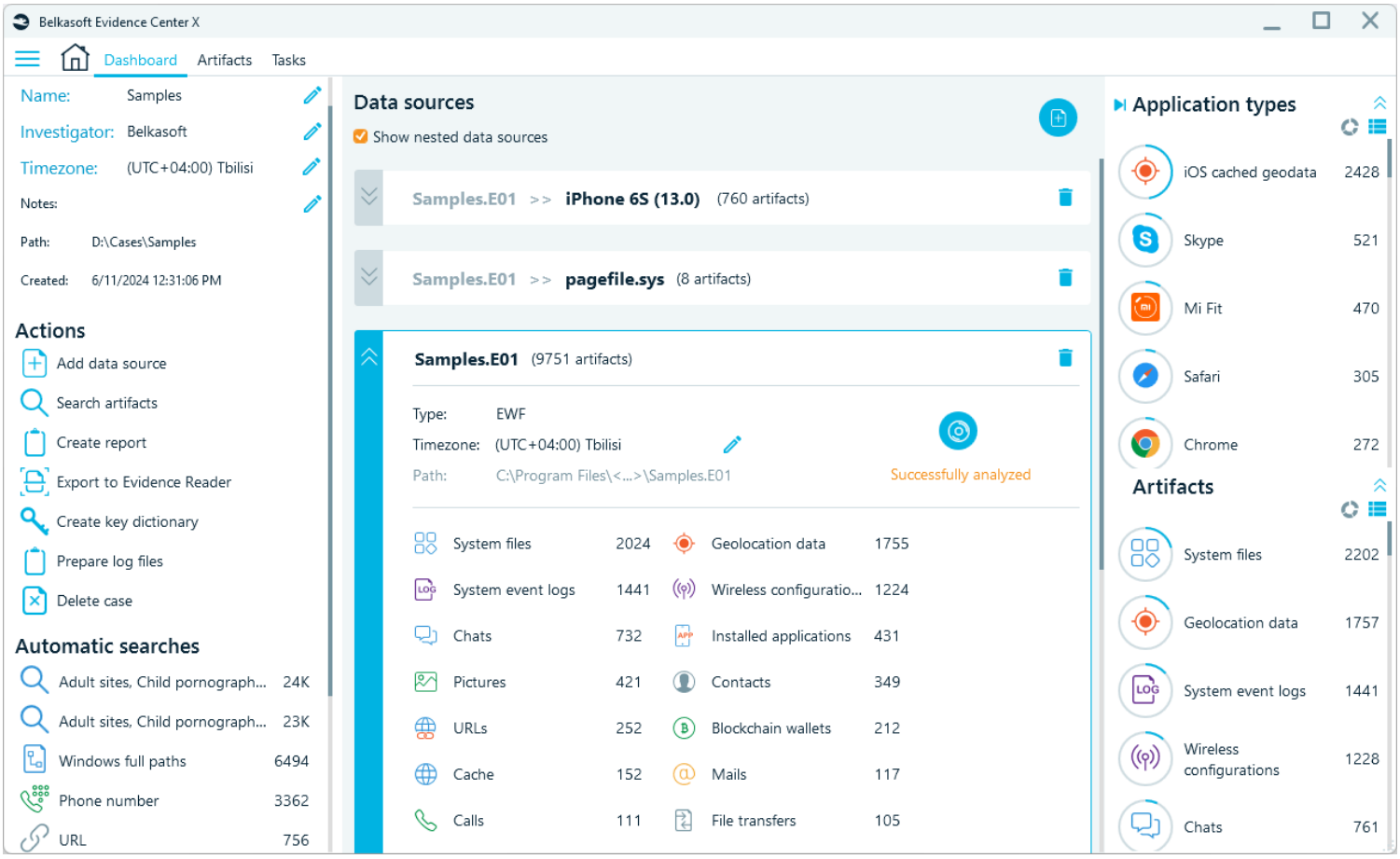
Почему стоит выбрать Belkasoft X для цифровой криминалистики и реагирования на кибер-инциденты?

Belkasoft X — это универсальный программный инструмент для цифровой криминалистики и расследования киберпреступлений, используемый правоохранительными органами, государственными органами и специалистами по корпоративной безопасности по всему миру. Что делает его комплексным и надежным выбором для задач цифровой криминалистики и расследования киберпреступлений?

В этой статье мы подробно рассмотрим каждую из этих функций, демонстрируя мощные возможности, заложенные в продукте.

Простой интерфейс

Belkasoft X обладает интуитивно понятным пользовательским интерфейсом. Благодаря тщательно продуманному и удобному дизайну, вы можете начать работать с ним сразу после установки, минуя недели платного обучения, которые требуются для эффективной работы с продуктами конкурентов.



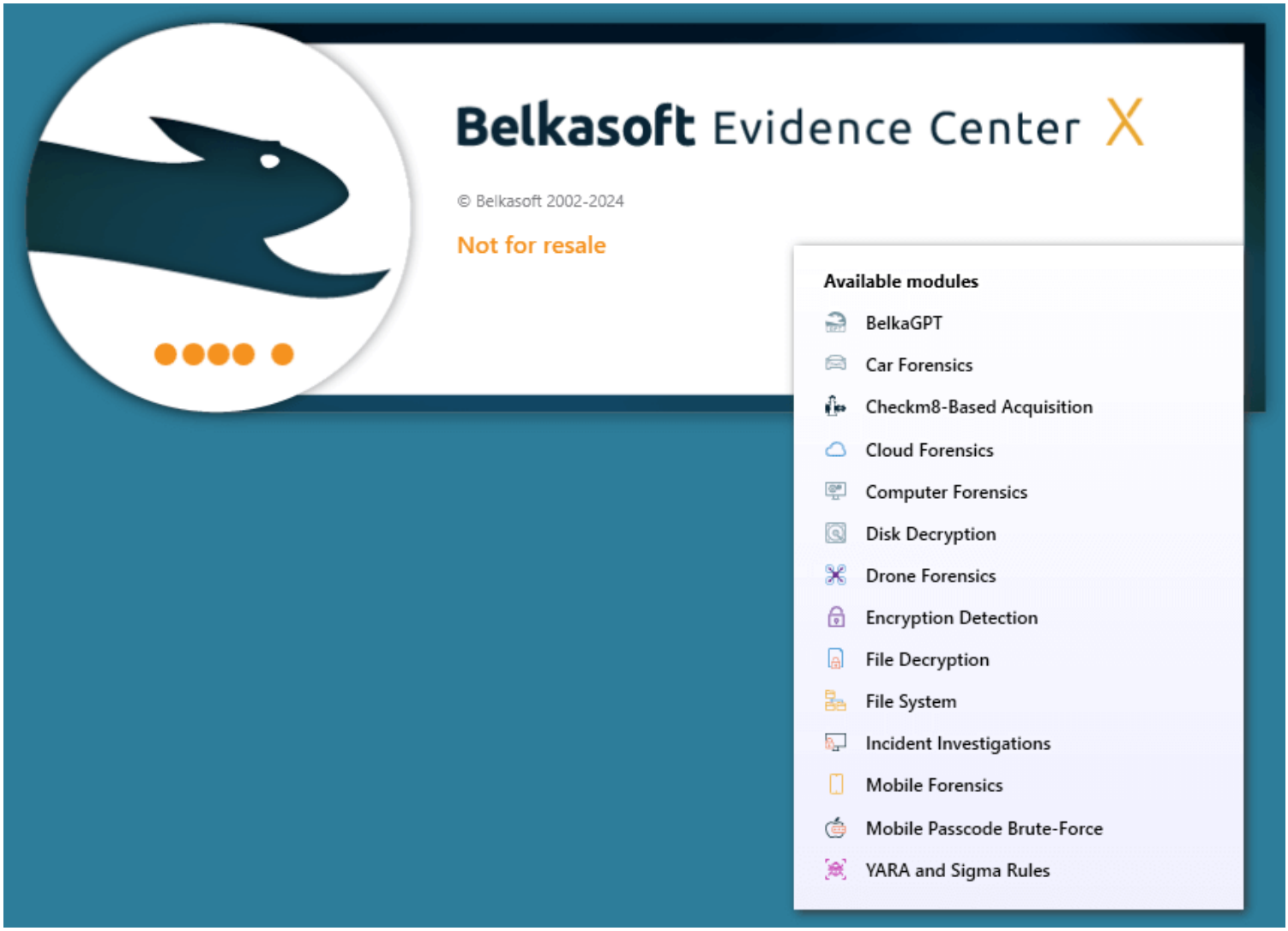
Интерфейс Belkasoft X предоставляет доступ к извлеченным артефактам и задачам расследования в любое время и в любом месте.

В комплект продукта также входят обучающие видеоролики и пошаговые инструкции, которые помогут вам начать работу с функциями инструмента или быстро ввести в курс дела новых членов команды; однако для более глубокого понимания функциональности продукта мы рекомендуем пройти обучение в Belkasoft.

ВЫБЕРИТЕ ВАШ ОФЛАЙН ИЛИ ПО ЗАПРОСУ КУРС ПО DFIR ОТ BELKASOFT

Универсальный инструмент

Belkasoft X поддерживает компьютерную, мобильную , беспилотную, автомобильную и облачную криминалистику — все в одном продукте. Такой подход позволяет специалистам по цифровой криминалистике собирать и анализировать все устройства и источники данных, имеющие отношение к расследованию, в рамках одного дела и проводить их всестороннее изучение .



Belkasoft X объединяет несколько модулей для проведения комплексных расследований в области цифровой криминалистики и разведки.

Belkasoft X может анализировать данные из различных источников:

- Физические и логические диски, а также образы дисков.
- Дампы памяти
- Дампы JTAG и чип-оффа
- Резервные копии мобильных устройств (включая резервные копии iTunes и ADB, а также Xiaomi MIUI и Huawei HiSuite).
- Образы файловой системы мобильных устройств
- Виртуальные машины (например, VMWare, VirtualBox, Microsoft VirtualPC)
- Данные с беспилотников (включая DJI, Parrot, Skydio, Yuneec и другие)

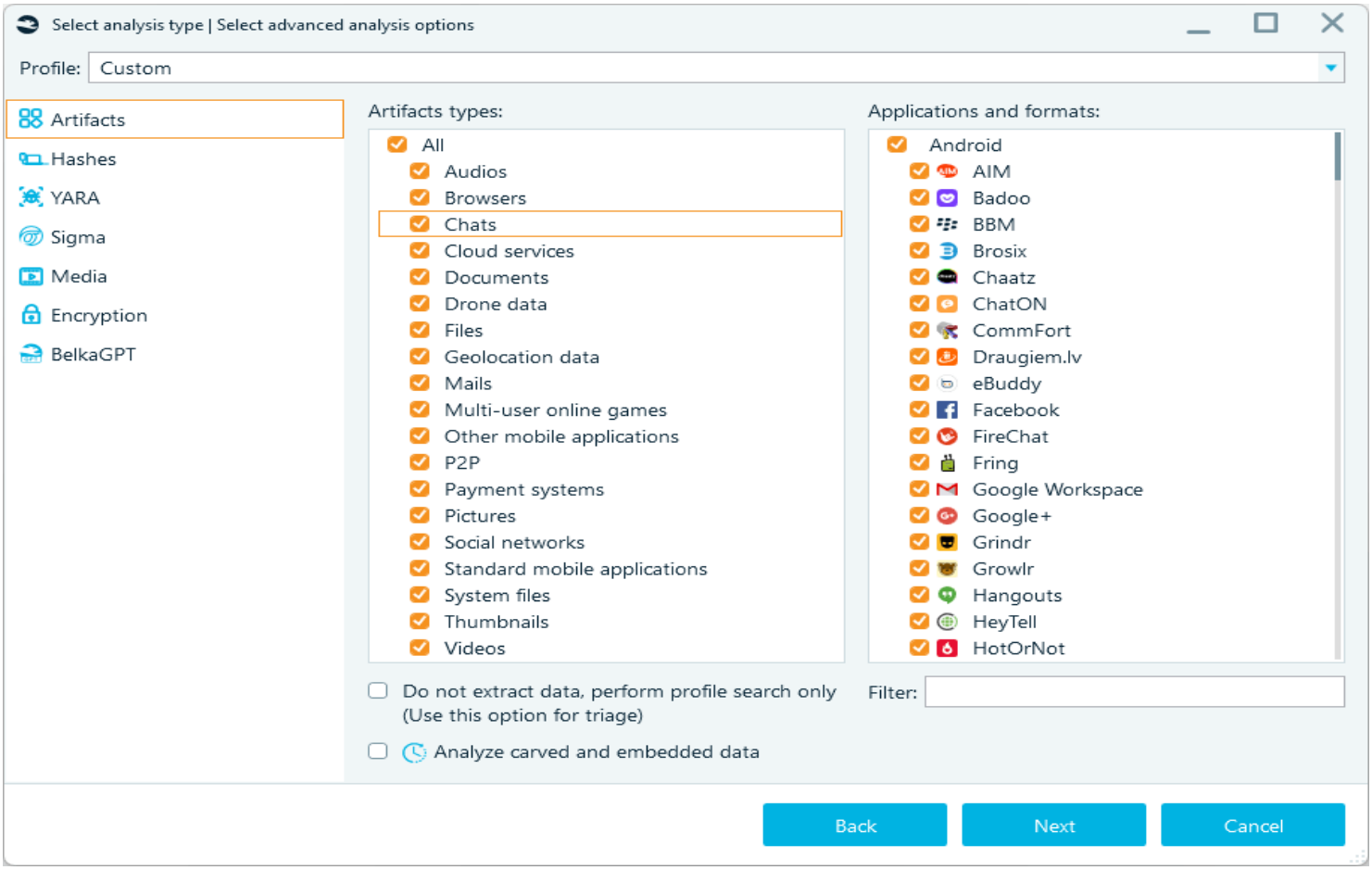
Кроме того, он поддерживает форматы изображений, созданные в других инструментах, таких как Cellebrite UFED, GrayKey, Magnet Forensics, Exterro FTK (Forensic Toolkit), OpenText EnCase, X-Ways, Oxygen Forensics, Elcomsoft и Berla.

Легкая и доступная криминалистика

Belkasoft X обнаруживает и анализирует более 1500 типов артефактов «из коробки». Автоматическое извлечение данных приложения, известное как «легкодоступные улики в цифровой криминалистике», часто оказывается достаточным для обнаружения ключевых доказательств в большинстве расследований.

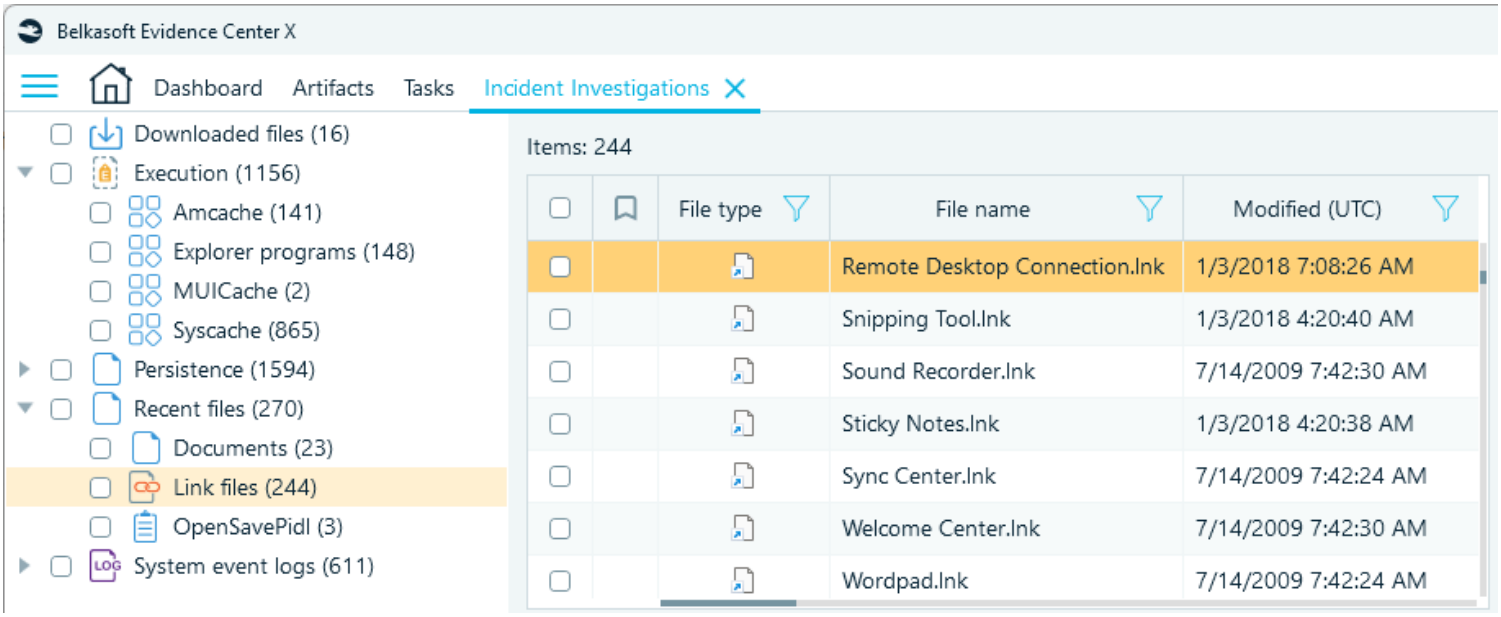
Благодаря обширной базе данных артефактов Belkasoft X вам не нужно знать все форматы данных, расположение файлов, схемы шифрования или подписи для извлечения файлов и отдельных записей. Продукт поддерживает:

- Популярные (и менее известные) мессенджеры, используемые по всему миру: WhatsApp , Telegram , WeChat, Signal , Kakao Talk, Kik, Line, Skype, Slack, Snapchat, Viber и другие.
- Социальные сети: Facebook, Instagram, LinkedIn, Twitter, TikTok, VK и др.
- Приложения для знакомств: Tinder, Badoo, Grindr и т. д.
- Основные браузеры: Chrome, Edge, Firefox, Opera, Onion, Safari, Tor и другие.
- Почтовые приложения: Outlook, Gmail, Yahoo и другие.
- Облачные и резервные сервисы: Carbonite, DropBox, Google Drive и другие.
- Стандартные приложения для Android и iOS: Контакты, Звонки, SMS, Календарь, Заметки и другие.
- Множество системных файлов Android и системных артефактов iOS , включая knowledgeC и Biome.
- Криптовалютные кошельки и многое другое



Belkasoft X позволяет выбирать типы артефактов, а также конкретные приложения и форматы для извлечения в процессе анализа.

Belkasoft X также извлекает множество артефактов, специфичных для реагирования на кибер-инциденты. Они помогают быстро отслеживать вредоносные файлы или выявлять механизмы горизонтального перемещения и закрепления при расследовании киберугроз.



Окно «Расследование инцидентов» — это удобный интерфейс для изучения материалов, связанных с реагированием на инциденты.

Всесторонняя поддержка задач цифровой разведки и реагирования на инциденты (DFIR).

Belkasoft X облегчает каждый этап вашего расследования, от сбора и анализа данных до составления отчетов и обмена доказательствами.

На этапе приобретения компания Belkasoft X поможет вам:

- Копирование жестких дисков
- Создание дампов мобильных устройств
- Получите содержимое SIM-карты
- Захват оперативной памяти (энергонезависимой памяти)
- Загрузите Google Диск и iCloud.
- Получайте доступ к данным облачных приложений , таких как Instagram, WhatsApp, Telegram и других.

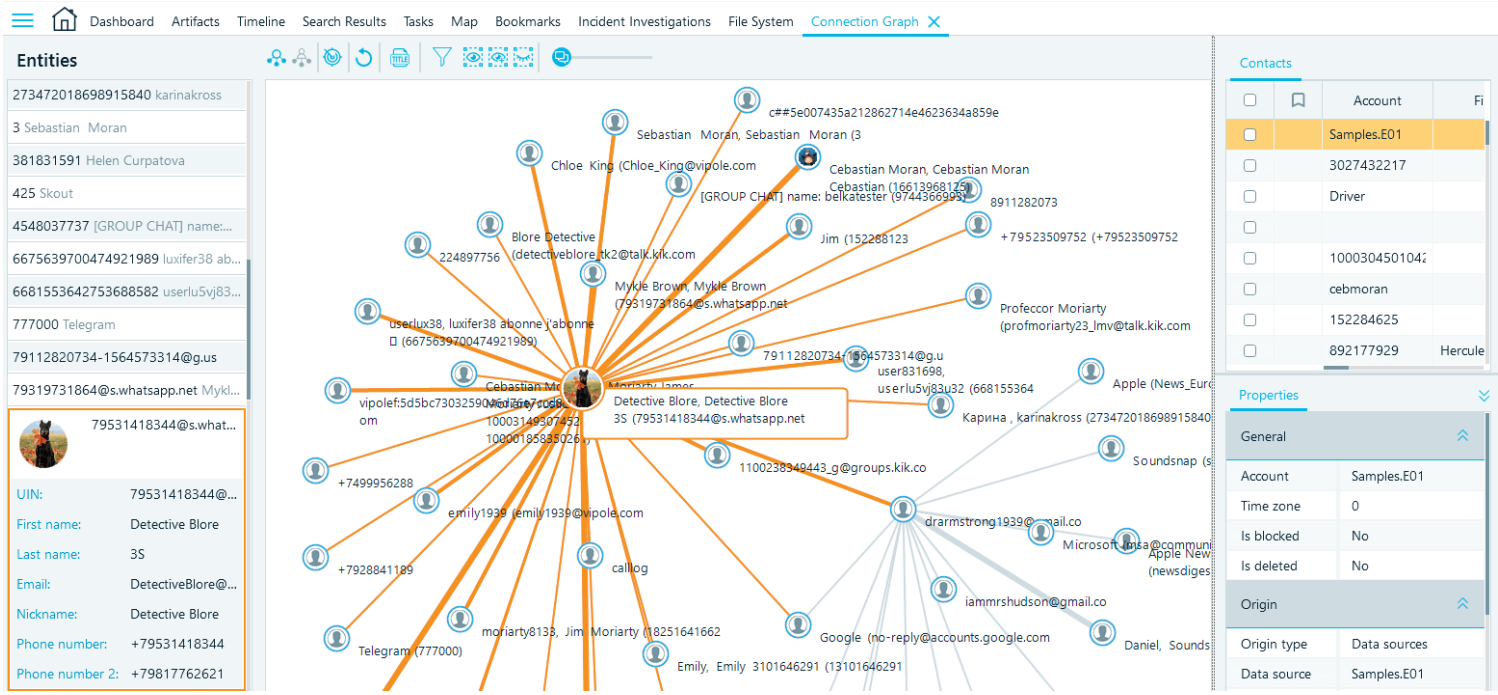
При анализе источников данных инструмент ищет артефакты не только в доступных файлах. Он исследует все потенциальные места их нахождения, такие как:

- Загруженная оперативная память
- Файл подкачки и hiberfil.sys
- Вложенные источники данных (виртуальные машины, резервные копии смартфонов и файлы гибернации)

- Снимки VCS (теневых копий томов)
- Нераспределенное и свободное пространство

Belkasoft X поддерживает обнаружение зашифрованных файлов и подбор паролей методом перебора, помогая взламывать как файловые, так и дисковые системы шифрования .

Мощные возможности поиска и аналитические функции продукта, такие как граф связей , временная шкала и анализ хэш-множеств , упрощают задачи исследования и позволяют быстро находить важные факты.

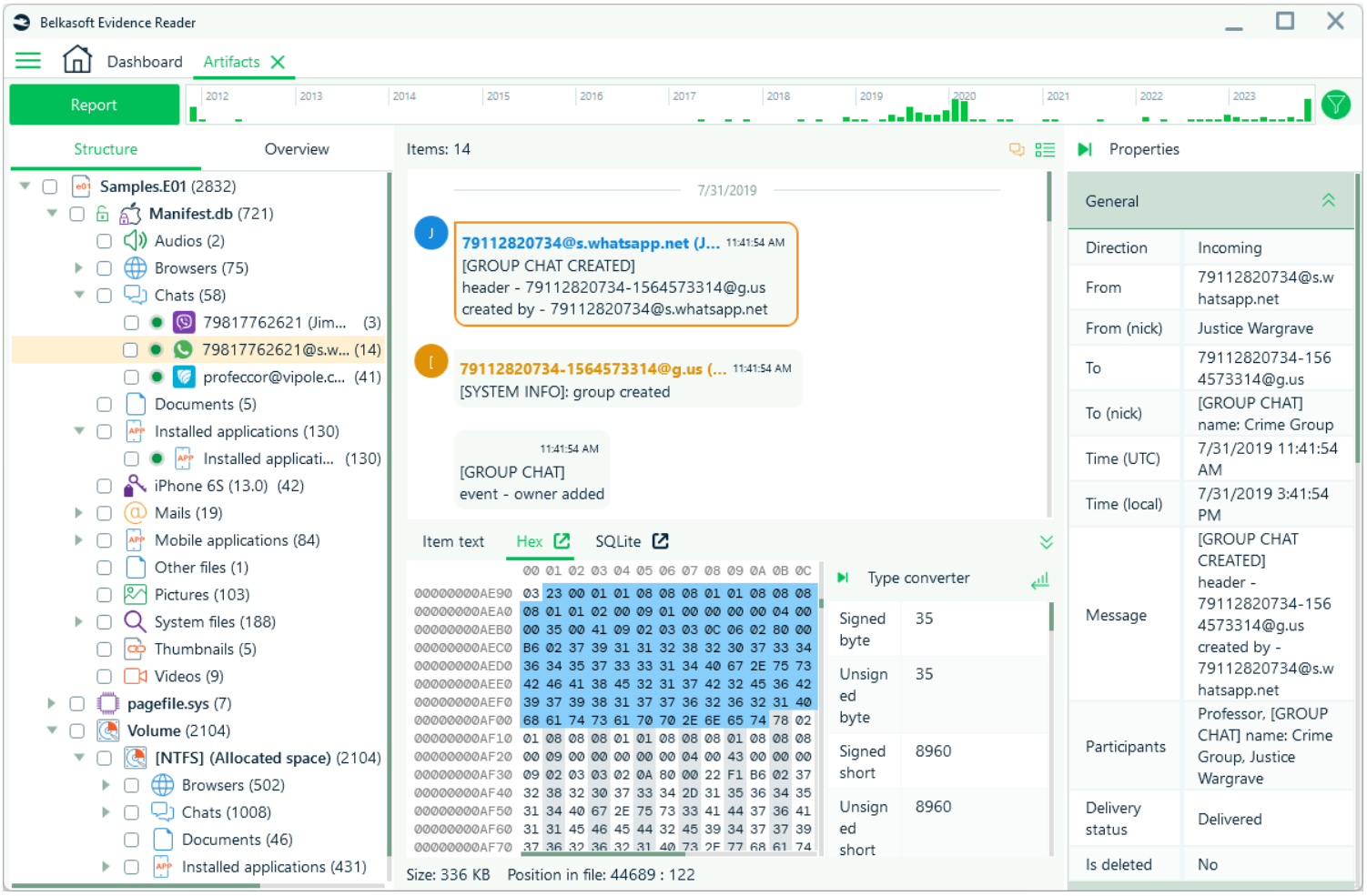


Граф связей помогает визуализировать общение между лицами, участвующими в деле.

Встроенная поддержка правил YARA и Sigma облегчает поиск следов вредоносного ПО.

Что касается документирования ваших результатов, Belkasoft X предоставляет удобные инструменты для создания упорядоченных закладок для артефактов и генерации отчетов в различных форматах, включая текст, HTML, XML, CSV, PDF, RTF, Excel, Word, EML, KML, ProjectVIC JSON, Semantics21 и другие.

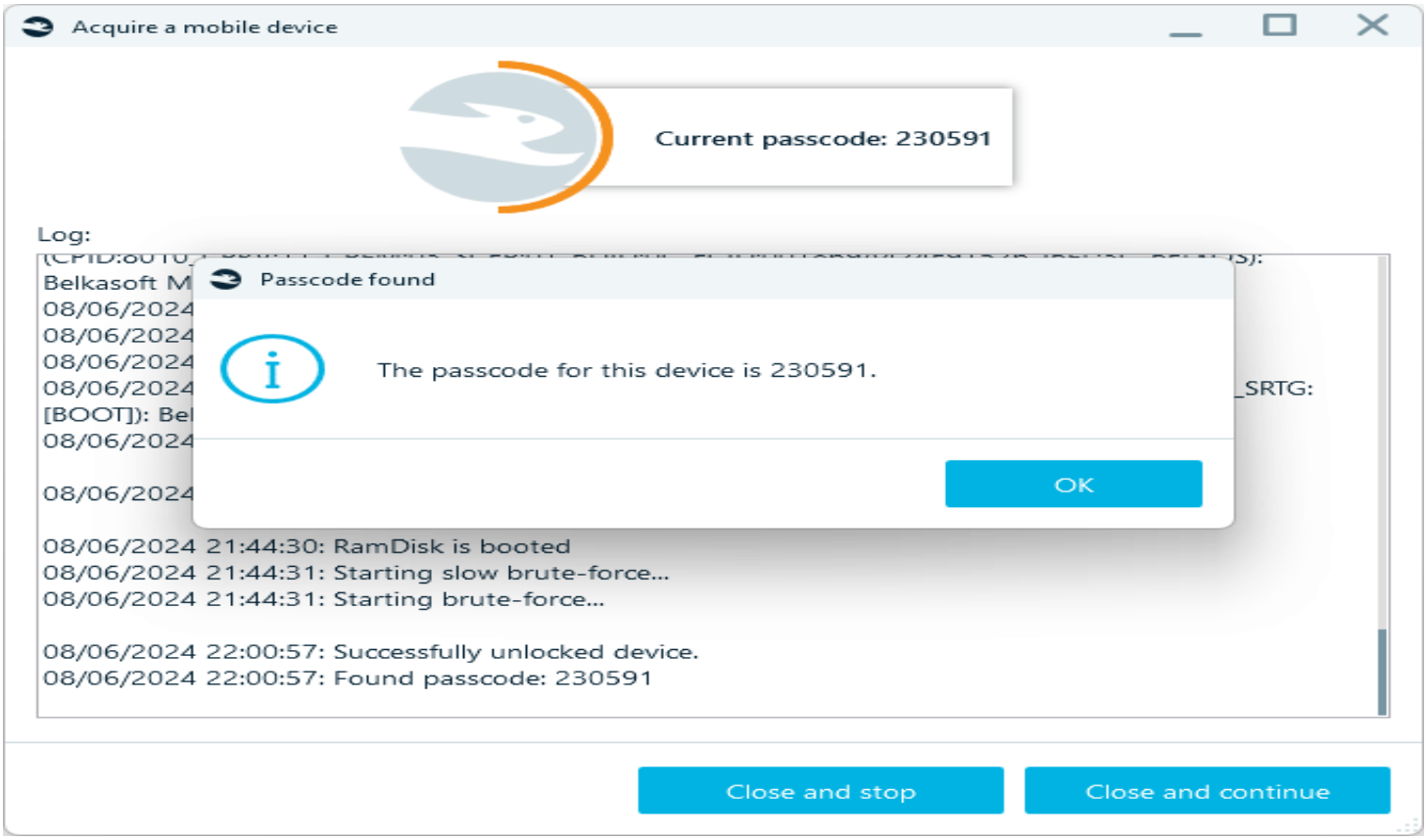
Бесплатная программа Evidence Reader , входящая в состав инструмента, позволяет создать портативную копию полученных данных и поделиться ими с другими следователями в удобном интерфейсе Belkasoft:



Программа Evidence Reader может отображать все экспортированные данные по вашему делу в режиме только для чтения — совершенно бесплатно!

Мобильные методы грубой силы и передовые методы сбора данных

В случаях, когда пароли устройства неизвестны, Belkasoft X предлагает модуль Mobile Passcode Brute-Force , который помогает разблокировать определенные модели устройств iOS и Android.



Мобильный брутфорс помогает обходить ограничения безопасности и автоматически подбирать пароли на определенных устройствах iOS и Android.

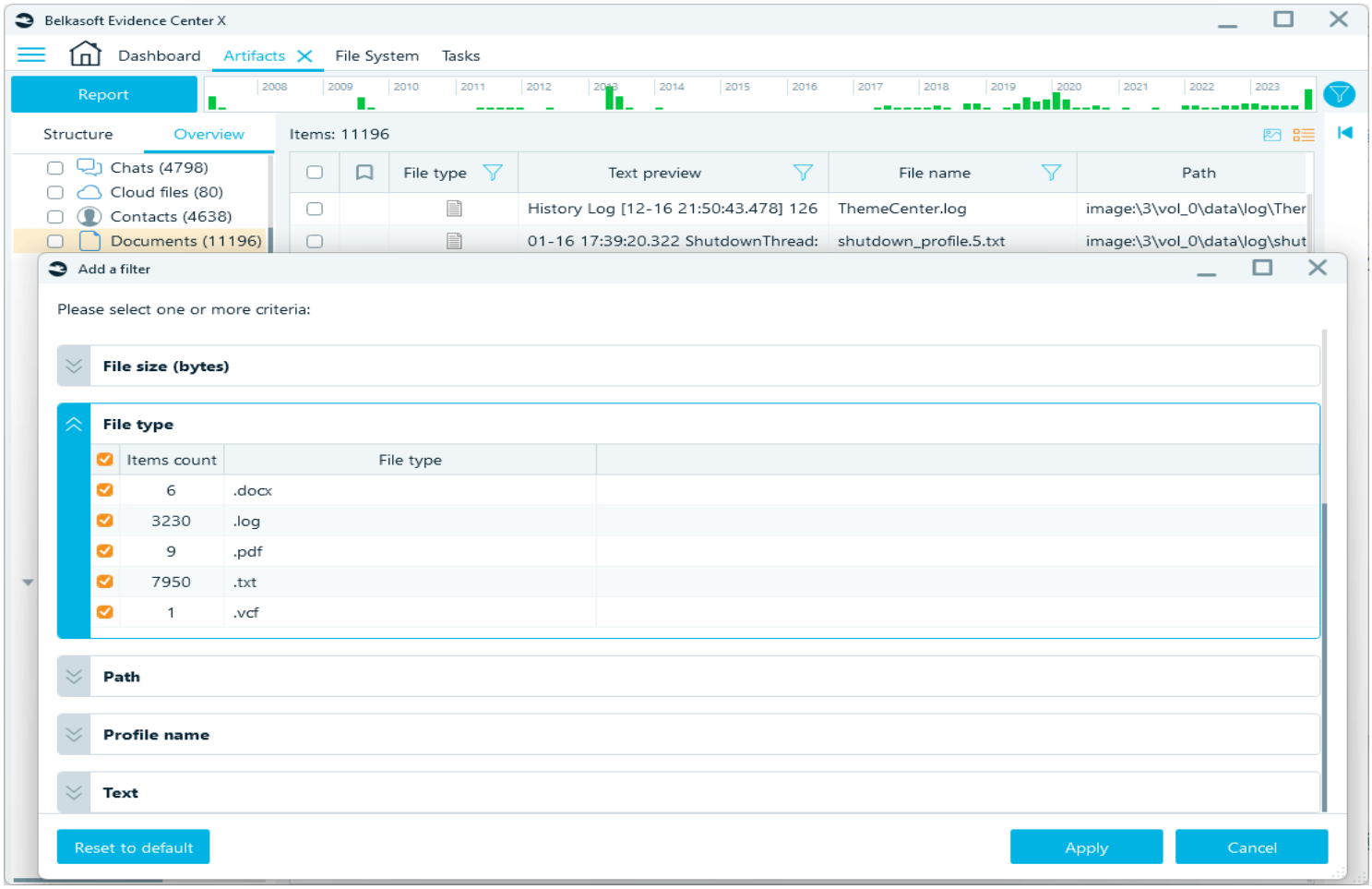
Набор инструментов для мобильной криминалистики Belkasoft X предлагает широкий спектр методов сбора данных со смартфонов и планшетов. Вы можете начать со стандартных и наиболее безопасных вариантов и постепенно перейти к более продвинутым методам, позволяющим получить больше данных.

В Belkasoft X доступны функции получения образов iOS, позволяющие копировать логические образы с помощью резервного копирования iTunes и службы Apple File Conduit (AFC), а также получать полную копию файловой системы мобильных устройств Apple с помощью таких методов, как получение образов на основе checkm8 , резервное копирование агента и образ устройства с джейлбрейком.

Методы получения образов Android предлагают различные способы копирования файлов устройства, включая резервное копирование ADB, методы на основе агентов и протоколы MTP или PTP. Вы также можете скопировать полные файловые системы рутированных устройств, получить доступ к ресурсам приложений с помощью метода понижения версии APK и использовать передовые методы на основе чипсетов для получения физических и логических образов устройств Android, работающих на чипах Kirin, MediaTek, Spreadtrum и Qualcomm. Для приложений, данные которых защищены шифрованием, можно использовать автоматизированный инструмент захвата экрана Android .

Эффективные возможности поиска и фильтрации.

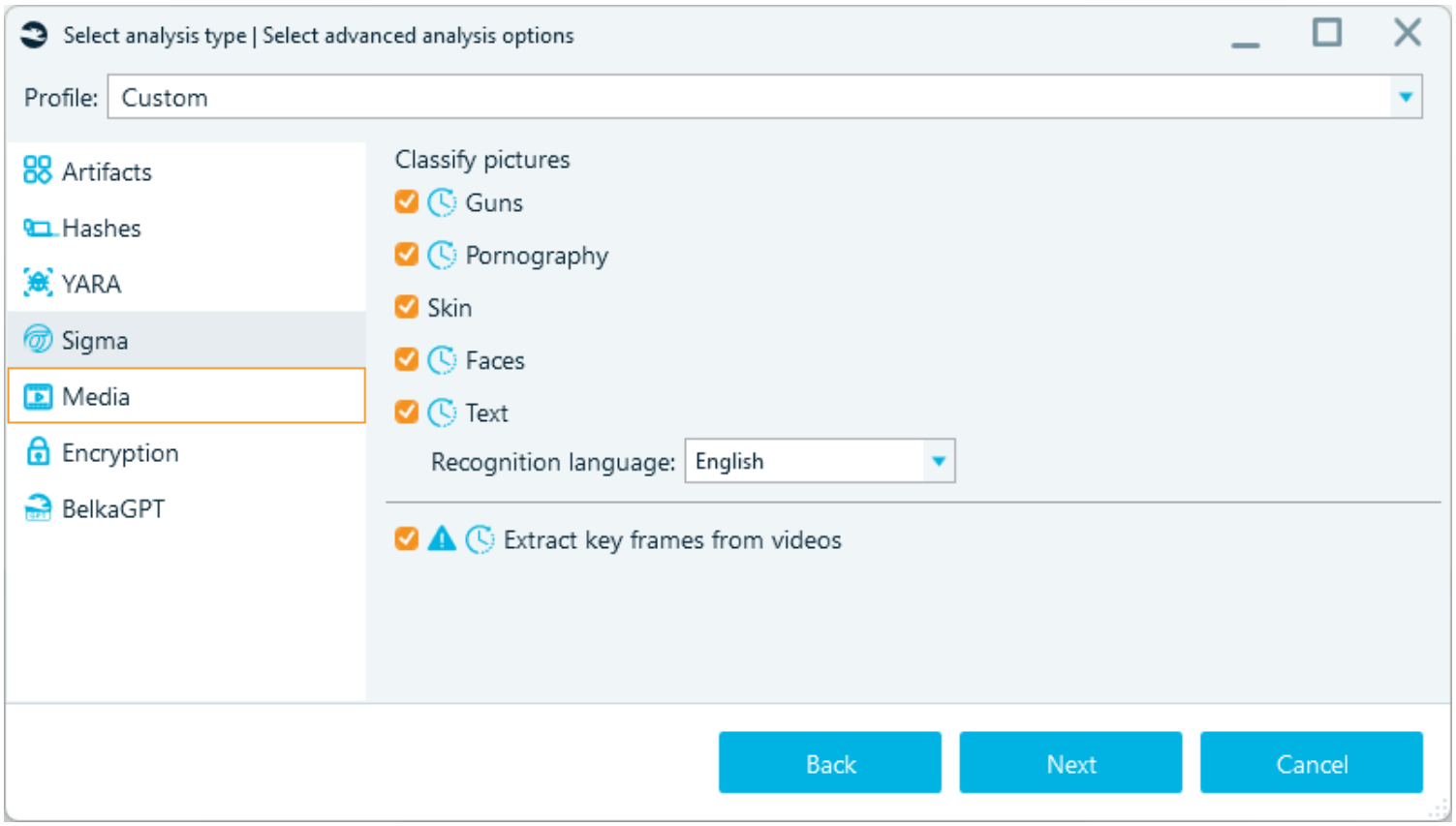
После того как Belkasoft X извлечет артефакты из вашего источника данных, вы можете выполнять текстовый поиск по всему делу с использованием специальных операторов и регулярных выражений для отслеживания определенных ключевых слов в содержимом файлов, именах и метаданных. Многочисленные параметры фильтрации позволяют мгновенно уточнять результаты поиска, артефакты по категориям и профилям или даже все данные по делу.



Функция фильтрации помогает уменьшить объем данных для анализа.

Расширенный анализ медиафайлов

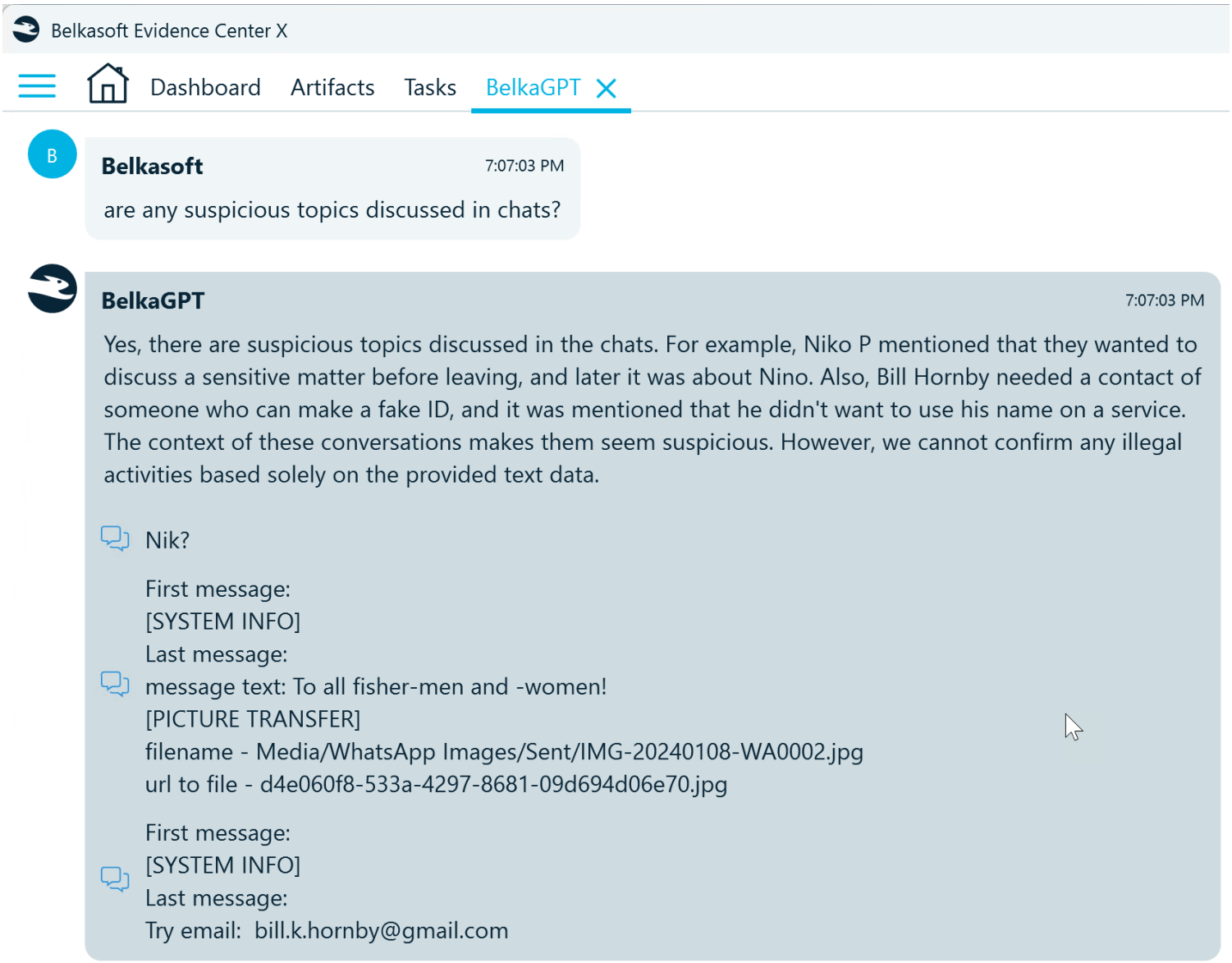
Когда дело доходит до анализа медиафайлов, ручная сортировка огромных объемов аудио, фото и видео редко бывает целесообразной. Помимо извлечения всех медиафайлов и их следов из образов устройств, Belkasoft X упрощает анализ медиафайлов , предоставляя набор инструментов для автоматического распознавания содержимого изображений и извлечения ключевых кадров видео.



Обнаружение и категоризация медиафайлов упрощают анализ изображений.

Расследования с использованием искусственного интеллекта с помощью BelkaGPT

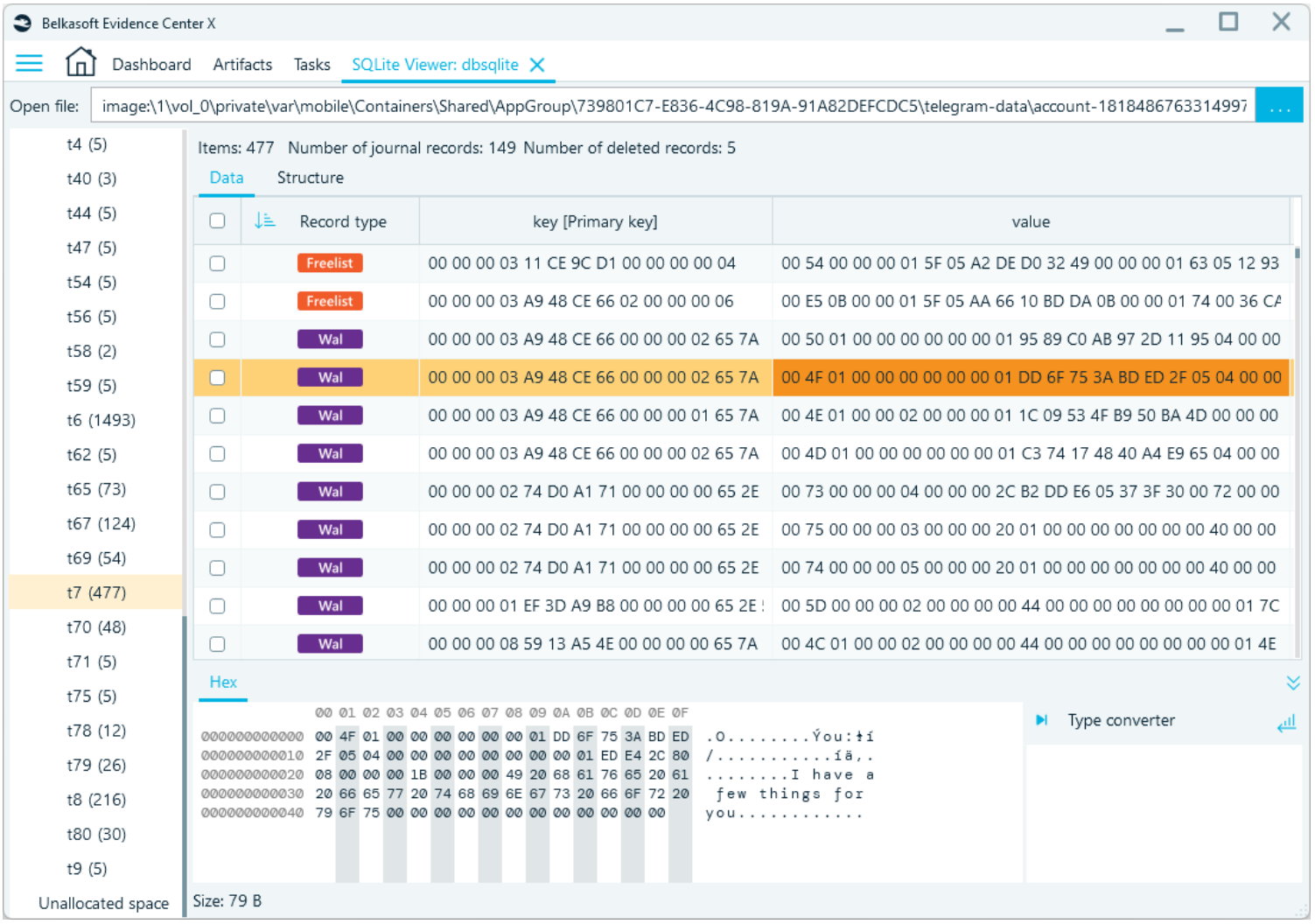
BelkaGPT выводит ваши расследования на новый уровень, используя возможности искусственного интеллекта, позволяя сэкономить часы, потраченные на изучение данных дела. ИИ-помощник Belkasoft основан на обширной языковой модели, которая обрабатывает текстовые данные из вашего дела и отвечает на вопросы по интересующим вас темам. Он работает полностью в автономном режиме и не предъявляет высоких требований к оборудованию. Вы можете безопасно и эффективно использовать его на обычной рабочей станции для цифровой криминалистики и расследований.



BelkaGPT использует интеллектуальный алгоритм обработки данных на основе искусственного интеллекта, чтобы предоставлять вам интересующую вас информацию и соответствующие материалы.

Восстановление данных в ходе судебно-криминалистической экспертизы

Благодаря настраиваемым функциям восстановления файлов и артефактов, анализу теневых копий томов и расширенным функциям анализа SQLite в Belkasoft X , вы можете восстановить максимально возможный объем данных из криминалистических образов, независимо от того, находятся ли данные в файлах, удалены или скрыты в нераспределенном или свободном пространстве.

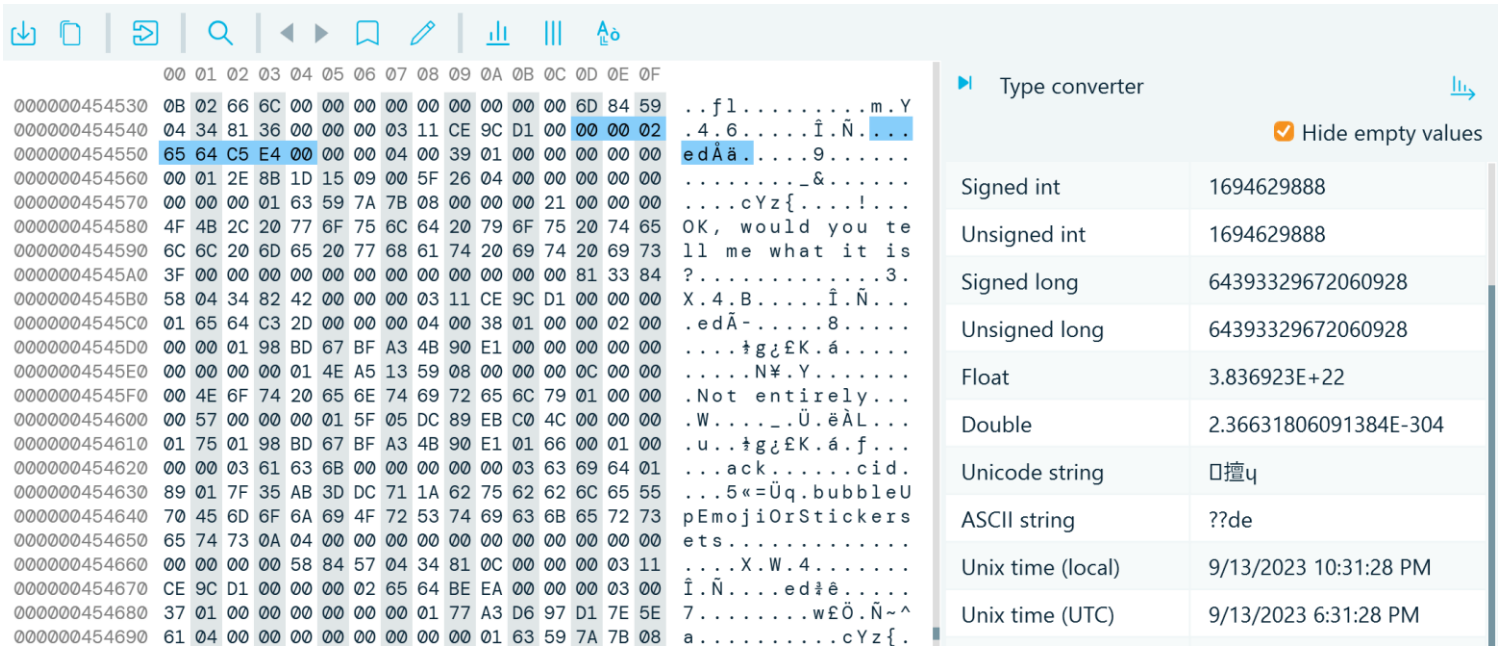


Анализ SQLite выявляет списки свободных ячеек, журнал предварительной записи, файлы журнала и нераспределенное пространство SQLite, которое может содержать удаленные и измененные записи.

Встроенные инструменты для низкоуровневого криминалистического анализа.

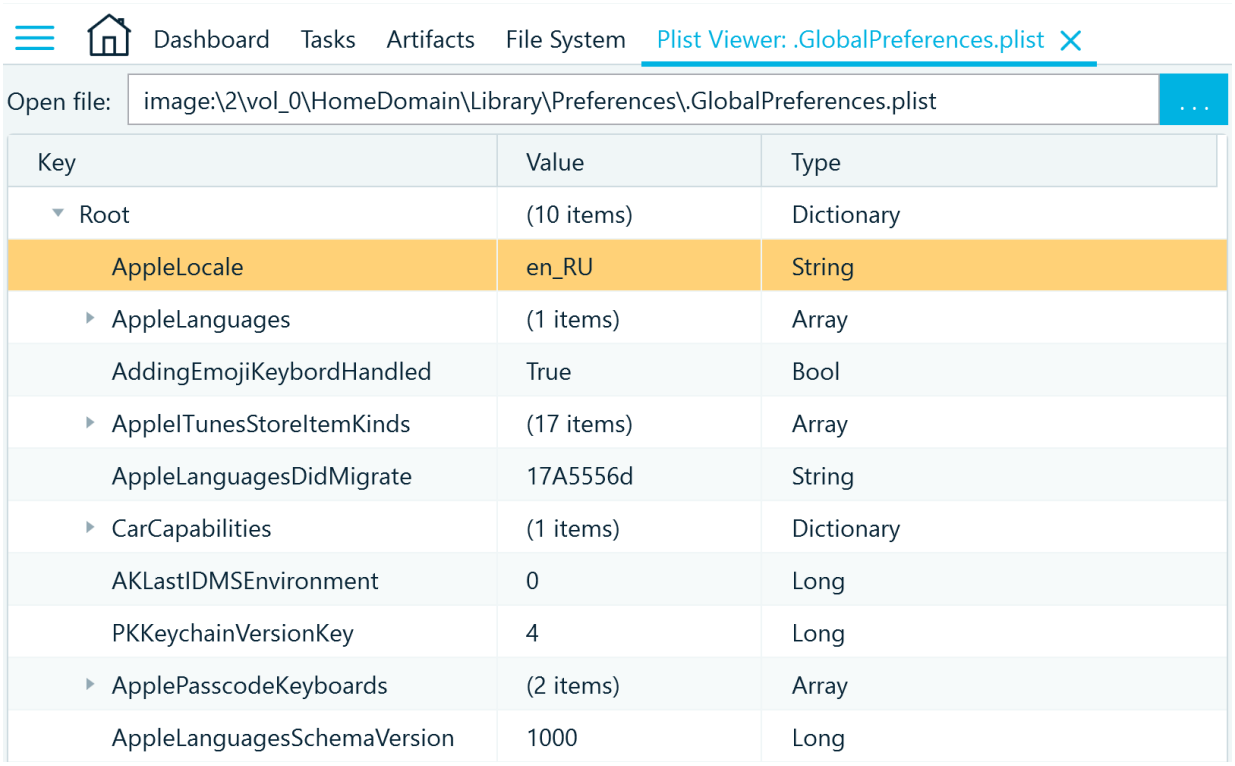
Хотя автоматического извлечения обычно достаточно, для некоторых сложных артефактов может потребоваться ручной поиск и анализ. Для таких исследований Belkasoft X предоставляет мощный файловый менеджер, который позволяет просматривать все тома и разделы внутри образа устройства с существующими и удаленными папками или файлами, а также снимки системы контроля версий.

Когда вам нужно углубиться в тему, Hex Viewer позволяет исследовать отдельные байты, изучать разделы файлов, преобразовывать двоичные значения в различные типы данных, создавать закладки, выполнять пользовательскую обработку данных и применять различные кодировки.



Программа просмотра шестнадцатеричных данных в Belkasoft X предоставляет доступ к низкоуровневому представлению данных.

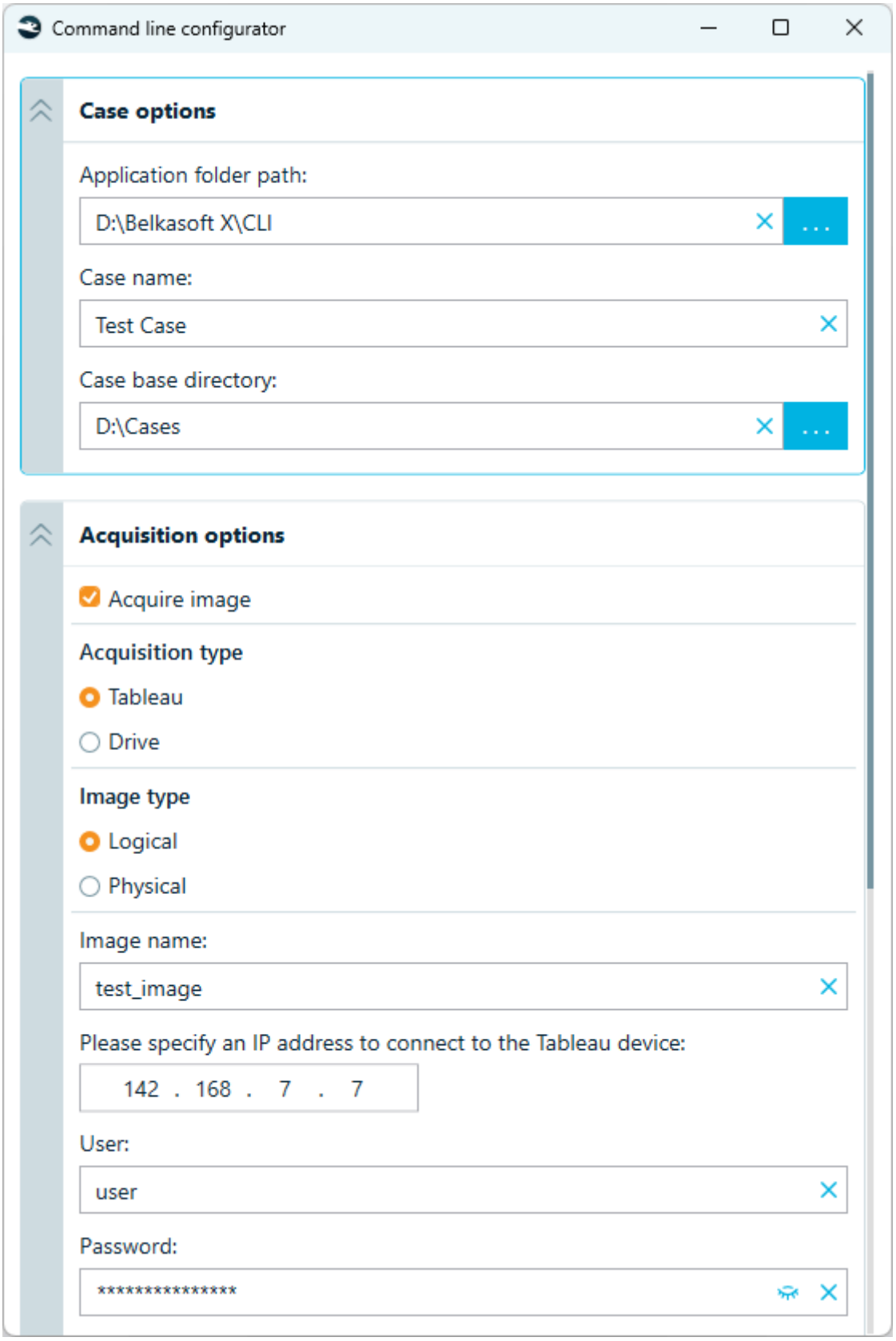
Программы для просмотра файлов PList, Registry и SQLite позволяют более тщательно работать с определенными типами данных и находить дополнительные сведения, которые не удалось обнаружить с помощью автоматического поиска.



Программа просмотра PList отображает структурированное содержимое файлов «списков предпочтений».

Функции автоматизации

Для выполнения рутинных задач расследования вы можете настроить интеллектуальные автоматизированные рабочие процессы и выполнять работу еще быстрее с помощью командной строки Belkasoft X.



Конфигуратор командной строки позволяет создать рабочий процесс для автономного запуска Belkasoft X.

Заключение

Belkasoft X выделяется как универсальный и всеобъемлющий инструмент для цифровой криминалистики и реагирования на кибер-инциденты. Его комплексные возможности оптимизируют весь процесс расследования, от сбора и анализа данных до составления итогового отчета. Расширенные функции, такие как перебор мобильных паролей и BelkaGPT, предоставляют уникальные преимущества, делая Belkasoft X бесценным активом для специалистов по цифровой криминалистике.

Ищете мощное, но при этом удобное и экономичное решение? Сделайте следующий шаг в развитии цифровой криминалистики, изучив Belkasoft X.