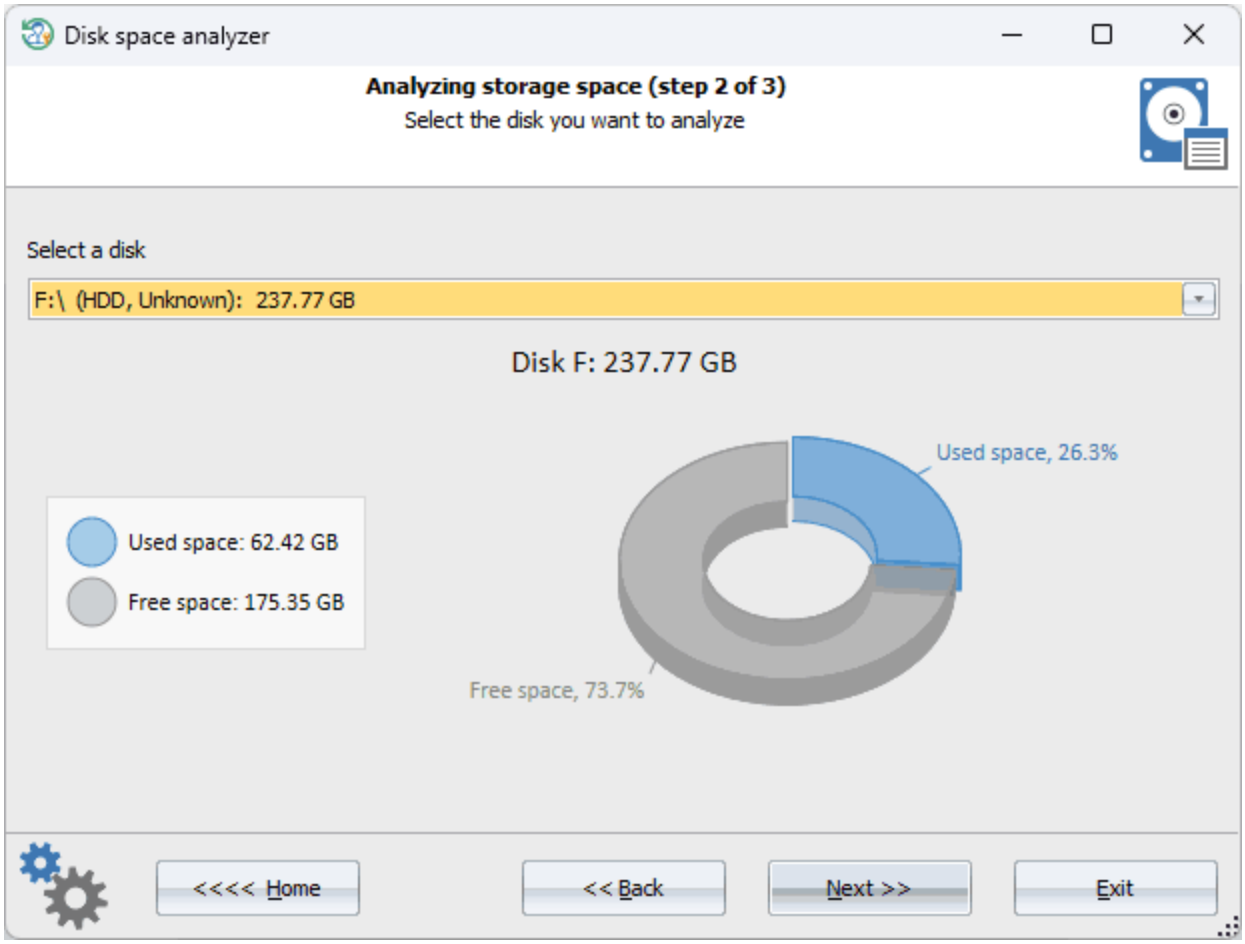
Программа автоматически организует файлы и папки в зависимости от их размера таким образом, что те, которые занимают наибольшее место на диске, отображаются в списке в первую очередь. Поэтому, можно быстро определить, какие файлы или папки занимают большую часть ценного дискового пространства. Пользователи могут использовать контекстное меню для открытия местоположения папки или файла, освобождения места путем удаления выбранных элементов или создания отчета о диске.

3.8.12 Анализ диска

Этот инструмент анализа файлов и папок позволяет вам:

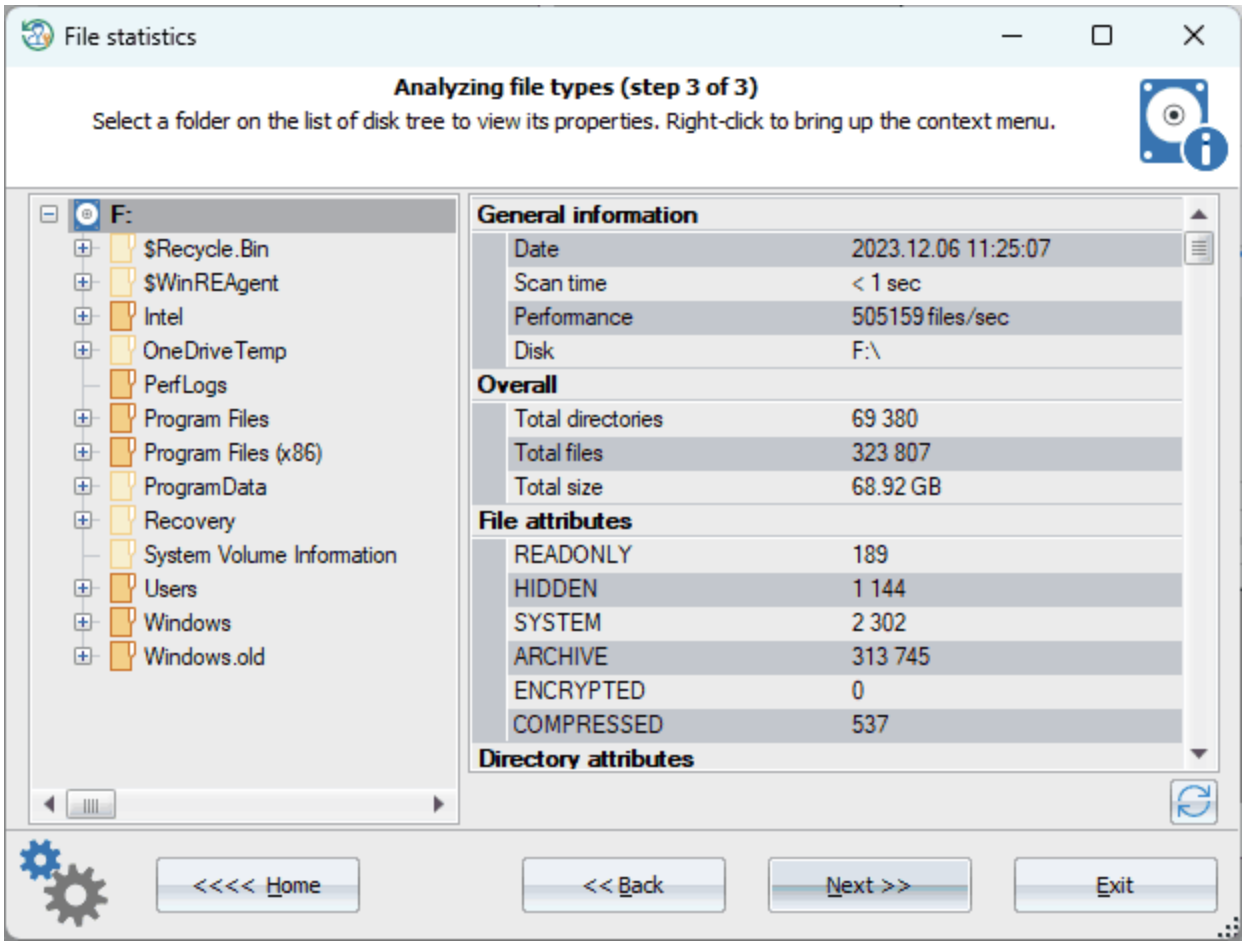
- Получить глубокое понимание структуры и содержания ваших жестких дисков
- Мгновенно сканировать отдельные папки или весь диск целиком
- Анализировать файлы по типу или размеру
- Мгновенно определять файлы определенных форматов, таких как изображения, видео или документы
- Производить поиск файлов или каталогов, занимающих самое большое место на диске
- Генерировать подробные отчеты, описывающие типы файлов, их размеры, атрибуты, даты модификации/создания и прочее.

Выбор логического диска



Выберите логический диск, который вам нужно проанализировать. При первом доступе программа сохраняет структуру файлов и папок в кэш-файл. Этот процесс обычно занимает менее минуты, хотя продолжительность может варьироваться в зависимости от объема элементов на диске и скорости самого диска. После этого каждый последующий доступ к закэшированному диску происходит почти мгновенно!

Анализ диска

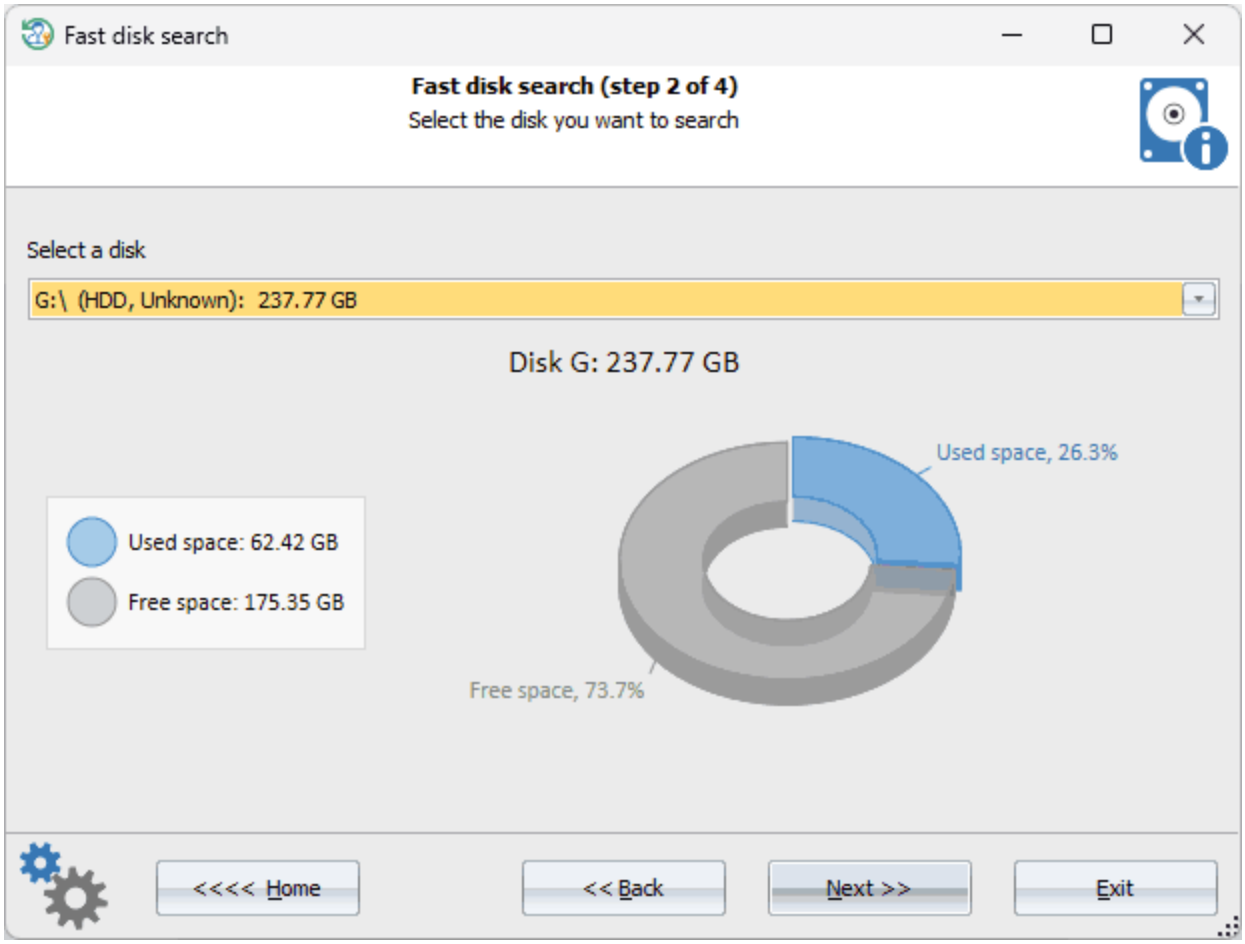


У вас есть возможность просматривать статистику как для всего диска, так и для отдельных папок. Просто выберите выделите соответствующий каталог. Чтобы создать отчёт в формате HTML, воспользуйтесь контекстным меню.

3.8.13 Быстрый поиск на диске

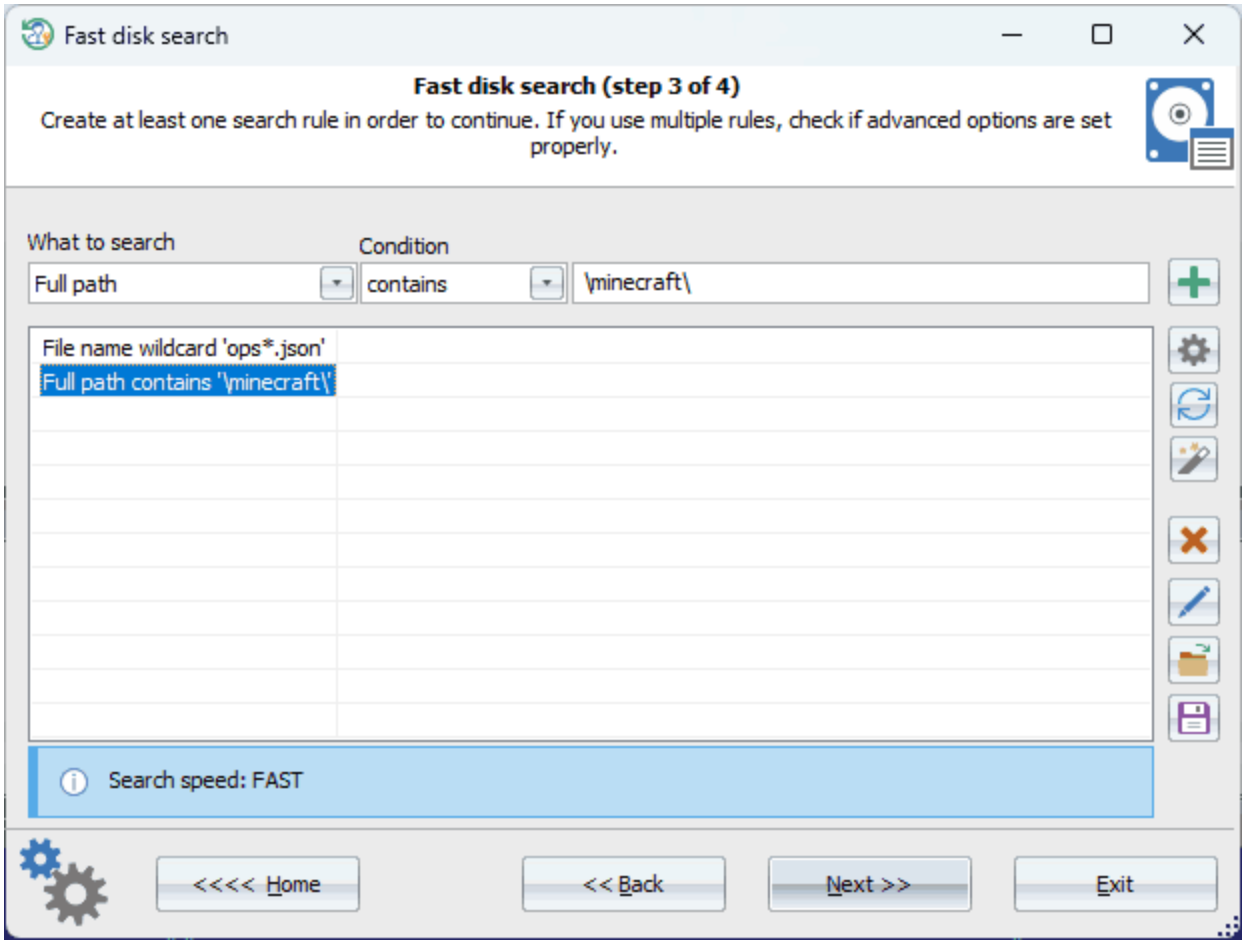
Этот инструмент предназначен для быстрого поиска файлов и их содержимого на выбранном диске. Наш поиск является самым быстрым среди аналогичных программ Windows. Например, поиск по имени файла на обычном диске (приблизительно около 1 миллиона файлов) происходит почти мгновенно и занимает около 1 секунды. Кроме того, программа имеет расширенные правила поиска, которые могут удовлетворить даже искушенного пользователя.

Выбор диска



Выберите диск, на котором необходимо выполнить поиск.

Настройка правил и параметров поиска



Программа предоставляет широкий спектр правил, которые можно комбинировать между собой. Кнопка с настройками задает порядок комбинирования правил:

- Если выбрать 'Совпадение всех правил', то поиск считается успешным, если искомый файл или папка удовлетворит всем заданных правилам
- Если выбрать Совпадение хотя бы одного правила', то поиск считается успешным, если искомый файл или папка подойдет хотя бы под одно заданное правило

Правила можно добавлять, удалять, редактировать, а также сохранять на диск или читать с него. Имеется также возможность применения готовых наборов правил для поиска секретных клоючей, паролей, дампов и др.

Каждое правило состоит из трех элементов: объект поиска, операция для объекта поиска и собственно условие. Например, на скриншоте выше задано:
Объект поиска - **полный путь**
Операция - **должен содержать**
Условие - **\minecraft**

Объекты поиска
Имя файла - имя файла с расширением. Например, readme.txt
Расширение файла - расширение (без точки). Например, EXE
Размер файла - размер
Тип файла - тип файла. Например, *Code* - файлы с исходным кодом.
Атрибуты файла - например, архивный, системный, только для чтения и т.д.
Дата создания файла - дата создания без указания времени

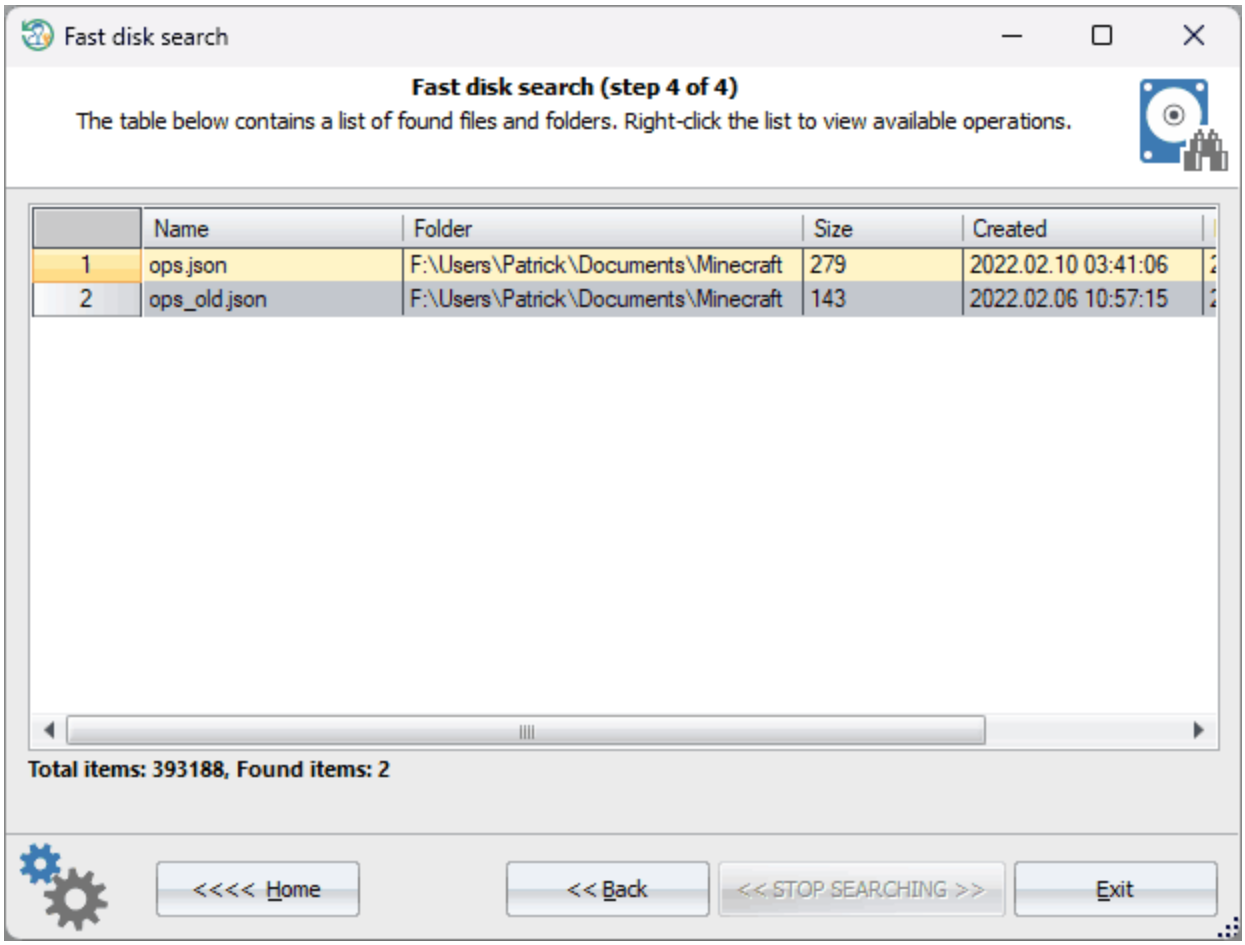
Дата модификации файла - дата изменения без указания времени
Время создания файла - полная дата создания с временем
Время модификации файла - полная дата последнего изменения с временем
Текстовая строка в содержимом - строка в файле. Программа выполняет трехпроходный поиск, автоматически определяя ANSI, UTF8 и UTF16 строки.
Бинарные данные в содержимом - бинарные данные в файле
Имя папки - имя папки с расширением, если есть. Например, windows.old
Расширение папки - расширение папки
Размер папки - размер всех файлов в папке (включая все вложенные папки)
Атрибуты папки - аналогично файловым атрибутам
Дата создания папки - аналогично файлам
Дата модификации папки - аналогично файлам
Время создания папки - аналогично файлам
Время модификации папки - аналогично файлам
Полный путь - полный путь папки или файла

Операции
Доступные операции зависят от объектов поиска. Например, если выбрать имя файла/папки или расширение, то будут доступны следующие операции:

- **Содержит в себе**
- **Не содержит**
- **Полностью соответствует**
- **Не соответствует**
- **Начинается с**
- **Заканчивается на**
- **Файловая маска**
- **Регулярное выражение**

Будьте аккуратны, задание регулярных выражений, а также поиск текстовых строк может сильно замедлить поиск.

Результаты поиска



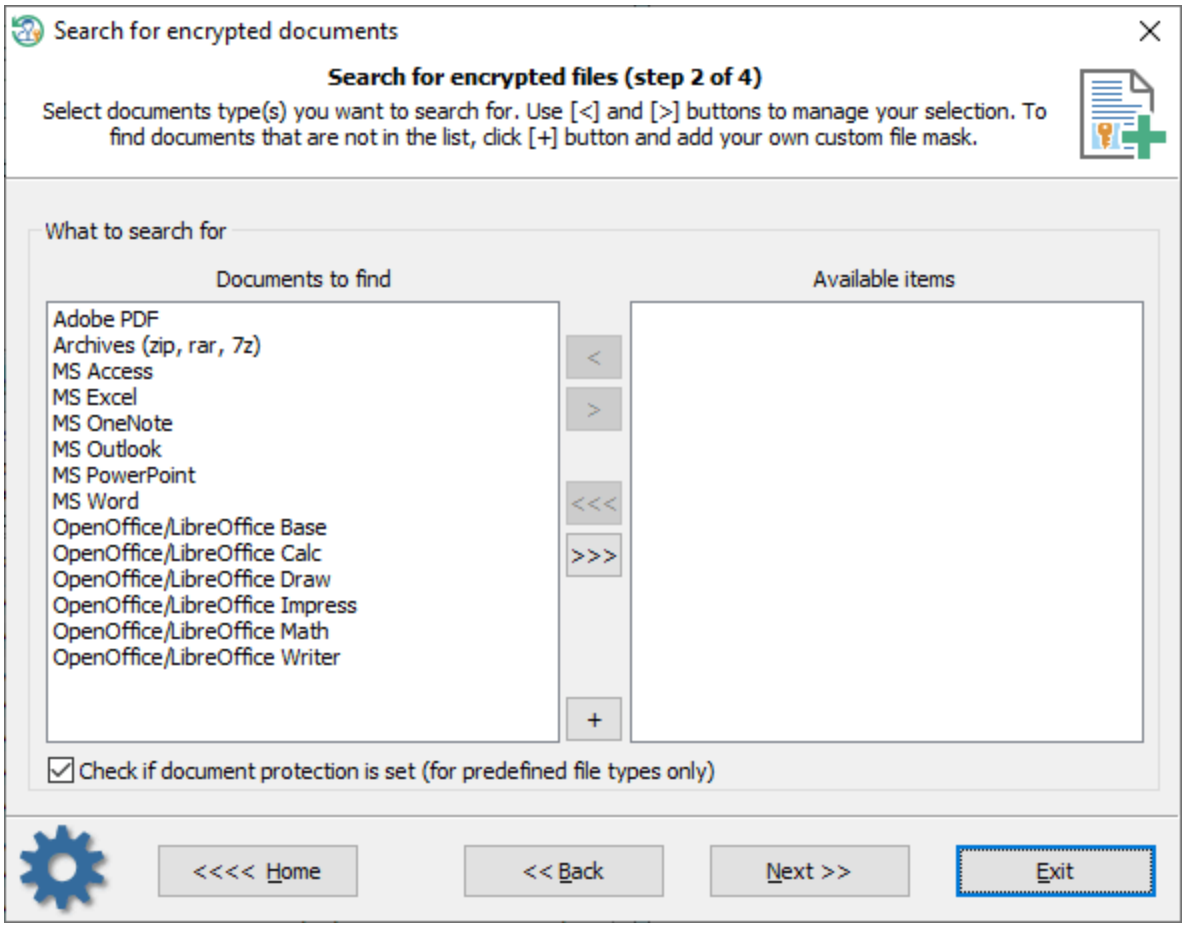
Результаты поиска можно скопировать в буфер обмена, создать HTML отчет или сохранить в ZIP архив.

3.9 Утилиты

3.9.1 Поиск документов с защитой

Эта функция программы предназначена для поиска на компьютере зашифрованных документов, защищенных паролем архивов и файлов. Утилита проста в использовании, быстра в работе и гибка в настройке. Можно задавать для поиска свои типы файлов.
Процесс настройки разделен на три части:

1 Выбор типа документа



По умолчанию программа производит поиск следующие типы документов:

- Файловые архивы (zip, rar, 7z)
- Документы Adobe PDF
- Документы MS Word
- Таблицы MS Excel
- Базы данных MS Access
- Презентации MS PowerPoint
- Заметки MS OneNote
- Файлы данных MS Outlook
- Документы OpenOffice/LibreOffice Writer
- Таблицы OpenOffice/LibreOffice Calc
- Базы данных OpenOffice/LibreOffice Base
- Презентации OpenOffice/LibreOffice Impress
- Документы OpenOffice/LibreOffice Draw
- Документы OpenOffice/LibreOffice Math

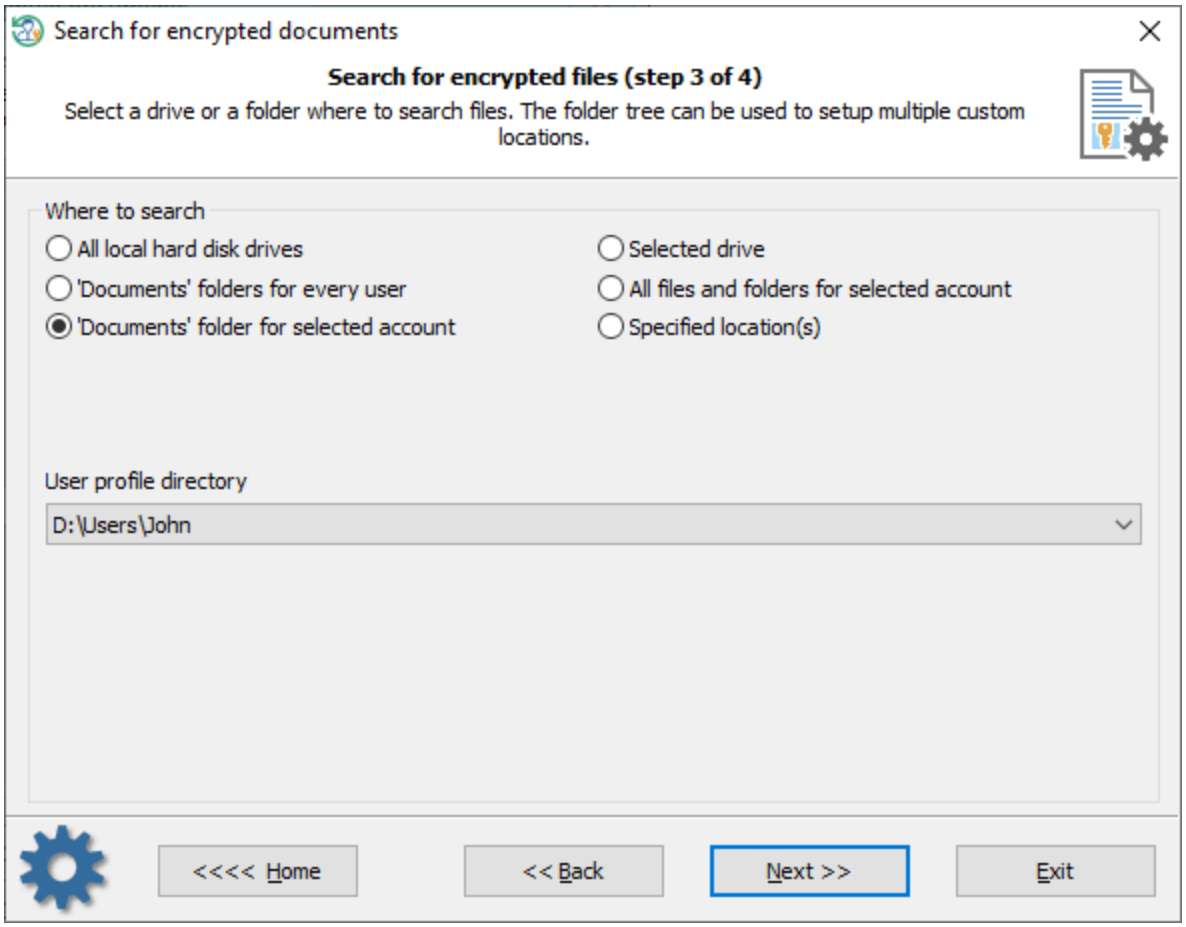
Кнопки [>] и [<] предназначены для включения в поиск или исключения из поиска определенных типов документов. Для добавления своего типа документа (кнопка [+]) укажите его описание и маску, по которой его следует искать. Например, при помощи вот этой маски можно добавить в поиск файлы данных KeePass:

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

Учтите, поиск и анализ защиты в файлах, заданных пользователем, не производится.

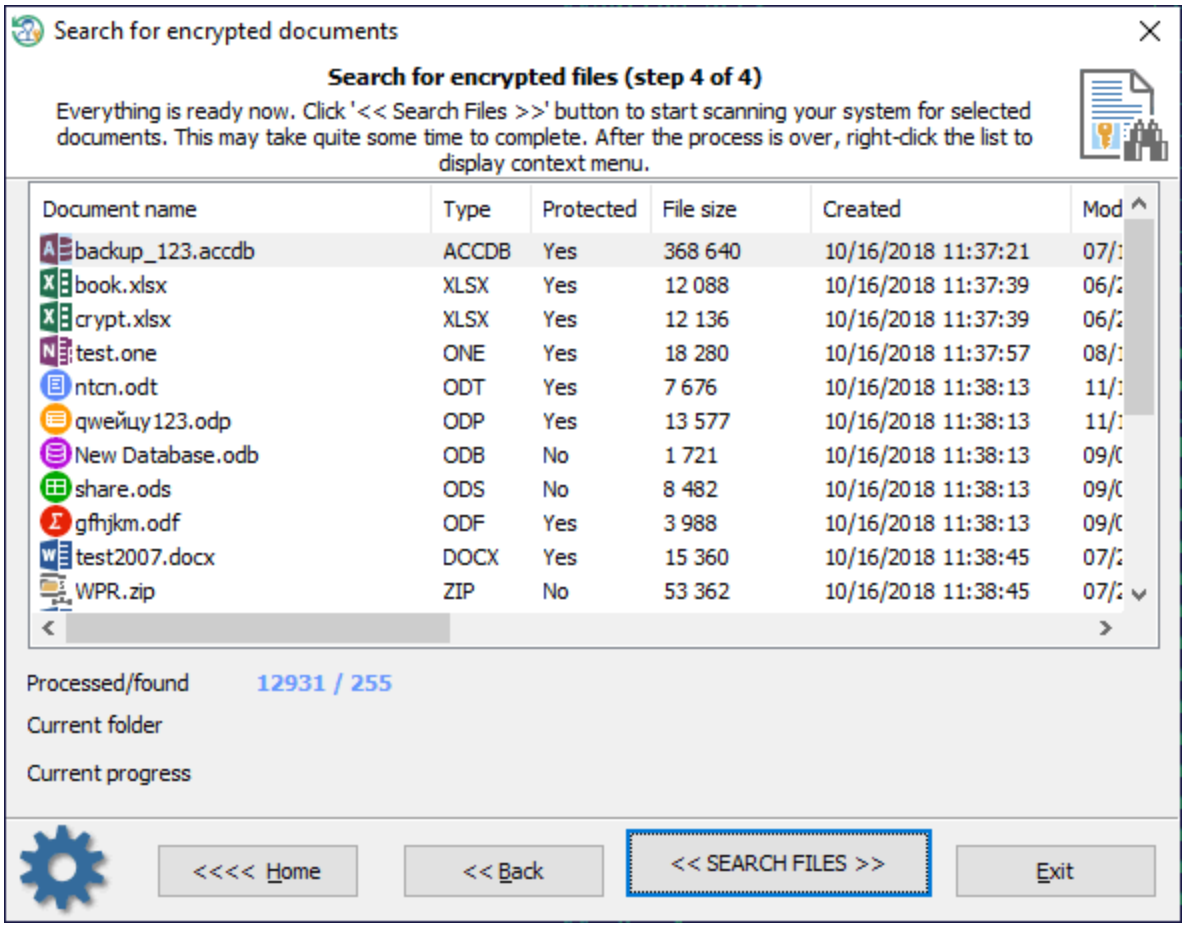
Опция "Проверять наличие пароля в искомых документах..." предназначена для отключения проверки защиты в найденных документах, что позволяет в определенных случаях существенно ускорить процесс поиска.

2 Выбор места сканирования



Для ускорения поиска можно сузить диапазон сканирования задав, к примеру, каталог "Мои Документы" определенной учетной записи или указав свой каталог.

3 Поиск выбранных документов



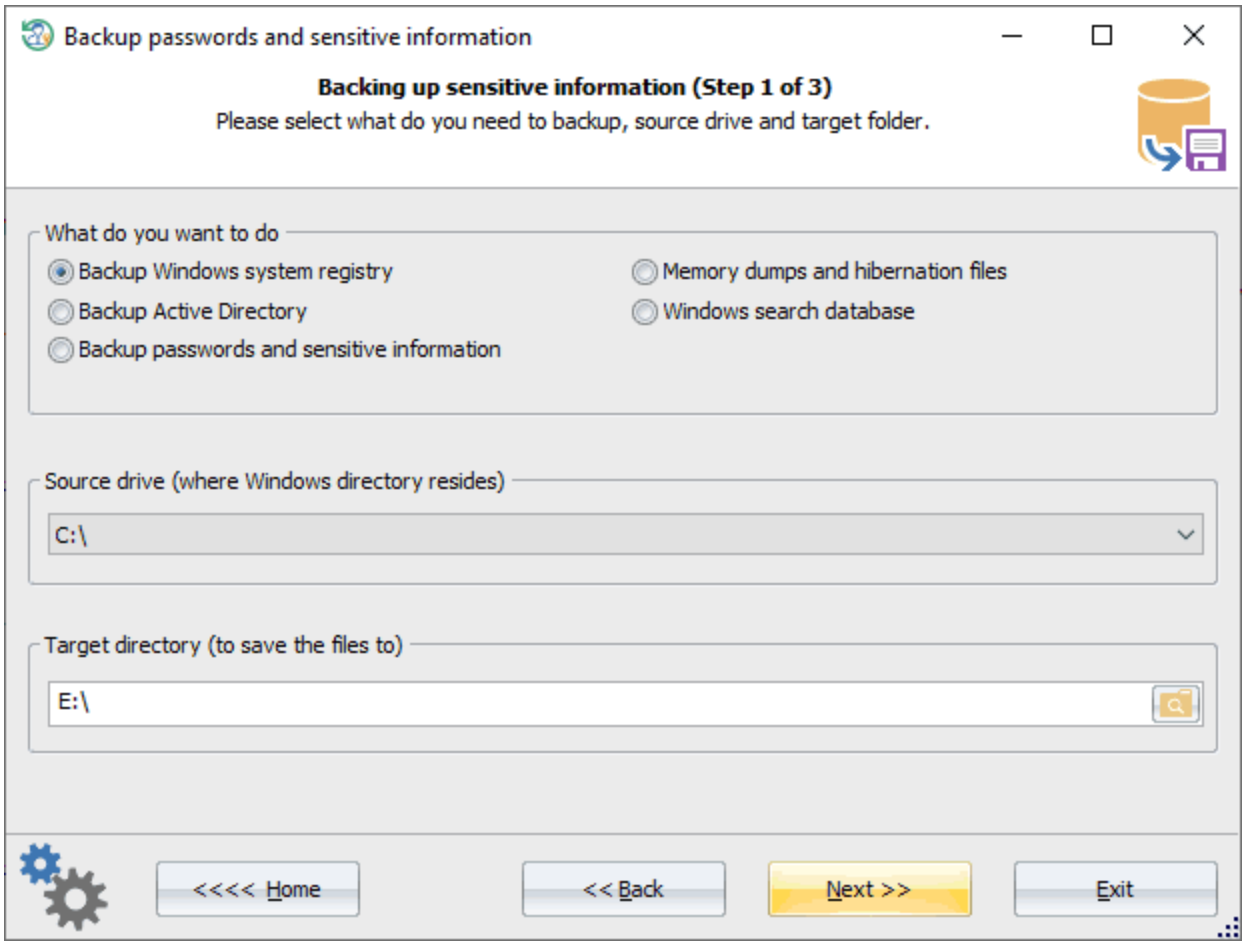
Несмотря на то, что программа оптимизирована для быстрого поиска, сканирование жестких дисков с большим количеством файлом может занять много времени.

После завершения поиска, щелкните правой кнопкой мыши на списке найденных документов для показа меню доступных операций. Например, можно сохранить список найденных файлов в текстовый/HTML файл или создать архив, который будет включать в себя указанные записи.

3.9.2 Создание резервной копии паролей и конфиденциальной информации

Иногда жизненно важно сохранить реестр Windows или базу данных Active Directory. Reset Windows Password может быть палочкой-выручалочкой для тех, кому необходимо легко и быстро сделать резервное копирование этих файлов. Кроме того, программа буквально за пару кликов мышкой может сделать копию всей персональной информации и паролей на целевом ПК.

Выбор источника файлов для резервной копии

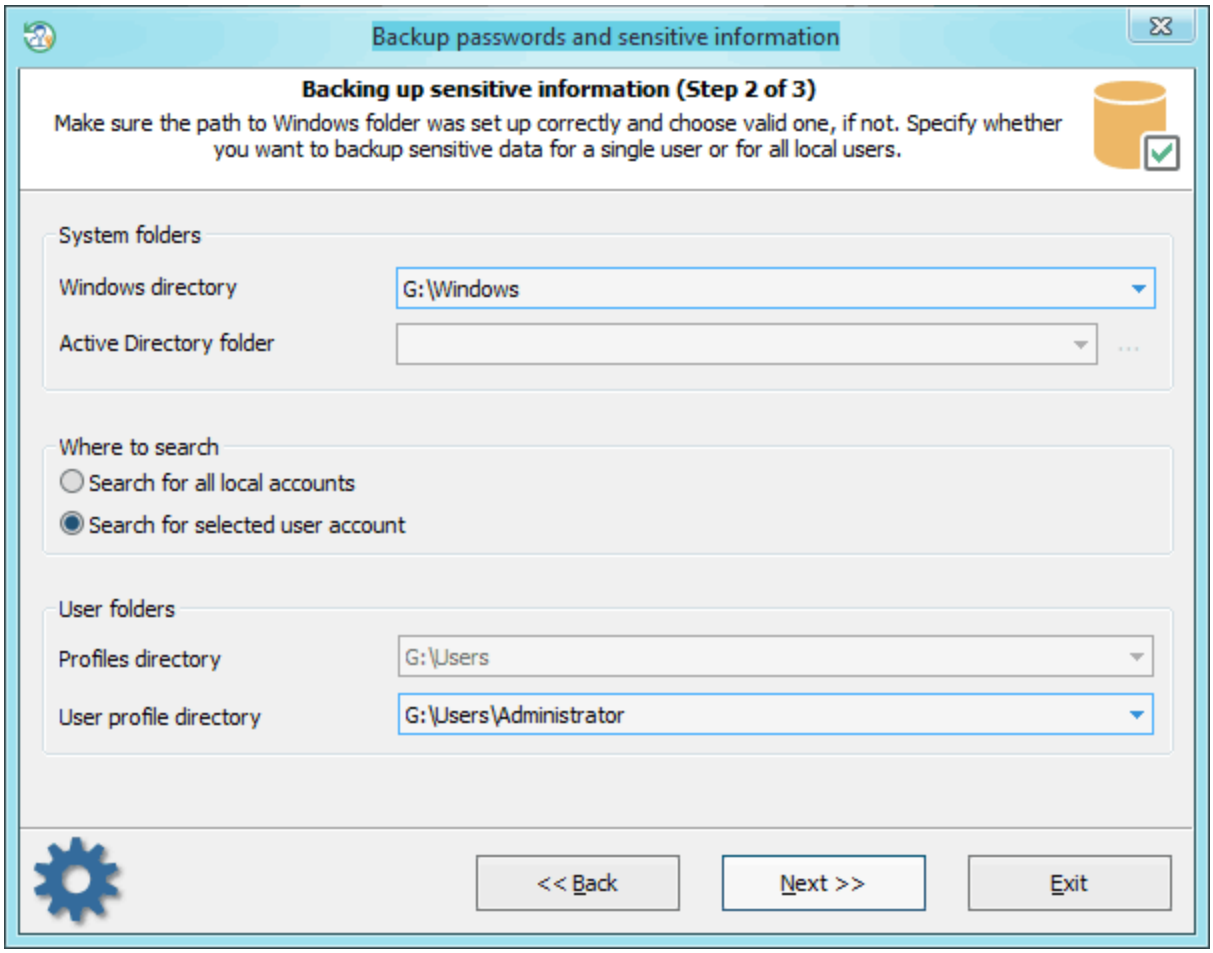


Сначала, выбрав этот инструмент, укажите, что необходимо сохранить:

- Файлы реестра Windows
- Базу данных Active Directory
- Персональную информацию, включая системные и пользовательские пароли и ключи шифрования, пароли почты и интернет, сертификаты, данные пользовательской и системной активности, артефакты для криминалистического анализа и т.д.
- Найденные файлы памяти или гибернации
- База данных поиска Windows

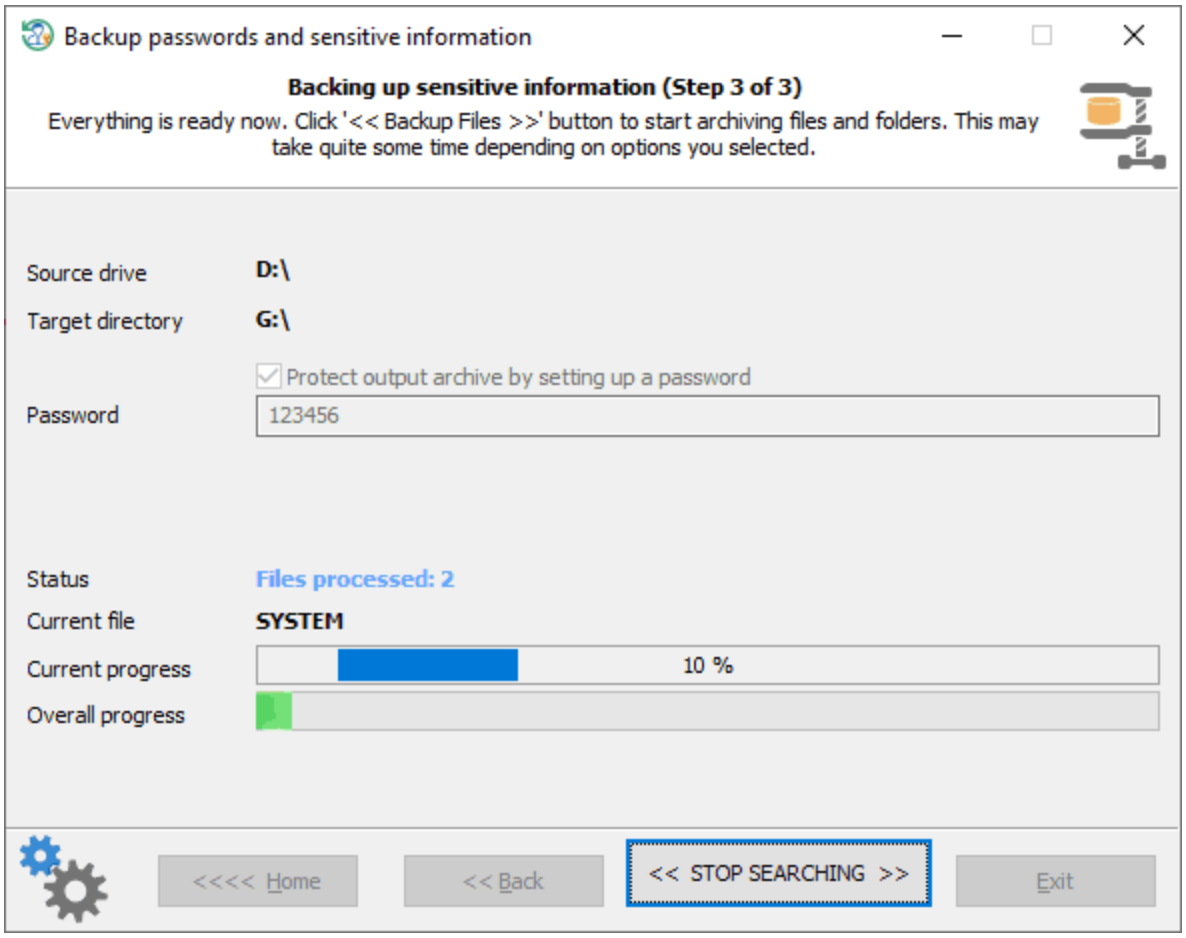
На первом шаге Мастера необходимо задать исходный диск, на котором находится каталог Windows, и целевой путь, куда будет сохранен полученный в результате работы архив с файлами. По умолчанию, программа предлагает первый жесткий диск в качестве источника данных и первый съемный диск (например, USB) в качестве целевого.

Выбор каталога Windows и учетной записи



Следующий шаг еще проще. В случае, если на предыдущем шаге было выбрано резервное копирование реестра или Active Directory, то все, что необходимо, это подтверждение правильно ли найдены каталоги Windows/NTDS. При резервном копировании паролей, требуется дополнительно задать либо профиль пользователя, либо папку с профилями всех пользователей. Соответственно, поиск паролей будет производиться либо в профиле выбранного пользователя, либо во всех найденных локальных профилях.

Резервной копирование

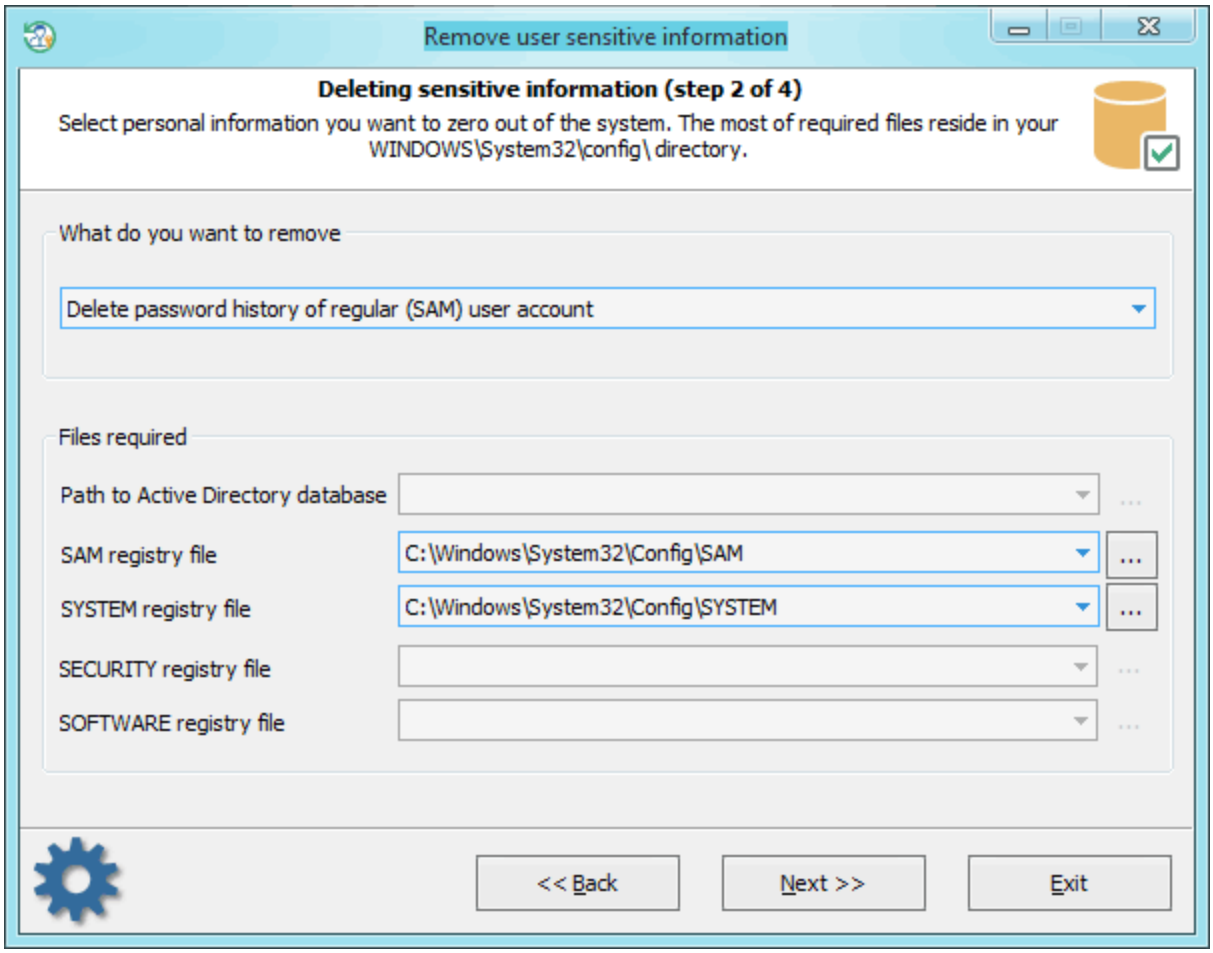


Финальный диалог есть не что иное, как прогресс запрошенной операции. Щелкните кнопку **<< Сохранение файлов >>** для запуска процесса копирования. После удачного завершения в целевом каталоге должен появиться *.ZIP архив с найденными файлами. Для защиты приватных данных программа позволяет установить пароль на ZIP архив.

Впоследствии, вы можете использовать найденные и сохраненные в архив файлы для анализа или аудита системы, а также для расшифровки паролей. Например, при помощи Windows Password Recovery.

3.9.3 Удаление приватной информации пользователя

Выбор источника данных



Программа имеет ряд дополнительных возможностей. Одна из которых - удаление информации, которая может быть использована потенциальными злоумышленниками для восстановления паролей учетных записей на вашем компьютере. Будьте внимательны, данная информация удаляется безвозвратно, без возможности дальнейшего восстановления. Итак, она включает в себя следующие пункты:

1. Удаление истории паролей стандартных учетных записей SAM и учетных записей пользователей Active Directory. История паролей SAM, к примеру, задается в групповой политике локального компьютера. Start -> Run -> gpedit.msc -> OK. Или, если отсутствует пункт Run (выполнить) в меню Windows, можно использовать горячие клавиши Win+R. В 'Computer Configuration' спускаемся вниз 'Windows Settings -> Security Settings -> Local Policies -> Security Options'. Находим следующую политику: *Interactive Logon: Number of previous logons to cache*.
2. Удаление кэшированных паролей домена. Подробнее о кэшированных паролях домена можно почитать здесь.
3. Удаление кэшированного пароля на вход в Windows.
4. Удаление информации о сбросе пароля. С помощью данной информации и дискеты сброса, потенциальный злоумышленник может легко восстановить оригинальный текстовый пароль.
5. Удаление подсказок о пароле.
6. Обнуление SYSKEY.

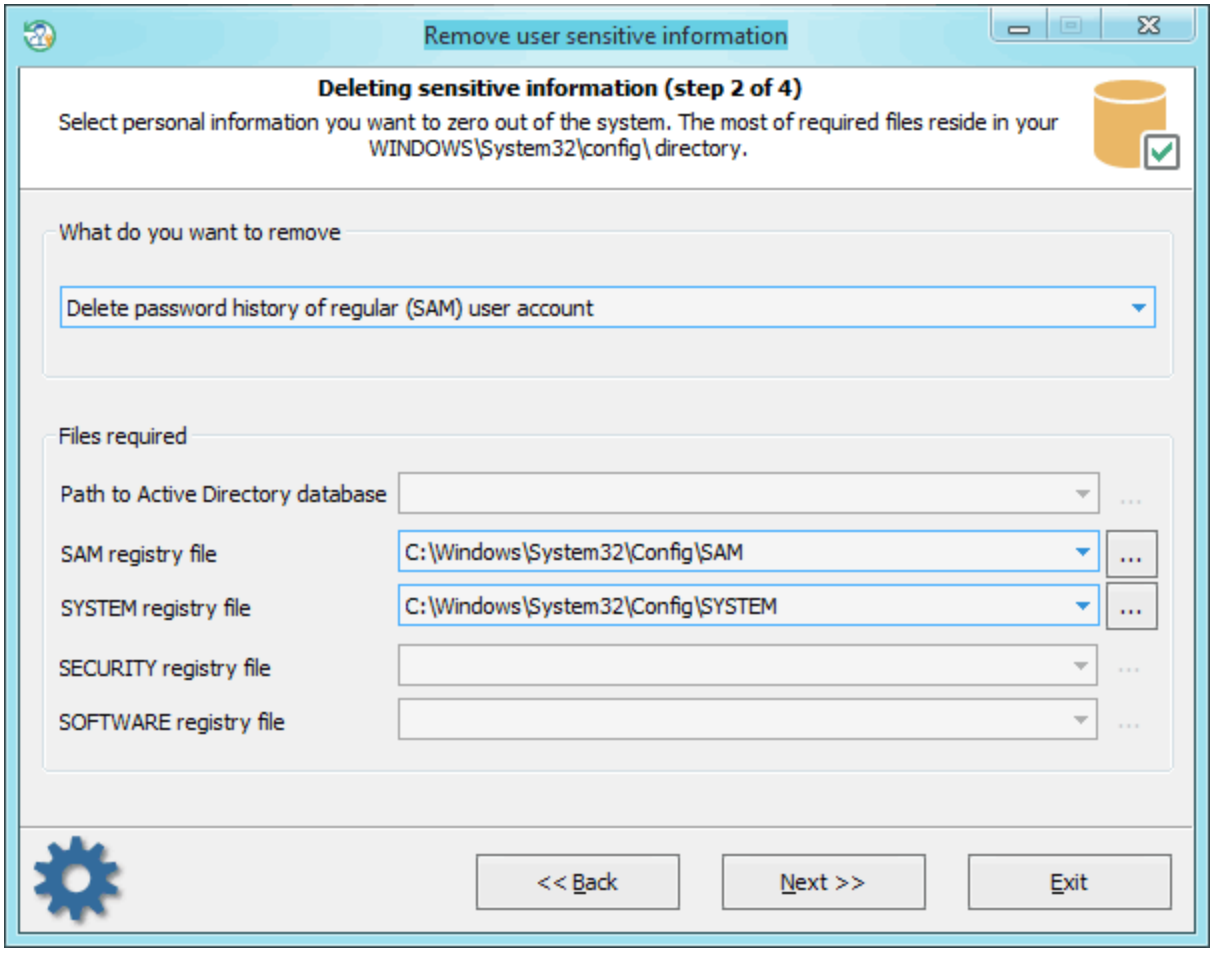
Для продолжения работы, программе требуется указать (или выбрать из найденных) следующие файлы:
- Удаление истории паролей Active Directory – файл реестра **SYSTEM** и база данных Active Directory (файл **ntds.dit**);

- Удаление истории паролей SAM – файлы реестра **SAM** и **SYSTEM**
- Удаление кэшированных паролей домена – файлы **SECURITY** и **SYSTEM**
- Удаление кэшированных логон паролей – файлы **SECURITY**, **SOFTWARE** и **SYSTEM**
- Удаление информации о сбросе пароля - файлы **SAM**, **SECURITY** и **SYSTEM**
- Удаление подсказок о пароле - **SAM**, **SOFTWARE** и **SYSTEM**
- Сброс SYSKEY - **SAM**, **SECURITY** и **SYSTEM**

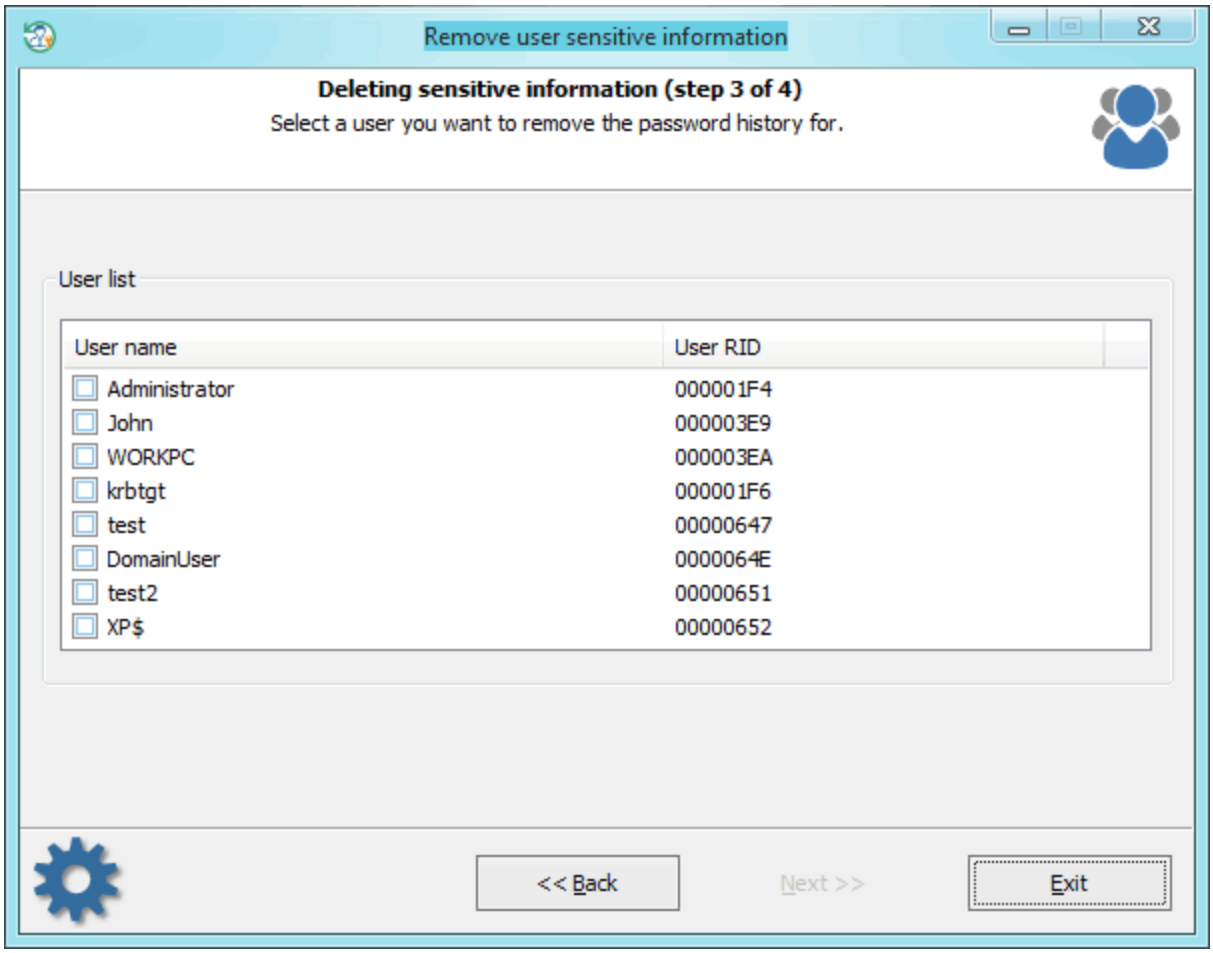
Все файлы реестра за исключением базы данных Active Directory находятся в каталоге **%WINDIR%\system32\config**. Где %WINDIR% - каталог Windows, по умолчанию C:\Windows. Месторасположение базы Active Directory задается при установке. По умолчанию, это каталог **%WINDIR%\NTDS**.

3.9.3.1 Удаление истории паролей

Выбор источника данных

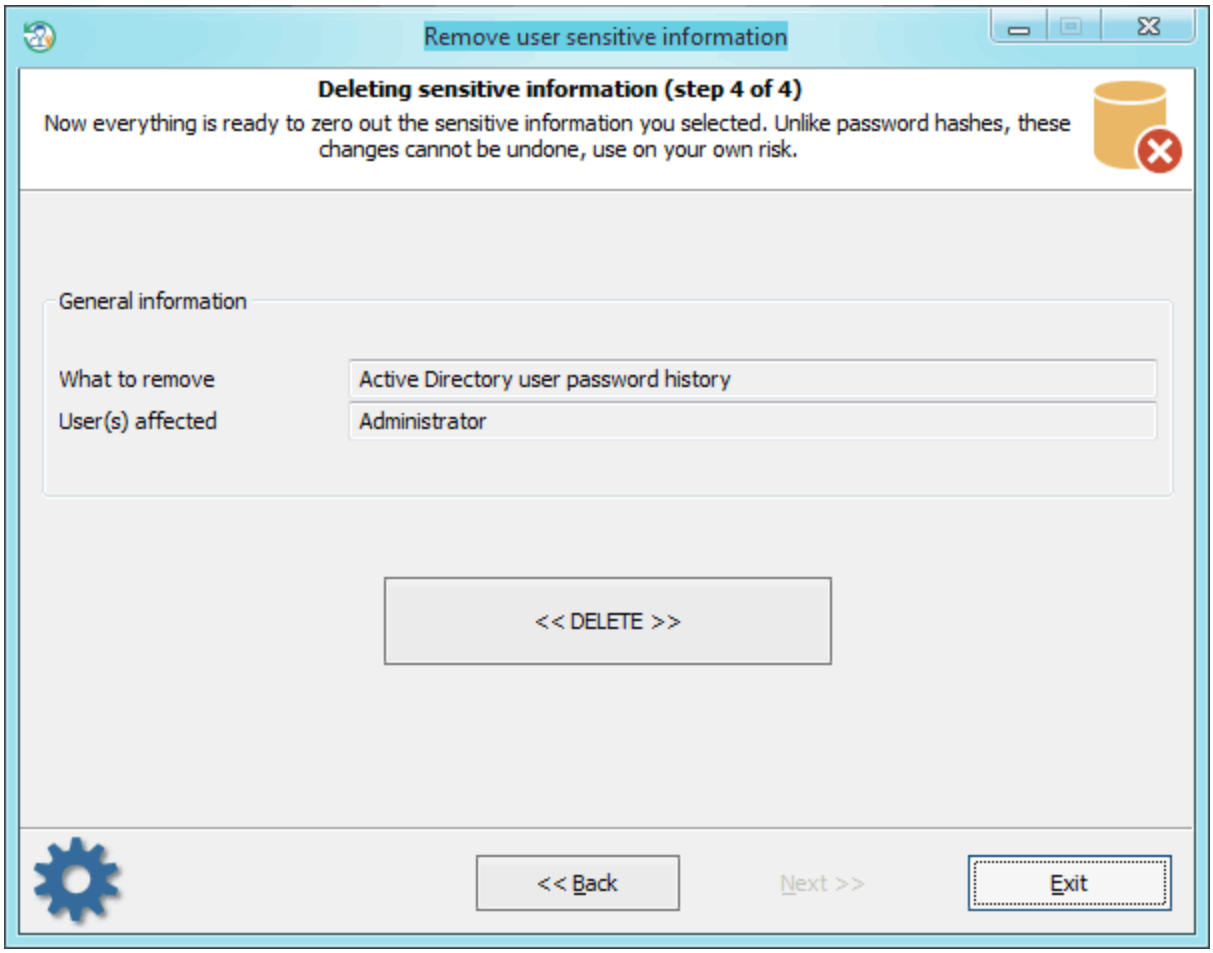


Выбор пользователя



Из списка учетных записей выбираем ту, для которой необходимо удалить историю паролей. Программа показывает только тех пользователей, у которых присутствует история.

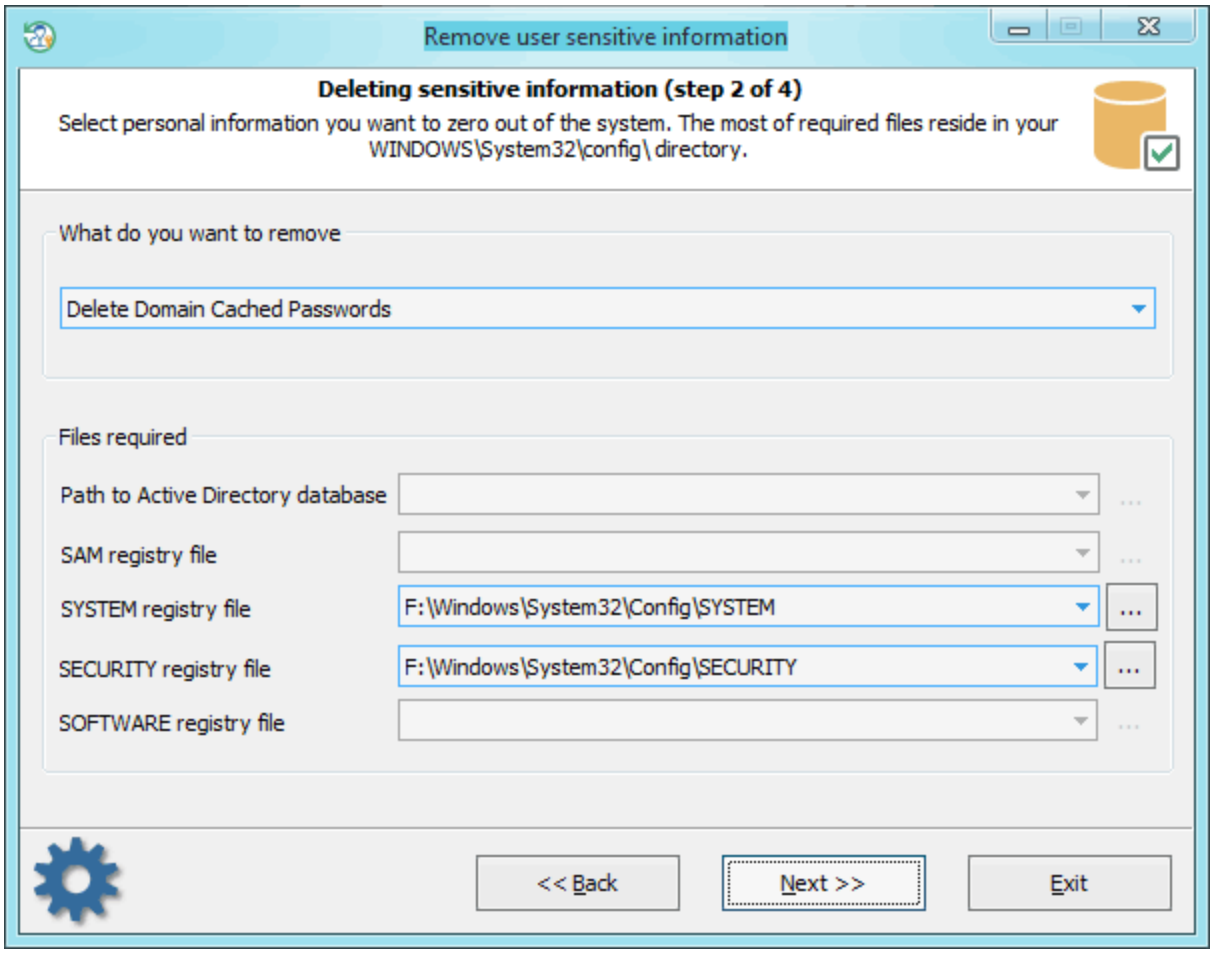
Удаление истории паролей



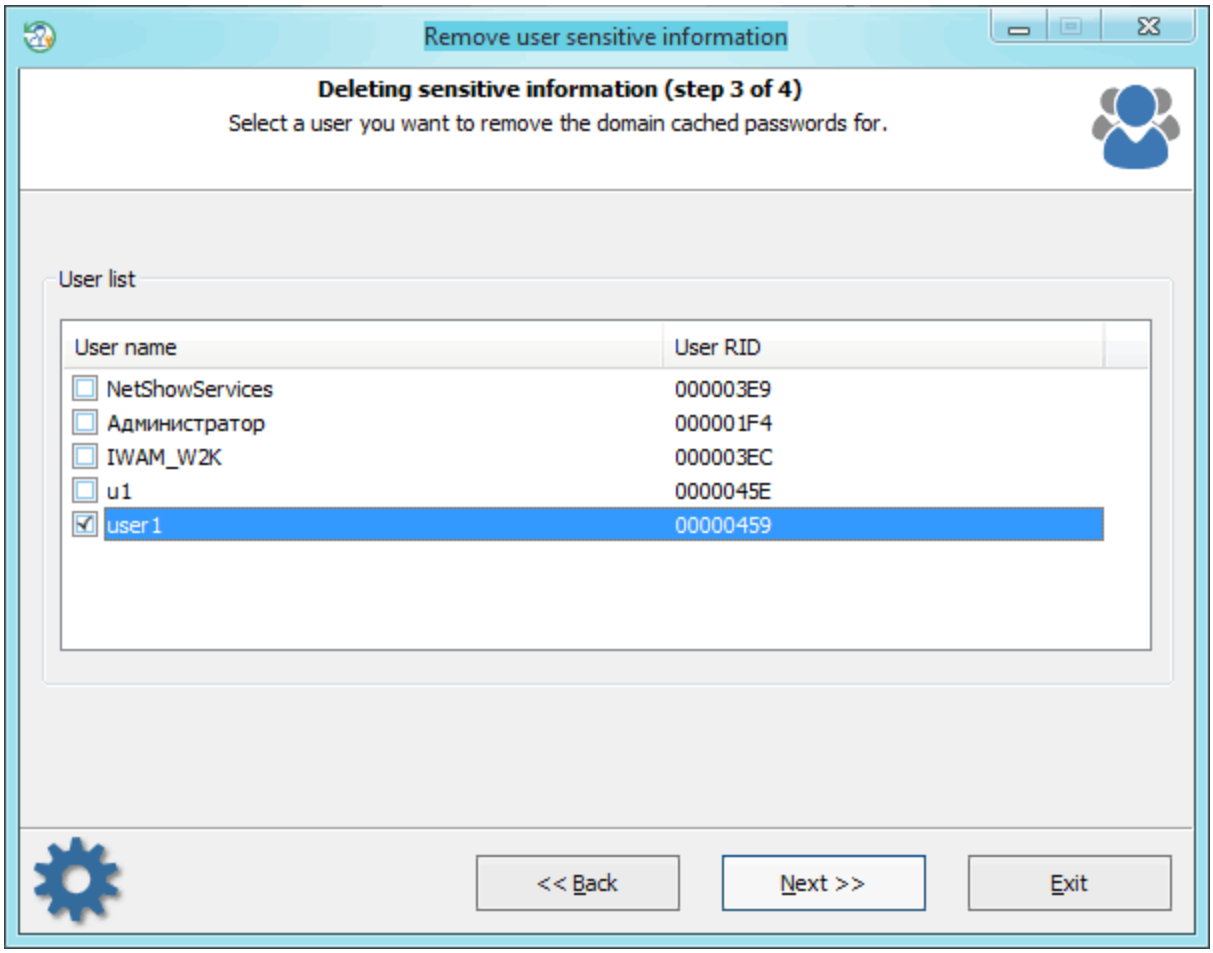
Жмем <<Delete>> и навсегда избавляемся от ненужной нам информации.

3.9.3.2 Удаление кэшированных паролей домена

Выбор источника данных

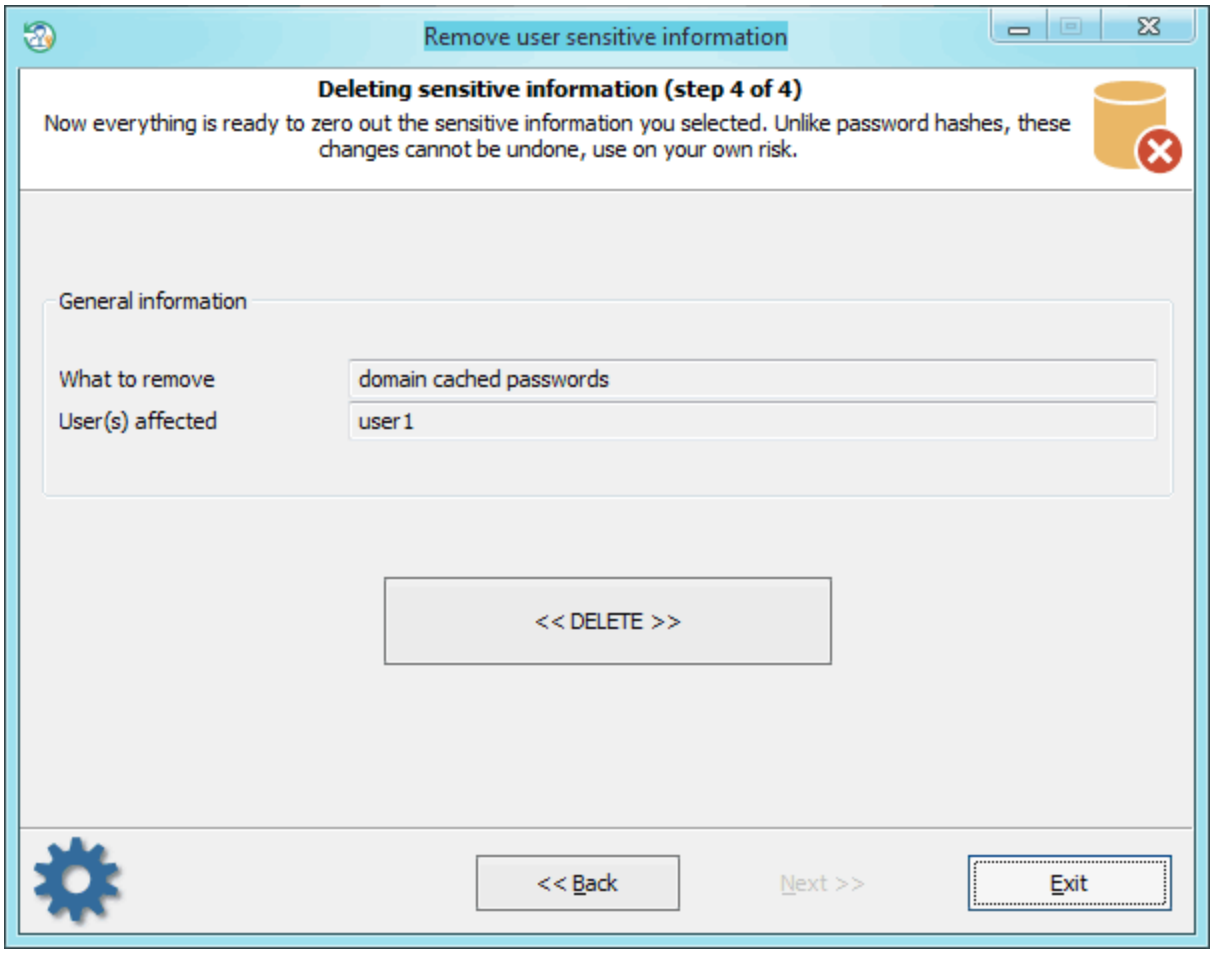


Выбор пользователя



Выбираем учетную запись, кэшированные пароли которой нам надо вычистить из системы.

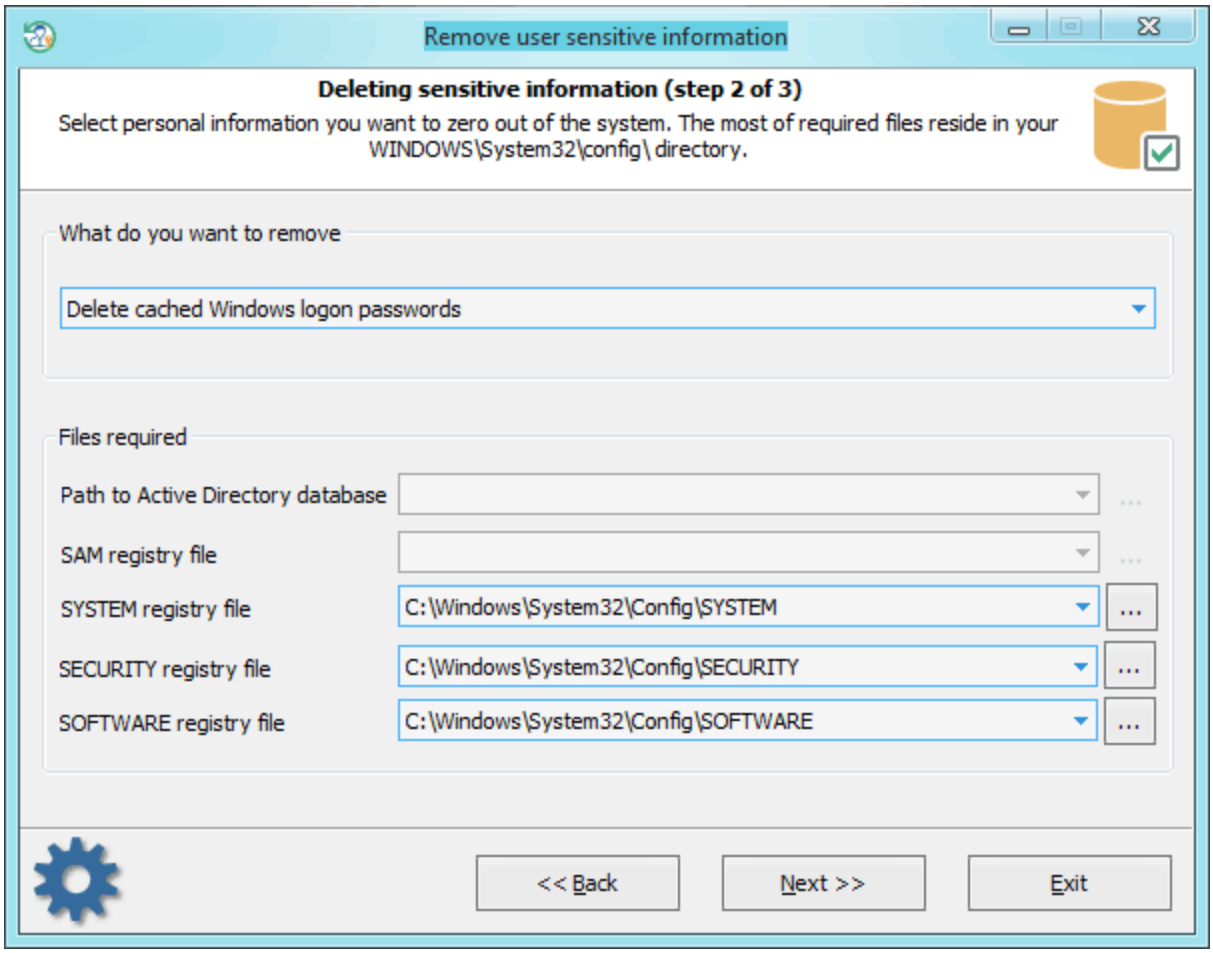
Удаление кэшированных паролей домена



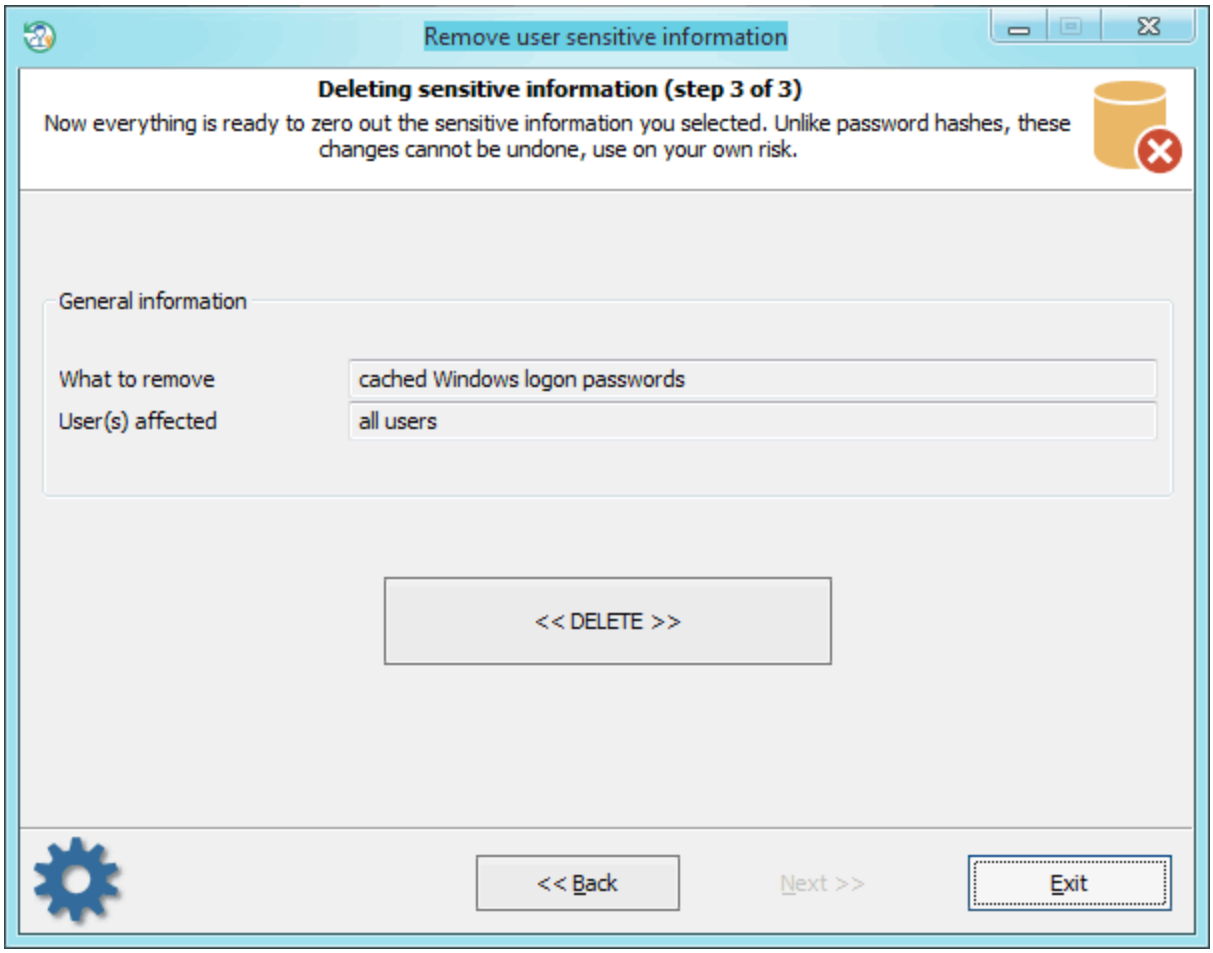
Подтверждаем удаление всех найденных кэшированных пароле для учетной записи домена user1.

3.9.3.3 Удаление локальных кэшированных паролей

Выбор источника данных



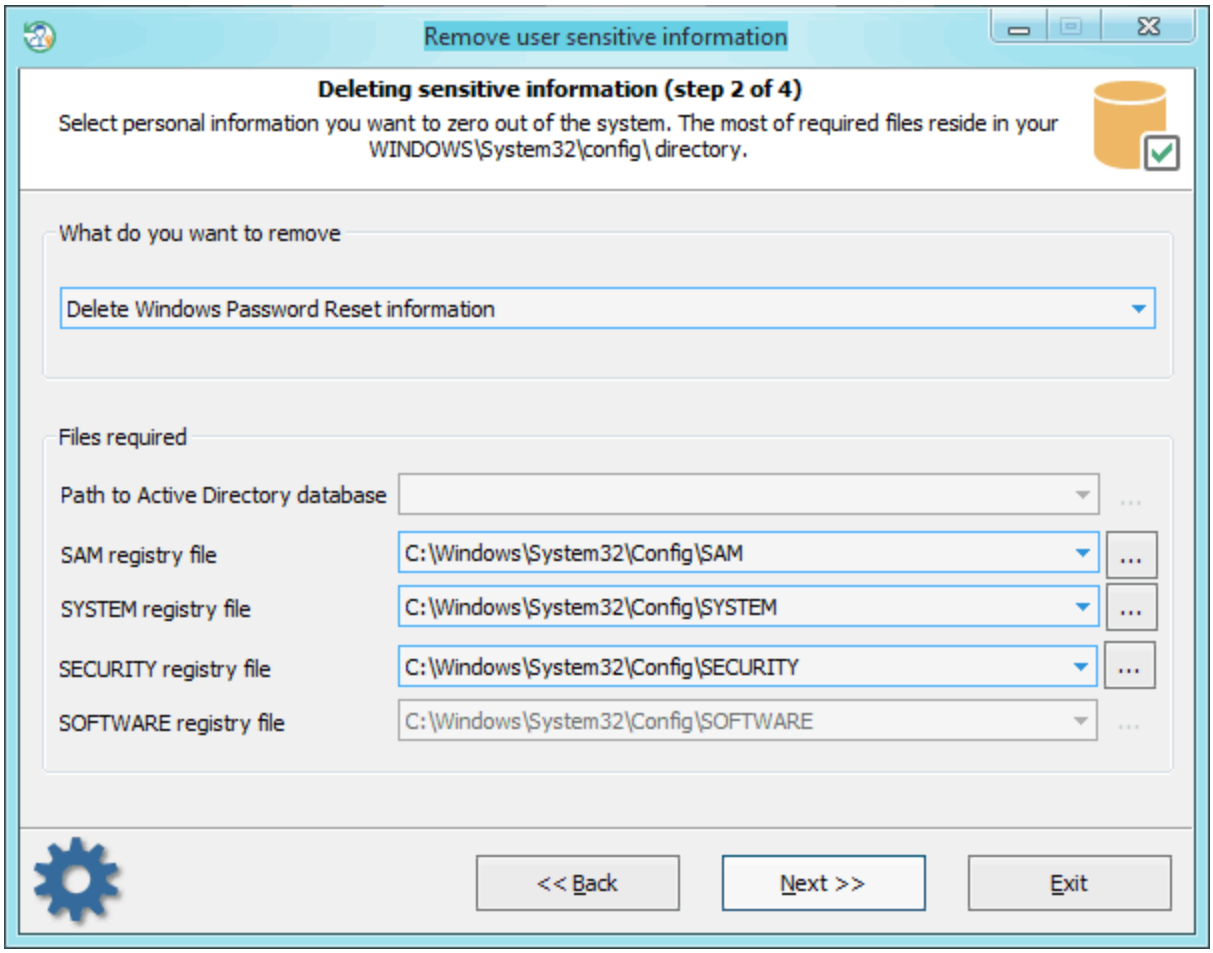
Удаление кэшированных паролей локальных учетных записей Windows



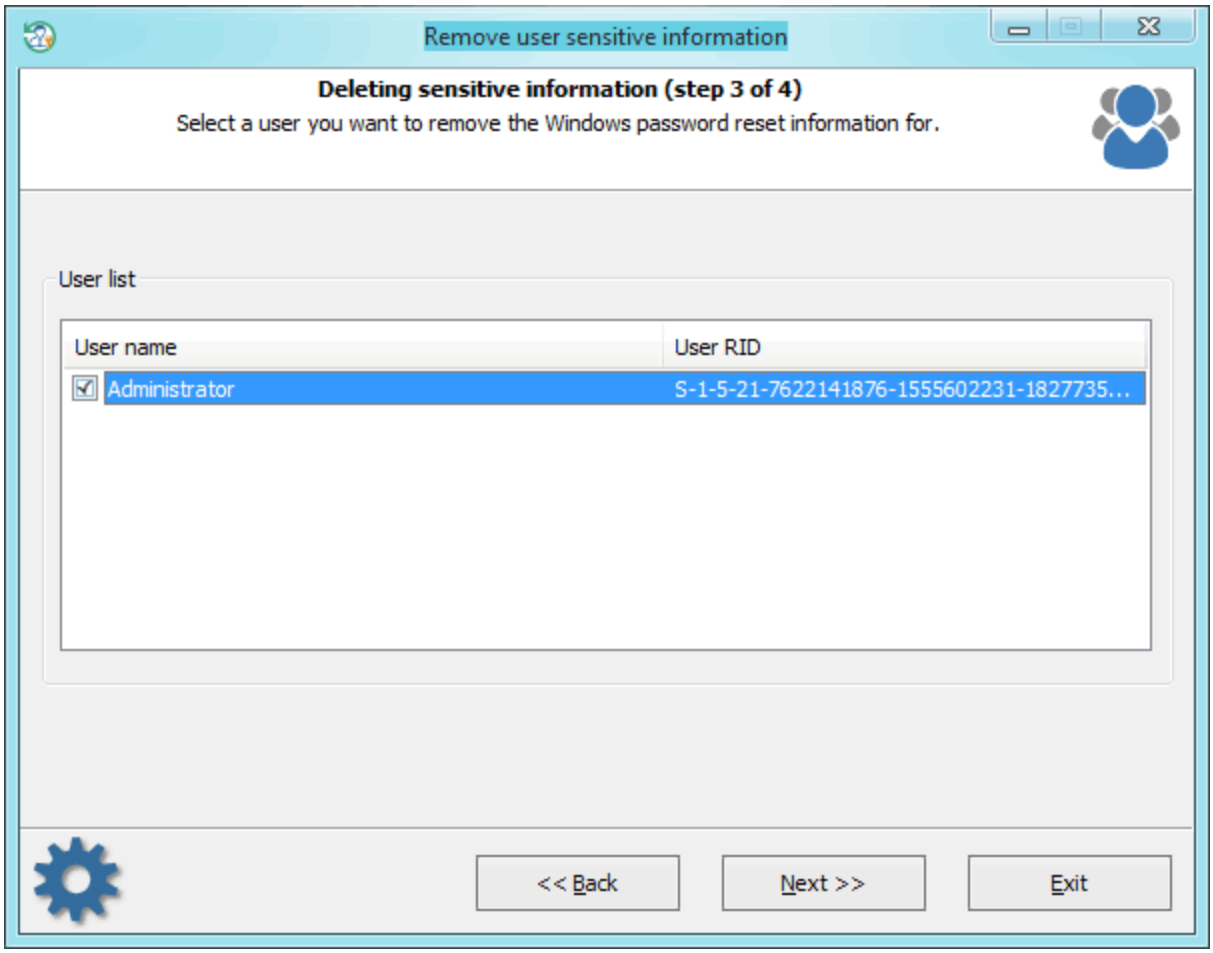
Подтверждаем удаление всех кэшированных паролей на локальном компьютере.

3.9.3.4 Удаление информации о сбросе пароля

Выбор источника данных

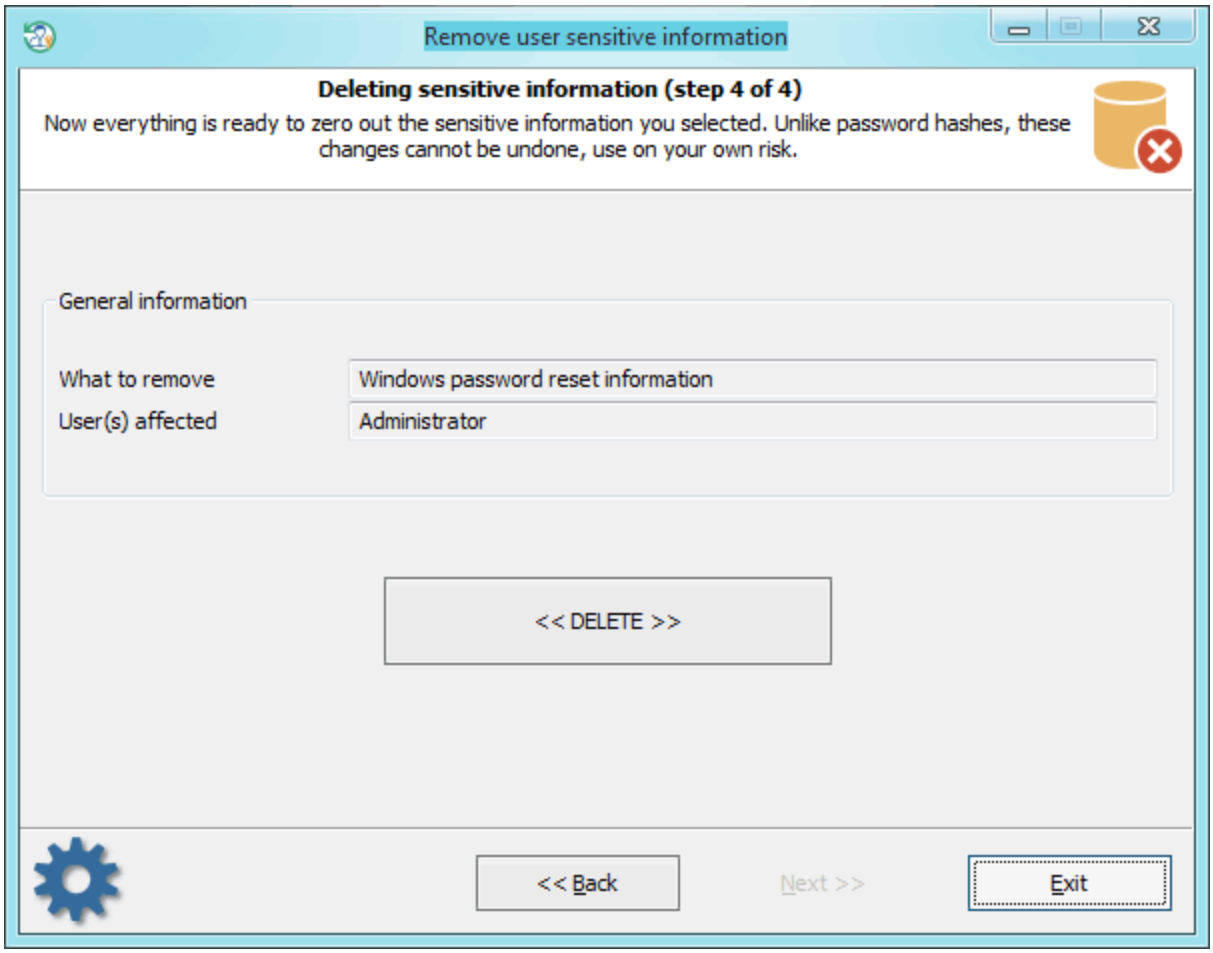


Выбор пользователя



Выбираем пользователя, чью информацию надо удалить. Во время создания дискеты сброса пароля, зашифрованный пароль пользователя сохраняется в реестре Windows. Тогда как на самой дискете находится ключ шифрования. Удаление зашифрованного пароля из реестра, делает дальнейшее существование дискеты бесполезным.

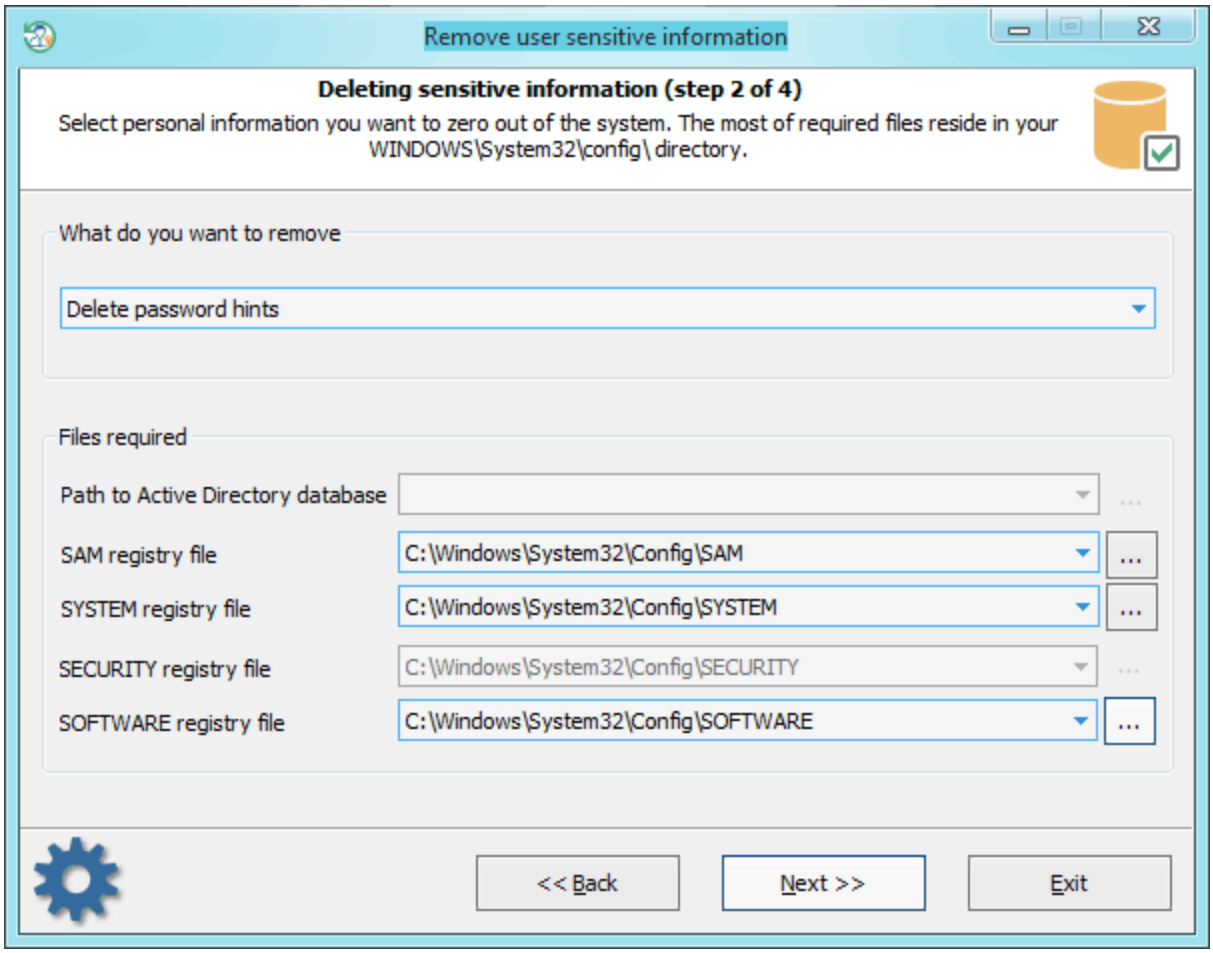
Удаление информации о дискете сброса пароля



Подтверждаем удаление.

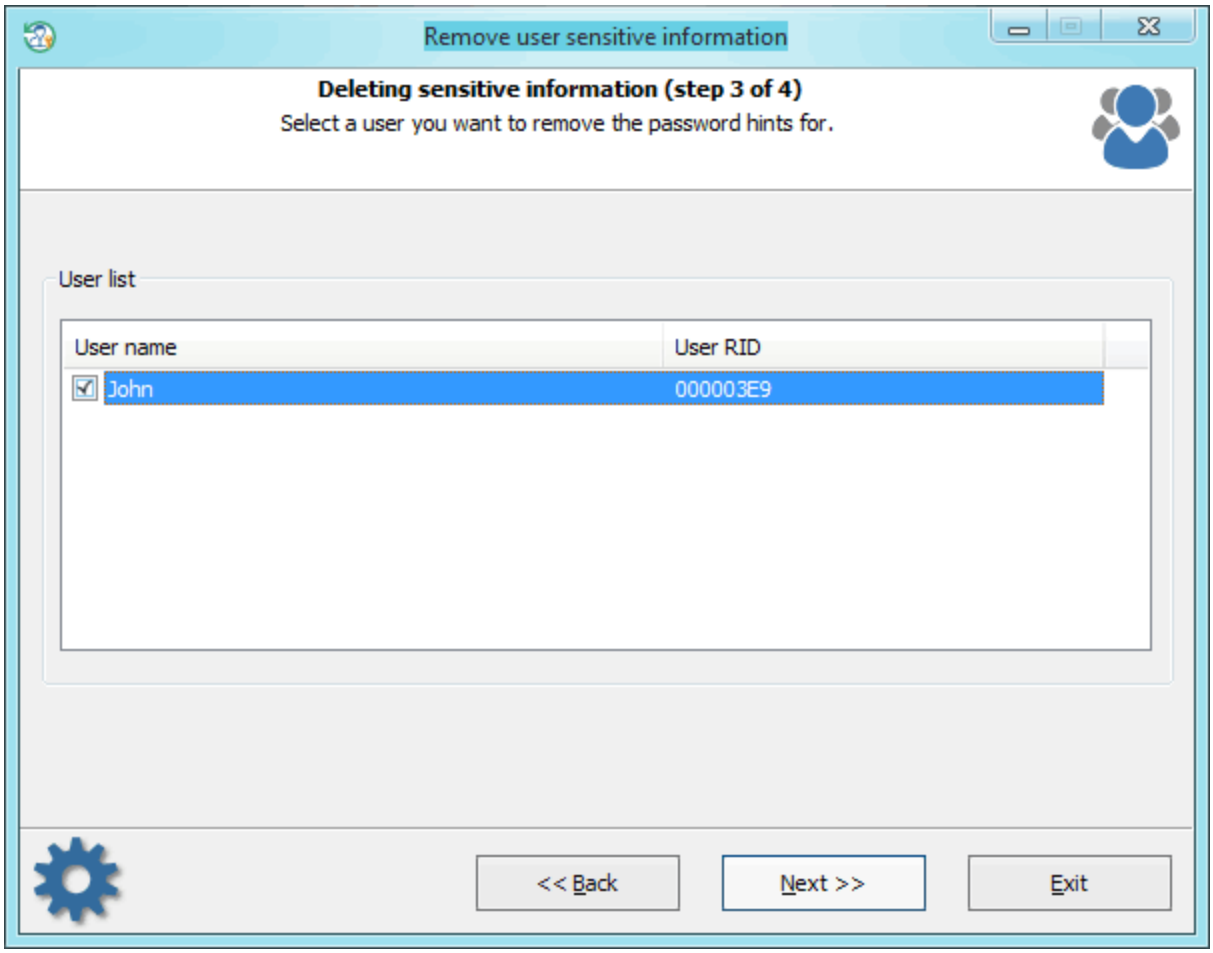
3.9.3.5 Удаление подсказок о пароле

Выбор источника данных



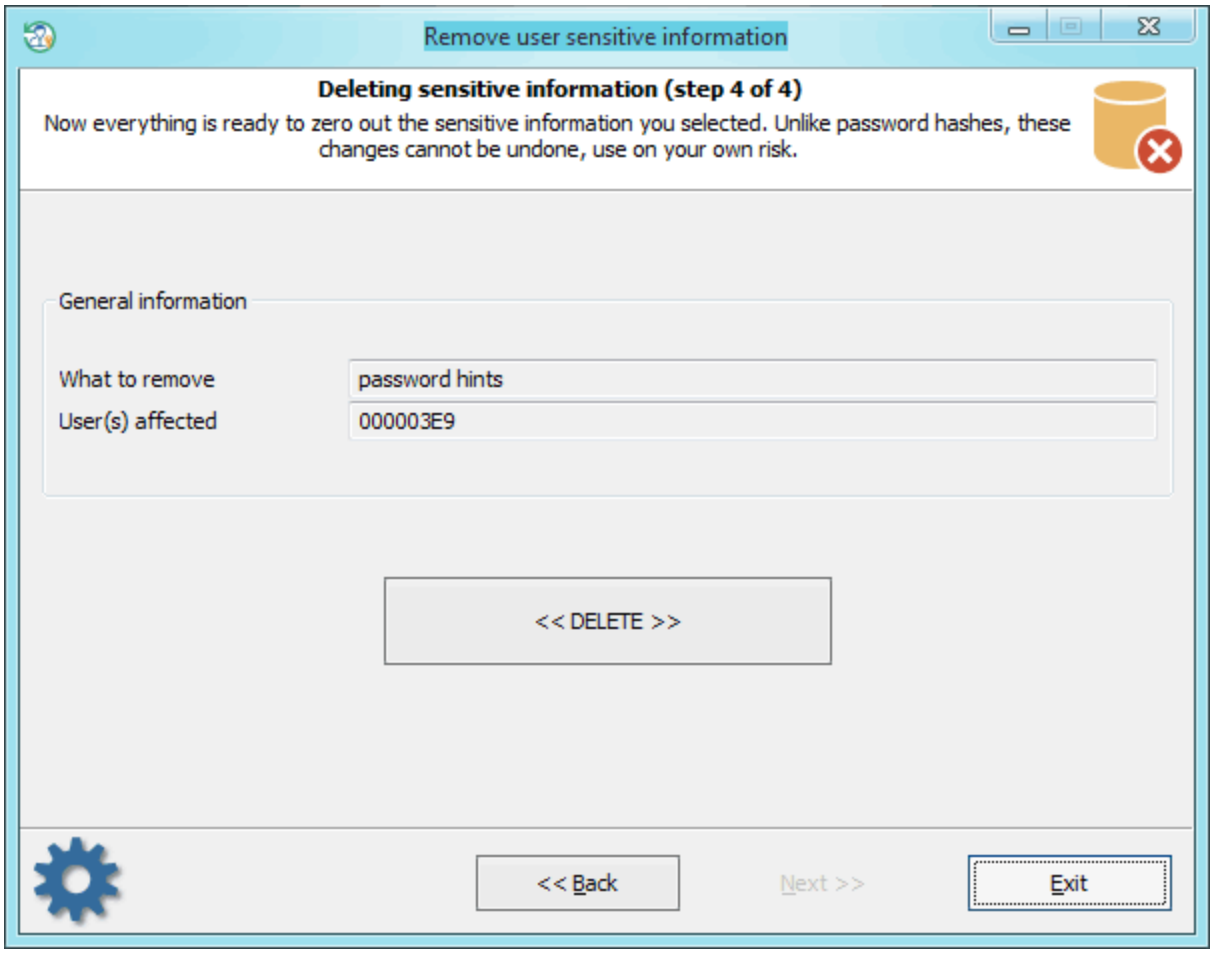
Подсказки о паролях хранятся либо в файле реестра SOFTWARE (операционные системы Windows XP, Windows 2003), либо в SAM файле (Windows Vista и выше). Расшифровка подсказок требует также наличие файла SYSTEM.

Выбор пользователя



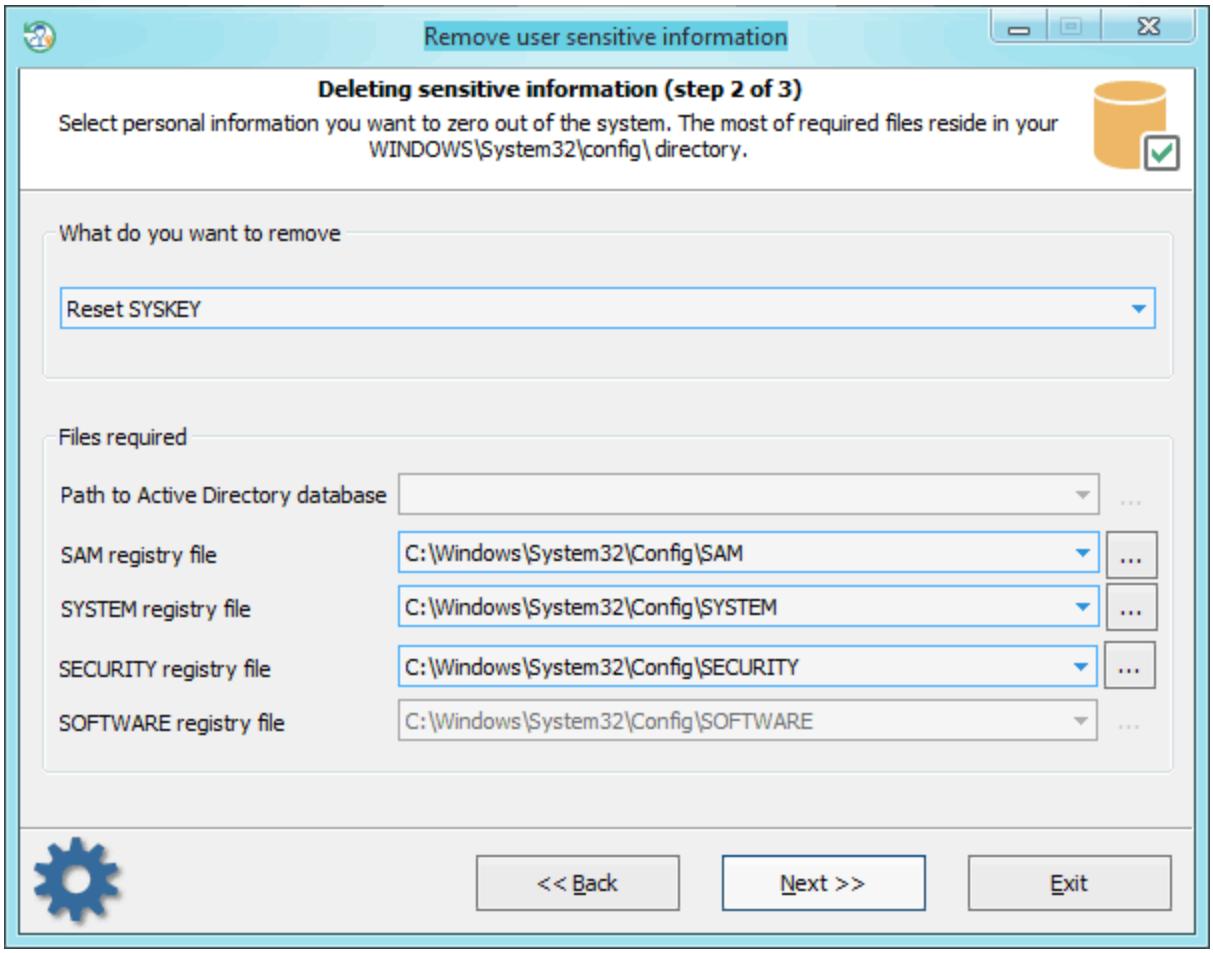
Выберите пользователя, чьи подсказки необходимо вычистить из системы и следуйте дальнейшем указаниям Мастера программы.

Удаление подсказок



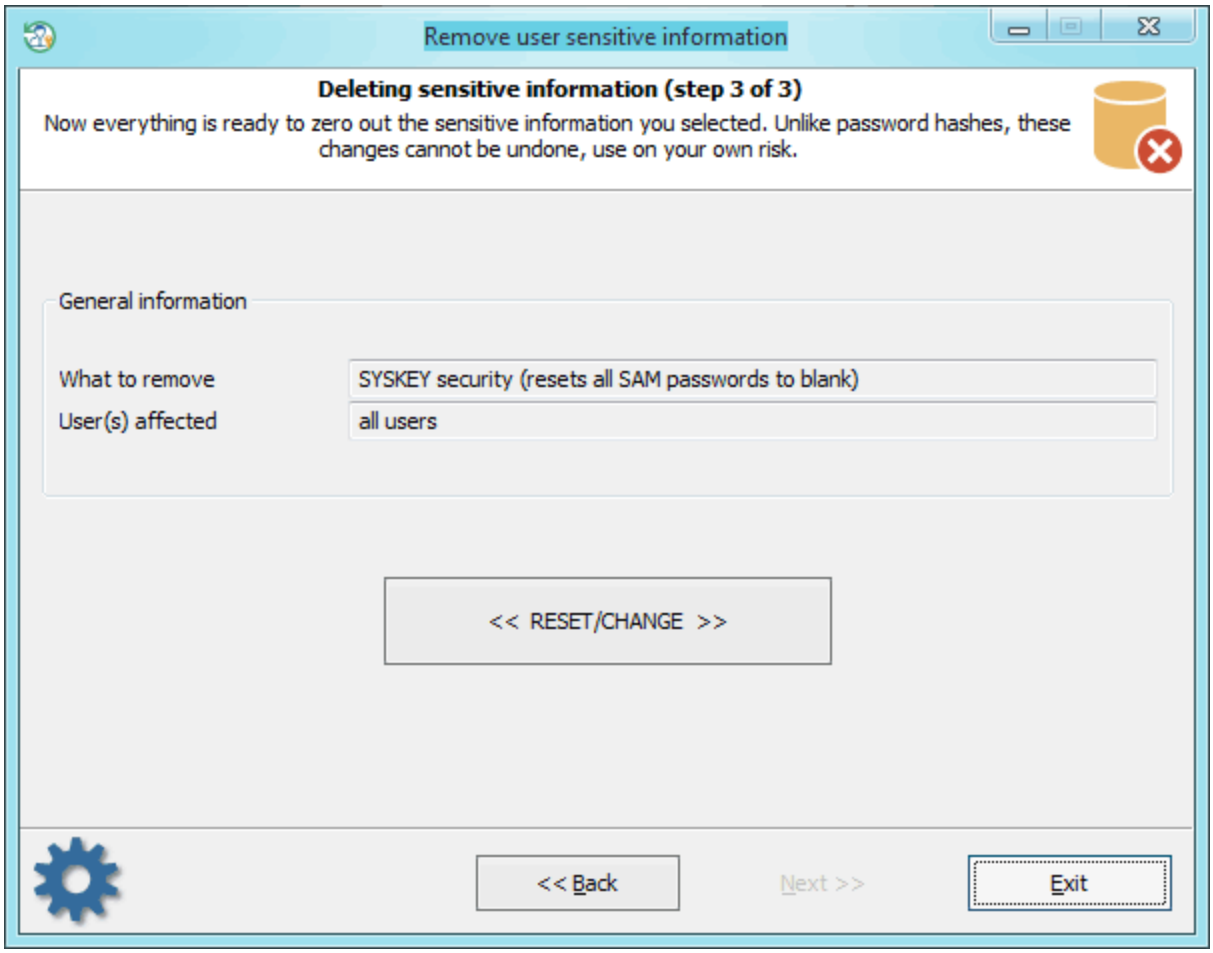
3.9.3.6 Сброс SYSKEY

Выбор источника данных



Для начала, необходимо указать пути к трем файлам реестра: **SAM**, **SYSTEM** и **SECURITY**. Обычно SYSKEY находится в реестре SYSTEM, прячась в ветке **HKLM\CurrentControlSet\Control\Lsa**. Но если однажды вы, к примеру, установили SYSKEY так, чтобы при загрузке системы запрашивался пароль, и забыли его, у вас нет ни единого шанса попасть в систему. Что тут и говорить - SYSKEY является чрезвычайно эффективным инструментом в руках умелого мастера. Установка начального пароля SYSKEY или дискеты с паролем является очень эффективным оружием против ВСЕХ(!) программ, восстанавливающих пароли Windows.

Сброс SYSKEY



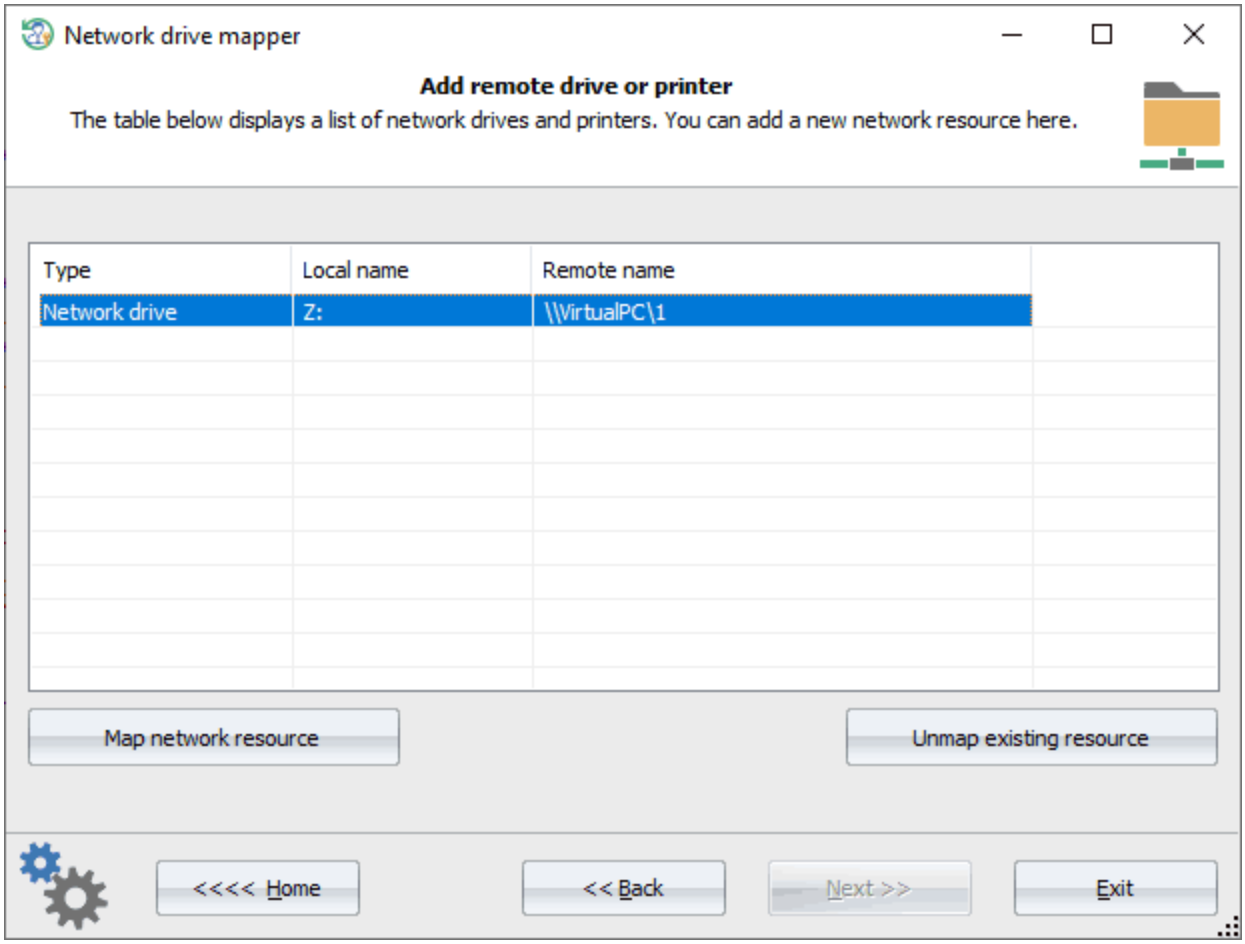
Внимание! Сброс SYSKEY является небезопасной операцией, влияющей на безопасность всей системы. Например, после сброса SYSKEY, даже если вы сможете залогиниться под своей учетной записью, то потеряете доступ к зашифрованным файлам EFS, всем данных, защищенным при помощи DPAPI, и даже настройкам рабочего стола.

В сети существует несколько программ, которые сбрасывают SYSKEY, но ни одна из них не работает корректно. Причиной является то, что кроме самого сброса SYSKEY, требуется выполнить ряд дополнительных мероприятий для предотвращения падения системы во время загрузки. Например, требуется обнуление сессионных ключей в домене SAM, перешифровка и сброс паролей локальных пользователей, LSA секретов и др. Reset Windows Password имеет в своем арсенале 2 алгоритма для сброса SYSKEY. Если не сработает основной, то автоматически запускается вспомогательный. После сброса SYSKEY все пароли локальных пользователей обнуляются.

Важно! После сброса SYSKEY на операционной системе Windows 8, вам необходимо установить любой непустой пароль для всех (или только для той, которая будет использоваться для входа) учетных записей LiveID. В противном случае, вы не сможете зайти в систему с пустым паролем.

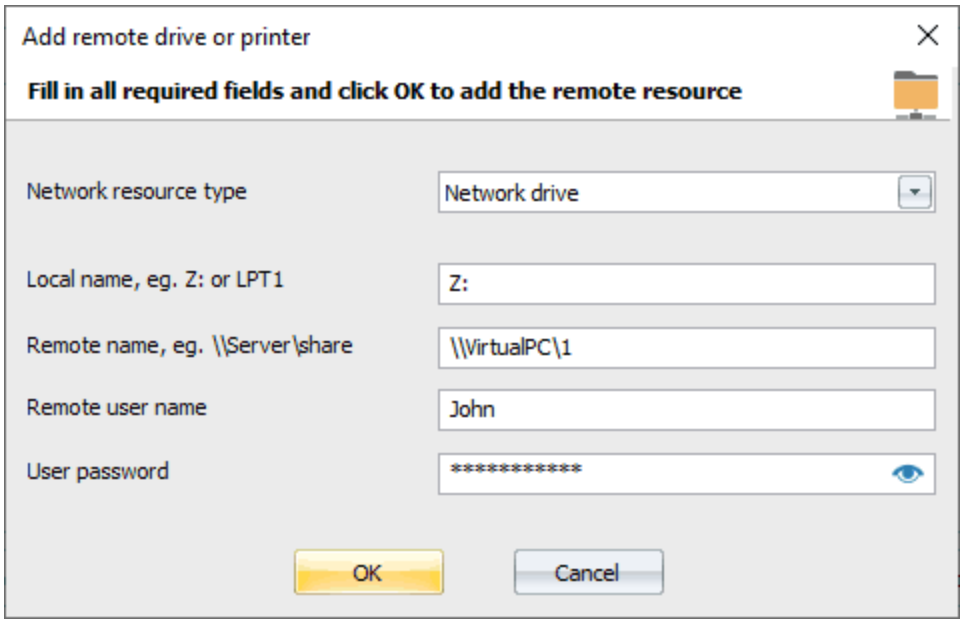
3.9.4 Подключение сетевых дисков

Эта утилита предназначена для подключения к локальным сетевым ресурсам компьютера.



Чтобы создать новый сетевой диск, нажмите кнопку 'Map Network resource'. В появившемся диалоге введите имя удаленного ПК в формате \\SERVER\SHARE, имя удаленного пользователя и его пароль.
где SERVER - удаленный ПК или его IP адрес
SHARE - имя ресурса с общим доступом

Например,
\\WIN-C2KSHD76D\forall
\\VPC\1
\\COMP2\C$

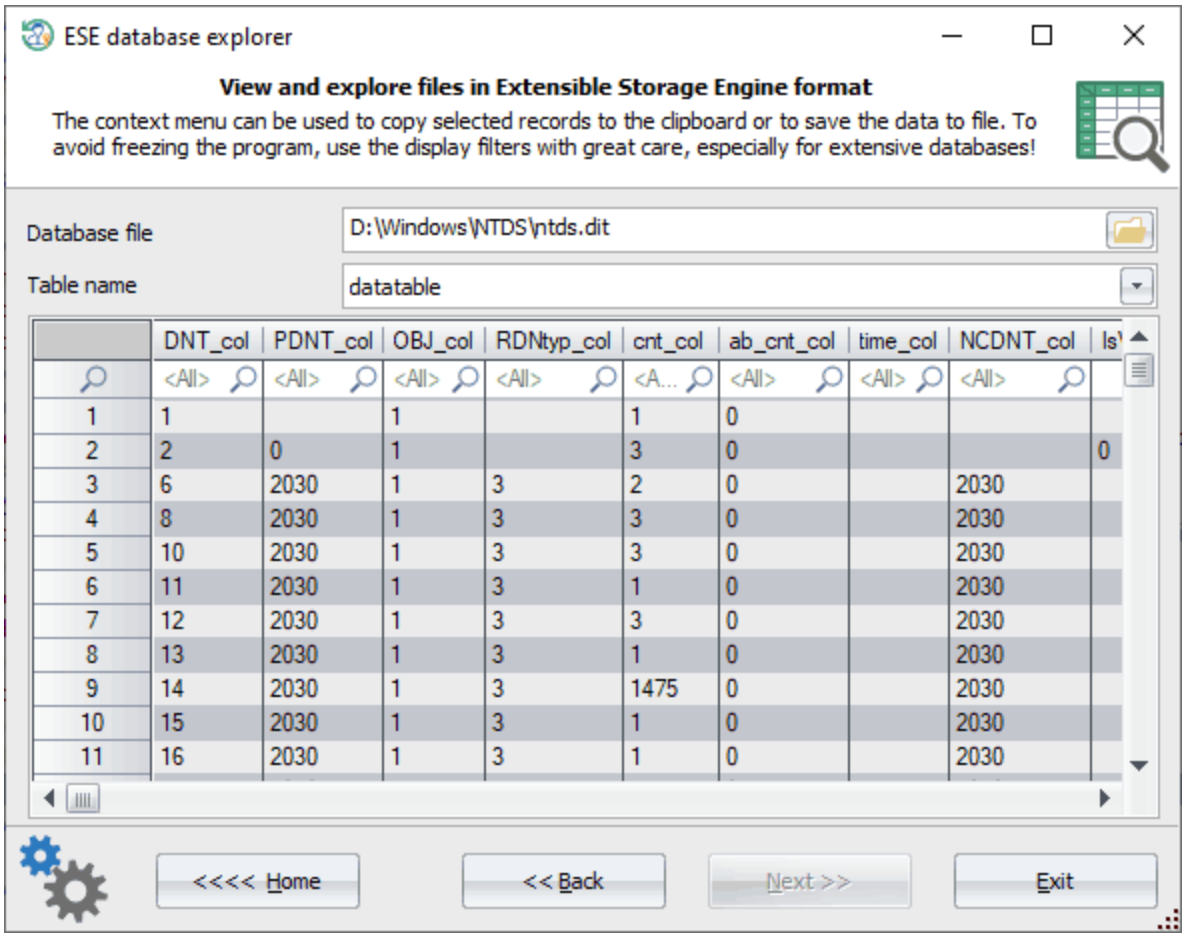


3.9.5 Обозреватель баз данных ESE (Extensible Storage Engine)

Extensible Storage Engine (ранее именуемый как **Jet Blue** в некоторых документах Microsoft) - это движок для хранения данных, разработанный Microsoft и не основанный на SQL. Он отлично работает с большим объемом данных и является ядром Active Directory, сервера Microsoft Exchange, Windows Search, центра обновления Windows, монитора использования системных ресурсов, веб-кэша и других компонентов Windows.

ESE имеет долгую и интересную историю создания, и изначально этот формат был закрытым. Вот почему чтение и анализ файлов в формате ESE являлось нетривиальной задачей в течение довольно продолжительного времени. Недавно Microsoft открыла спецификацию этого формата.

В отличие от некоторых бесплатных инструментов, которые читают файлы в формате ESE с ошибками (например, ESEDatabaseView от NirSoft), RWP применяет более надежный способ парсинга: точно такой же, какой используются в приложениях Microsoft (при помощи документированных API функций). Однако функциональность обозревателя ESE оставляет желать лучшего. В большинстве случаев он хорош только для первоначального анализа баз.



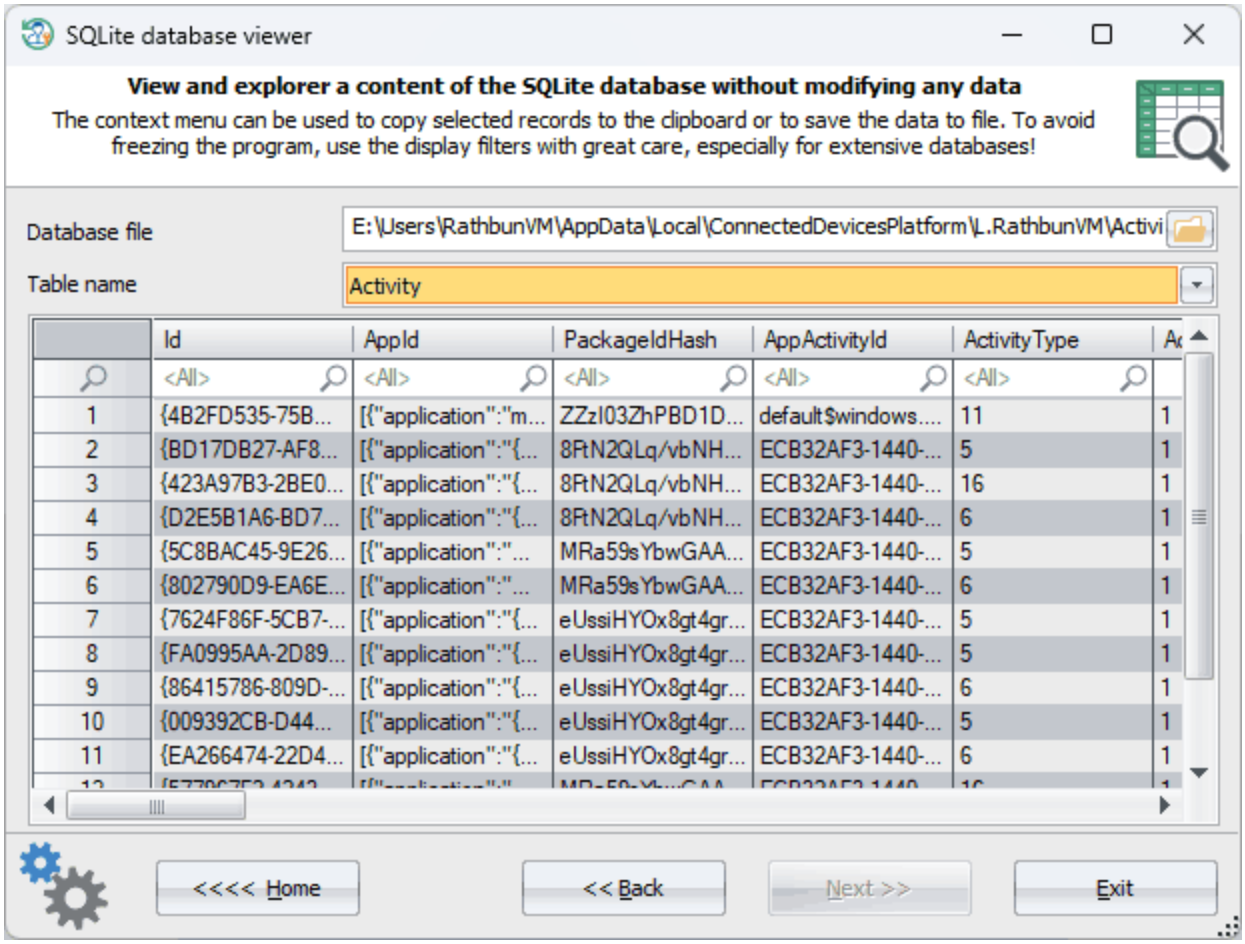
Интерфейс инструмента чрезвычайно прост. После того как вы укажете путь к файлу базы данных, можно открыть одну из найденных там таблиц. Далее, используя контекстное меню, можно, например, экспортировать таблицу в CSV-файл для дальнейшего изучения с помощью сторонних приложений.

Для разбора некоторых баз данных ESE программа имеет в своем наличии парсеры более высокого уровня. Например, база данных Windows Search представляет собой ESE файл, расположенный по адресу: *%SYSTEMDRIVE%\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb*

Несмотря на то, что можно открыть и просмотреть файл в обозревателе ESE, более разумным способом его анализа было бы использование вместо этого утилиты Windows Search explorer.

3.9.6 Просмотр баз данных SQLite

Средство просмотра баз данных SQLite - это чрезвычайно простой инструмент для просмотра и анализа баз данных в формате **SQLite**.



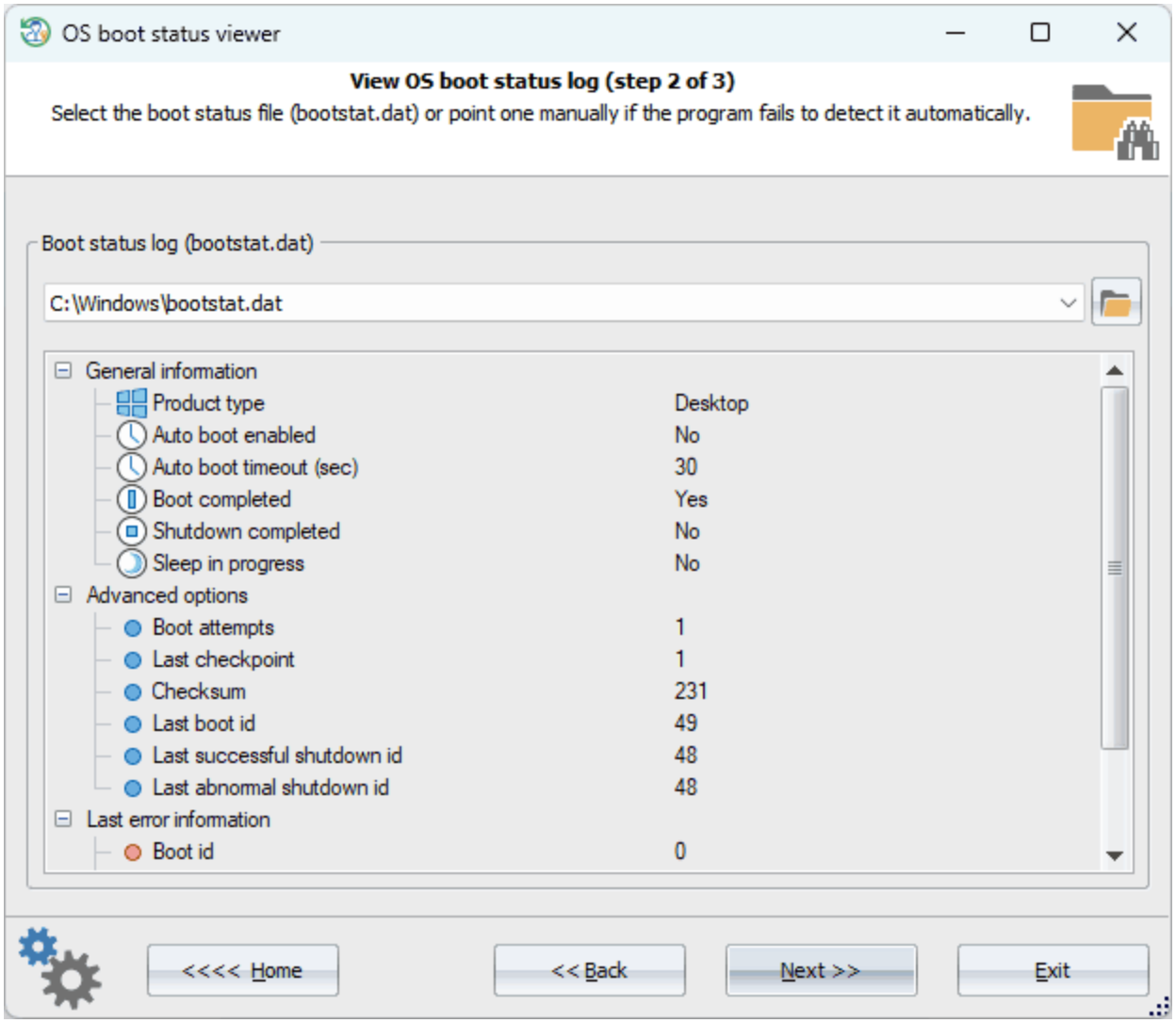
После того как указан путь к файлу SQLite, можно будет выбрать для просмотра одну из таблиц, которые содержатся в этой базе данных. Далее, используя контекстное меню, вы можете, например, сохранить данные любой ячейки или экспортировать всю таблицу в CSV-файл для дальнейшего изучения с помощью сторонних приложений.

3.9.7 Журнал состояния загрузки ОС

Утилита для просмотра состояния загрузки отслеживает процесс загрузки операционной системы и выявляет проблемы, которые могут возникнуть во время загрузки. Данный инструмент анализирует файл **bootstat.dat** и извлекает информацию о загрузке, которая хранится в диспетчере загрузки Windows, включая (но не ограничиваясь) предыдущую последовательность загрузки, последнюю успешную загрузку, а также все предыдущие неудачные попытки.

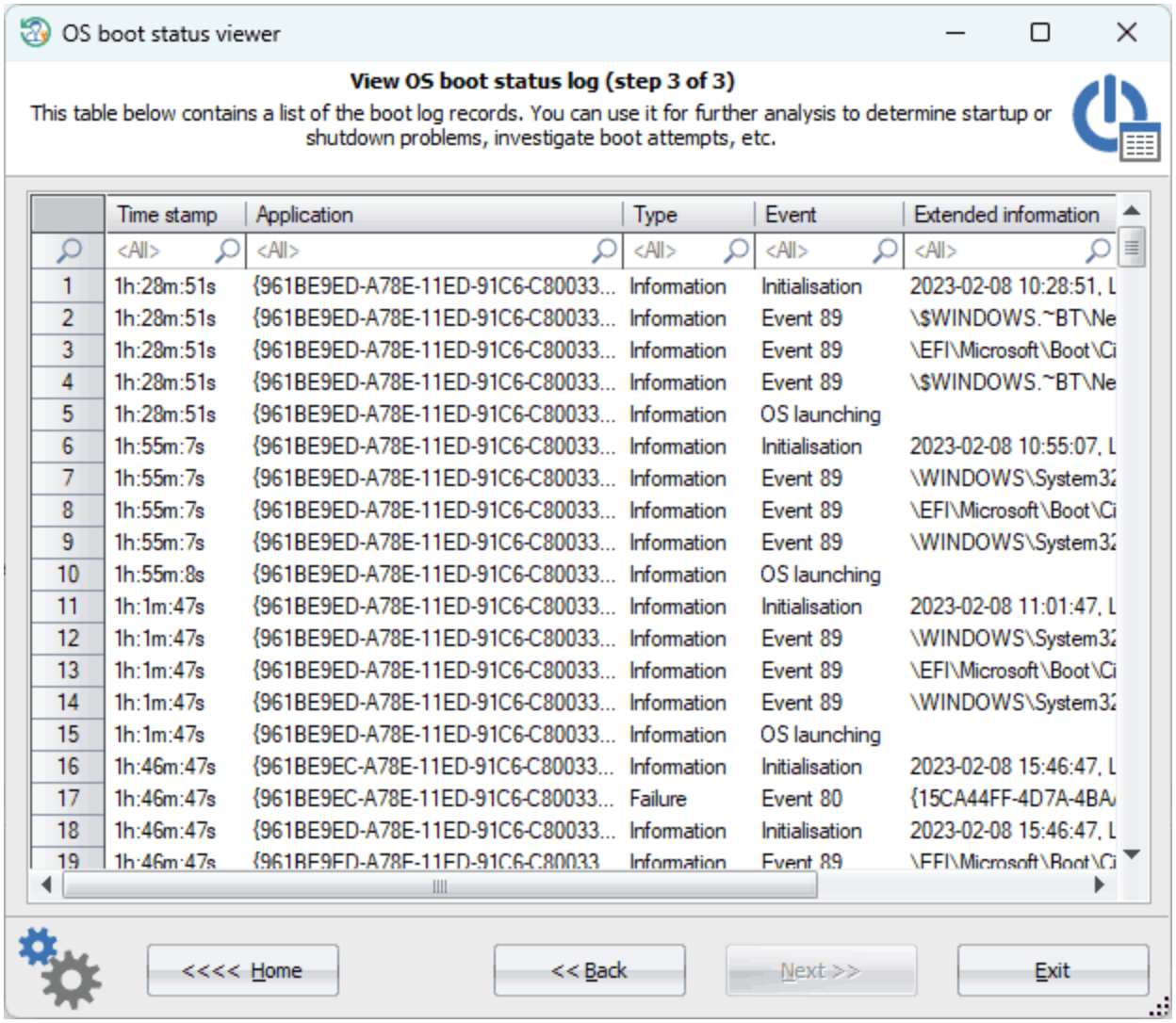
Это может быть важно, когда необходимо определить причину любых ошибок загрузки ОС, таких как непредвиденный сбой или неожиданное завершение работы. Если Windows не запускается должным образом, данный инструмент можно использовать для определения причины сбоя и обеспечению путей по устранению проблемы.

Выбор файла bootstat.dat



Файл bootstat.dat находится либо в каталоге Windows, либо в загрузочном разделе EFI, обычно в скрытом разделе Windows. Если обнаружены скрытые разделы, программа автоматически предложит просканировать их на предмет ниличия bootstat.dat.

Анализ журнала загрузки Windows



Журнал состояния загрузки состоит из записей о событиях. Каждая запись описывает событие, связанное с процессом загрузки в Windows и содержит следующие поля:

- **Time stamp** - время BIOS (в секундах) с начала дня. В Windows 10 и более поздних версиях это значение может быть обрезано.
- **Application** - идентификатор исходного приложения.
- **Type** - тип записи. Например, ошибка, предупреждение или информация.
- **Event** - идентификатор события. Некоторые идентификаторы событий недокументированы.
- **Extended info** - расширенная информация о событии.

Лицензия и регистрация

4 Лицензия и регистрация

4.1 Лицензионное соглашение

==========
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.

4.2 Регистрация

Программа поставляется в трех редакциях: Light, Standard и Advanced. Подробный список всех функций по редакциям можно найти на этой странице.

Подробные инструкции о покупке программы даны на странице заказа. Интернет заказы доступны в режиме 24/7.

Через некоторое время после покупки, на указанный электронный адрес будет выслано регистрационное письмо с ссылкой на полную версию программу. При заполнении формы оплаты обязательно укажите ваше имя и фамилию и действующий e-mail адрес, иначе вы будете не в состоянии получить регистрационное письмо.

Для завершения процесса регистрации, скачайте программу по ссылке, полученной вами в регистрационном письме, и следуйте инструкциям для создания загрузочного диска.

4.3 Ограничения демонстрационной версии

Незарегистрированная версия **Reset Windows Password** показывает только первые 3 символа найденных паролей и имеет функциональные ограничения. В частности, полноценно работает только дамп хэшей и создание резервных копий паролей.

4.4 Редакции программы

Программа доступна в трех редакциях: Light, Standard и Advanced. Подробный список возможностей и отличий представлены в таблице.

Возможность	Light	Stan-dard	Advan-ced
Поддержка рабочих станций Windows NT/2000/XP/Vista/7/8/10/11	+	+	+

Возможность	Light	Stan-dard	Advan-ced
Поддержка серверных ОС Windows NT/2000/2003/2008/2012/2016/2019/2022	+	+	+
Поддержка Windows 32/64-bit	+	+	+
Поддержка Русской Windows	+	+	+
Поддержка паролей в национальных кодировках	+	+	+
Расширенные набор драйверов IDE/SATA/SCSI/RAID	+	+	+
Обнаружение и поддержка нескольких Операционных Систем	+	+	+
Extended download warranty	+	+	+
14-дневный возврат денег	+	+	+
Использование в бизнесе, корпоративных государственных учреждениях	-	-	+
Лицензия	**персональная**	**персональная**	**бизнес**
Поддержка всех типов учетных записей Windows, включая Live ID, Microsoft account и т.д.	+	+	+
Создание загрузочного CD/DVD для сброса пароля	+	+	+
Создание загрузочного USB для сброса пароля	+	+	+
Создание загрузочного HDD для сброса пароля	+	+	+
Поддержка UEFI	+	+	+
Поддержка сети, обозреватель Интернет	+	+	+
Простейшие утилиты для работы с диском	+	+	+
Сброс пароля локального Администратора	+	+	+
Изменение пароля локального Администратора	+	+	+
Включение, разблокировка, включение просроченного пароля локального Администратора (1)	+	+	+
Сброс пароля Администратора домена	-	-	+
Изменение пароля Администратора домена	-	-	+
Включение, разблокировка, включение просроченного пароля Администратора домена (1)	-	-	+
Редактирование свойств учетной записи SAM	+	+	+
Редактирование свойств учетной записи Active Directory	-	-	+
Сброс пароля обычной (SAM) учетной записи	+	+	+
Изменение пароля обычной (SAM) учетной записи	+	+	+
Включение, разблокировка, включение просроченного пароля учетной записи SAM (1)	+	+	+
Расшифровка секретных вопросов и ответов Windows 10	+	+	+
Сброс пароля учетной записи пользователя Active Directory	-	-	+
Изменение пароля учетной записи пользователя Active Directory	-	-	+
Включение, разблокировка, включение просроченного пароля учетной записи Active Directory (1)	-	-	+
Сброс/изменение пароля учетной записи DSRM (2)	-	-	+

Возможность	Light	Stan-dard	Advan-ced
Сброс пароля кэшированной записи домена (DCC)	-	+	+
Изменение пароля кэшированной записи домена (DCC)	-	+	+
Установка и загрузка IDE/SATA/SCSI/RAID/NVME драйверов 'на лету'	+	+	+
Откат изменений (восстановление предыдущих измененных паролей)	+	+	+
Поддержка шифрования SYSKEY	+	+	+
Поддержка шифрования SYSKEY-пароль	+	+	+
Поддержка шифрования SYSKEY-дискета	+	+	+
Поиск и вывод подсказок о паролях	+	+	+
Дамп LM/NTLM хэшей обычных пользователей (SAM)	+	+	+
Дамп хэшей истории паролей	-	+	+
Дамп кэшированных паролей домена	-	+	+
Дамп LM/NTLM хэшей учетных записей пользователей Active Directory	-	-	+
Дамп Windows PIN	+	+	+
Мгновенная расшифровка паролей некоторых учетных записей Active Directory (3)	-	-	+
Мгновенная расшифровка паролей к некоторым учетным записям пользователей SAM	-	+	+
Мгновенная расшифровка уязвимых кэшированных паролей домена	-	-	+
Поиск текстовых паролей	-	+	+
Примитивный анализ по словарю	-	+	+
Улучшенный словарный анализ (4)	-	-	+
Примитивная атака перебором для простых паролей	-	+	+
Восстановление паролей при помощи настраиваемых атак: словарной, гибридной и атаки по маске	-	+	+
Восстановление паролей при помощи Искусственного Интеллекта	-	+	+
Восстановление паролей при помощи глубокого обучения	-	+	+
Анализ последних используемых пользователем файлов	-	+	+
Анализ переписки Skype	-	+	+
Поиск и расшифровка паролей документов Microsoft Office, OpenOffice, LibreOffice, MyOffice, PDF	-	+	+
Поиск и расшифровка Индийских электронных документов Aadhaar and e-pan	-	+	+
Поиск паролей в популярных браузерах: Internet Explorer, Opera, все обозреватели на базе Chromium, Firefox и др.	-	+	+
Поиск паролей в удаленных файлах, в файле подгрузки, hiberfil.sys и др.	-	+	+
Подбор текстовых паролей при помощи Идентификационной атаки	-	+	+
Удаление хэшей истории паролей для обычных (SAM) учетных записей	-	+	+
Удаление хэшей истории паролей для пользователей Active Directory	-	+	+
Удаление кэшированных паролей домена	-	+	+
Удаление кэшированных паролей на вход Windows	-	+	+

Возможность	Light	Stan-dard	Advan-ced
Удаление пароля сохраненного во время создания Дискеты Сброса Пароля	-	+	+
Удаление подсказок о паролях	-	+	+
Обнуление SYSKEY (с полной перешифровкой паролей пользователей)	-	+	+
Поиск стартового пароля SYSKEY	-	+	+
Мгновенная расшифровка паролей учетных записей с установленным графическим паролем	-	+	+
Мгновенная расшифровка паролей учетных записей со входом при помощи отпечатков пальцев (5)	-	+	+
Восстановление PIN	-	+	+
Расшифровка ранее использованных PIN (8)	-	+	+
Менеджер файлов	-	+	+
Создание виртуальных дисков из файлов-образов	-	+	+
Обозреватель скрытых томов и разделов	+	+	+
Подключение сетевых дисков	+	+	+
Обозреватель баз данных ESE (6)	-	-	+
Автоматическое обнаружение и подключение виртуальных операционных систем	+	+	+
Поиск паролей виртуальных машин	-	+	+
Поиск регистрационных ключей и серийных номеров	-	+	+
Изменение типа уч. записи с Microsoft Live ID на локальную	+	+	+
Резервное копирование паролей, реестра Windows и Active Directory	+	+	+
Поиск и расшифровка паролей интернет-браузеров	-	+	+
Поиск и расшифровка паролей почтовых клиентов	-	+	+
Поиск и расшифровка сетевых паролей	-	+	+
Поиск и расшифровка беспроводных паролей	-	+	+
Создание новой учетной записи SAM	-	+	+
Расшифровка дисков зашифрованных Bitlocker	+	+	+
Поиск паролей Bitlocker, хранимых в Active Directory	-	-	+
Изменение параметров входа в систему	-	+	+
Редактор локальной политики паролей	-	+	+
Редактор политики паролей домена	-	-	+
Редактор настроек входа в систему	-	+	+
Редактор ограничений интерфейса и системы	-	+	+
Поддержка беспарольного входа в систему	+	+	+
Расшифровка биометрических паролей	-	+	+
Расшифровка паролей Windows Hello (8)	-	+	+
Статистика учетных записей (6)	+	+	+
История оборудования (7)	+	+	+
История установок ПО (7)	+	+	+

Возможность	Light	Stan-dard	Advan-ced
История сетевых соединений (7)	+	+	+
Последняя активность пользователя (6)	+	+	+
Поиск последних открываемых документов (7)	+	+	+
Временная шкала выполнения программ (7)	+	+	+
Системные события Windows (6)	+	+	+
Анализ закачек Telegram (6)	+	+	+
Расшифровка пароля Telegram	-	-	+
Расшифровка локальных файлов Telegram	-	-	+
История Интернет (6)	+	+	+
История IP адресов пользователей (6)	+	+	+
Последние измененные файлы	-	+	+
Последние измененные папки	-	+	+
Записки Windows (6)	+	+	+
Доступ к камере и микрофону (6)	+	+	+
Временная шкала активности Windows (6)	+	+	+
История буфера обмена (6)	+	+	+
История USB (6)	+	+	+
История корзины (6)	+	+	+
Анализ истории удаленного рабочего стола (6)	+	+	+
Windows media: анализ изображений	-	-	+
Windows media: анализ видеофайлов	-	-	+
Windows media: действия пользователя	-	-	+
Windows Photos: анализ изображений и видео	-	-	+
Windows Photos: действия пользователя	-	-	+
Media Player: анализ элементов	-	-	+
Media Player: действия пользователя	-	-	+
Монитор использования системных ресурсов (6)	-	-	+
Обозреватель баз данных Windows Search (6)	-	-	+
Обозреватель баз данных SQLite (6)	-	-	+
Журнал состояния загрузки ОС (6)	-	-	+
Калькулятор контрольной суммы или хэша (7)	-	+	+
Поиск дубликатов файлов (7)	-	+	+
Анализ свободного места на диске (6)	-	-	+
Анализ типов файлов (6)	-	-	+
Удаление ненужных файлов и очистка реестра	-	+	+
Быстрый поиск на диске (7)	+	+	+
Пароль доступа к программе	+	+	+
Создание образов дисков в формате *.RAW и *.ZIP	+	+	+

Возможность	Light	Stan-dard	Advan-ced
Создание образов дисков в формате *.E01	-	+	+

Пояснения:
(1) Если учетная запись заблокирована, отключена или истек срок действия пароля
(2) Directory Services Restore Mode
(3) Если в системе была установлена опция обратного шифрования. Данная опция находится в политике управления паролями домена.
(4) Используются простые мутации и следующие словари: Английский, Арабский, Испанский, Китайский, Немецкий, Португальский, Русский, Французский.
(5) Поддерживаются не все учетные записи.
(6) Все функции контекстного меню доступны только в редакции Advanced
(7) Все функции контекстного меню доступны только в Standard и Advanced редакциях
(8) Если не установлена дополнительная защита TPM

Техническая поддержка

5 Техническая поддержка

5.1 Ошибки и проблемы

Если вы обнаружили ошибку в работе программы, напишите письмо на support@passcape.com. Пожалуйста, укажите следующую информацию:

- Полное имя и версия программы
- Версия Windows, включая сервиспаки
- Регистрационная информация, если есть
- Подробное описание проблемы или ошибки, является ли проблема повторяющейся или спонтанной
- Если это возможно, вышлите скриншот, лог программы и файл **RWPCrash.log**, если имеется.

5.2 Предложения

Если у вас имеются вопросы, комментарии или предложения по работе программы, присылайте их на адрес info@passcape.com. Пожалуйста, не забудьте упомянуть полное название программы и ее версию. Убедитесь также, что у вас установлена последняя версия.

5.3 Контакты

Вопросы по работе программы присылайте только после прочтения FAQ. Адрес тех. поддержки: support@passcape.com.
Мы ответим вам в течение одного-двух дней. Зарегистрированные пользователи имеют приоритет в технической поддержке.

По вопросам регистрации обращайтесь, пожалуйста, по следующему адресу: sales@passcape.com

Пишите на русском или английском языке!