



Elcomsoft System Recovery

Версия 8.30

Elcomsoft System Recovery (ESR) помогает экспертам-криминалистам получить доступ к защищённым учётным записям и зашифрованным томам. Создаёт портативные загрузочные устройства. Идеальный инструмент для быстрого извлечения улик при работе на выезде.

Краткий обзор

В обновлении Elcomsoft System Recovery 8.30 появилась возможность восстанавливать PIN-коды к учётным записям Windows 10 и Windows 11 на компьютерах, не оборудованных TPM. Кроме того, улучшена работа загрузочного криминалистического инструментария, добавлено определение шифрования LUKS2 и учётных записей Microsoft Azure.

Важные изменения

Учётные записи с PIN-кодом

В новой версии Elcomsoft System Recovery представлена возможность восстановления PIN-кодов к учётным записям Windows 10 и Windows 11 на компьютерах, не оборудованных модулем безопасности TPM или его эмулятором. Microsoft рекомендует использовать PIN-коды вместо паролей в системах, для входа в которые используются учётные данные Microsoft Account. В то же время параметры PIN-кодов по умолчанию (только цифры, 4 или 6 знаков) открывают возможность перебора всего пространства паролей за считанные минуты. В Elcomsoft System Recovery 8.30 добавлена возможность как перебора цифровых PIN-кодов средствами самого приложения, так и извлечения метаданных для последующей атаки на буквенно-цифровые PIN-коды в Elcomsoft Distributed Password Recovery (требуется обновление).



Фильтры в криминалистическом инструментарии

В обновлении Elcomsoft System Recovery улучшена работа инструментария для поиска цифровых улик в процессе анализа компьютеров в полевых условиях. Ранее доступные функции инструментария для просмотра списка установленных в системе приложений и анализа действий пользователей на компьютере с привязкой к временной шкале теперь поддерживают фильтры, позволяющие исключить из выдачи не относящиеся к расследованию данные. Так, попытка узнать, к каким файлам и папкам пользователь обращался в заданном промежутке времени может выдать тысячи результатов, подавляющая часть которых относится к обращениям к системным файлам Windows. Включение фильтра позволяет исключить системные файлы из выдачи, позволив эксперту сфокусироваться на действительно важных данных.



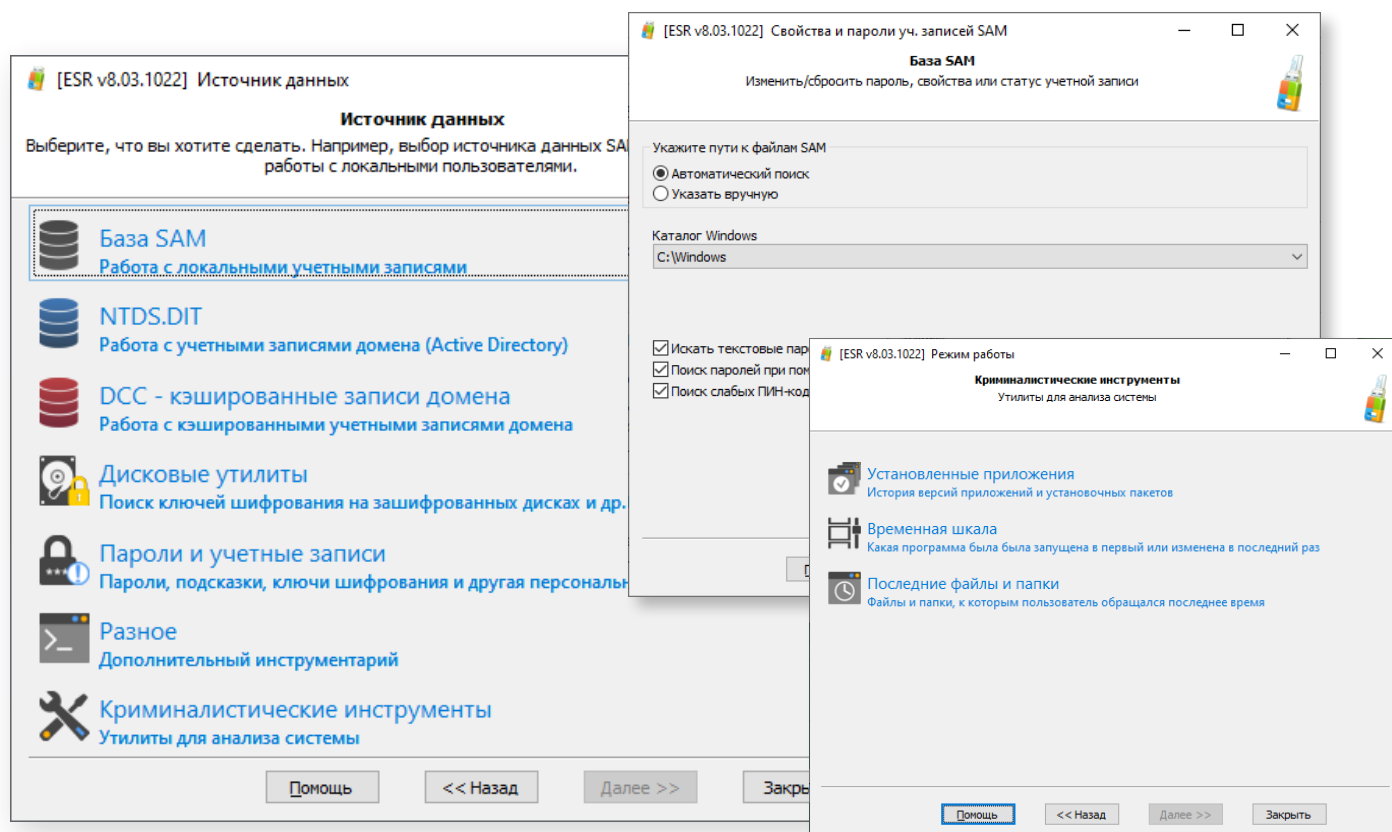
Детектирование LUKS2 и Microsoft Azure

Кроме того, в новой версии Elcomsoft System Recovery добавлено детектирование шифрования дисков в новом формате LUKS2 с извлечением метаданных для последующей атаки в Elcomsoft Distributed Password Recovery (требуется обновление); также добавлено определение учётных записей Microsoft Azure.



Список всех изменений в ESR 8.30

- Учётные записи Azure Active Directory:
 - ⌘ Определение и отображение учётных записей
- Учётные записи с PIN-кодом (локальные, локальные Microsoft, Azure Active Directory):
 - ⌘ Перебор простых PIN-кодов (до 6 цифр)
 - ⌘ Извлечение данных для последующего перебора в Elcomsoft Distributed Password Recovery (требуется обновление)
- Шифрование дисков LUKS2:
 - ⌘ Определение зашифрованных дисков
 - ⌘ Извлечение данных для последующего перебора в Elcomsoft Distributed Password Recovery (требуется обновление)
- Добавлены фильтры для раздела Криминалистические инструменты (Установленные приложения, Временная шкала, Последние файлы и папки)



Как обновить продукт

1. Всем активным пользователям инструмента Elcomsoft System Recovery предлагается загрузить новую версию продукта, введя действующий регистрационный ключ в онлайн-форме <https://www.elcomsoft.ru/key.html>.
2. Пользователи, у которых истёк срок действия лицензии продукта, могут продлить свою лицензию по соответствующей цене, которую можно узнать, введя регистрационный ключ в онлайн-форме (<https://www.elcomsoft.ru/key.html>).

Свяжитесь с нами по электронной почте sales@elcomsoft.com для получения более подробной информации по обновлению или продлению лицензии.

