РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

# Belkasoft X

Практическое руководство по сбору, исследованию, анализу и документированию цифровых доказательств

Русскоязычное учебно-практическое издание
Подготовлено на основе официального раздела Belkasoft X Help.

Редакция: 20 ноября 2026 г.
Названия команд: сохранены на английском для сопоставления с интерфейсом.

Важно: документ не заменяет официальную документацию, обучение, юридические полномочия и методики экспертной организации. Доступность методов извлечения зависит от версии ПО, лицензии, модели устройства, версии ОС, состояния блокировки и шифрования.

# СОДЕРЖАНИЕ

Нажмите на название раздела для перехода внутри PDF. Также создана панель закладок документа.


1. Назначение и возможности
2. Криминалистические принципы
3. Подготовка и установка
4. Лицензирование и активация
5. Интерфейс
6. Создание дела
7. Добавление источников данных
8. Компьютеры и диски
9. Получение данных с iOS
10. Получение данных с Android
11. Облачные источники
12. Обработка и задачи
13. Артефакты и файловая система
14. Поиск и фильтры
15. Временная шкала и геолокация
16. Граф связей
17. Низкоуровневые просмотрщики
18. Закладки
19. Incident Investigation
20. Отчёты и Evidence Reader
21. Сквозной сценарий
22. Контроль качества и ошибки

# 1. Назначение и возможности

## Назначение

Belkasoft X — комплексная платформа цифровой криминалистики для получения данных, извлечения артефактов, восстановления доступной информации, анализа и подготовки отчётов. Официальная справка описывает компьютерную, мобильную, облачную и RAM-криминалистику, а также Incident Response.

## Основные задачи

Компьютеры и накопители; смартфоны iOS и Android; резервные копии; облачные источники; электронная почта, чаты, браузеры, документы и изображения; поиск удалённых данных; временные шкалы; геолокация; графы связей; отчёты и переносимые кейсы.

## Рабочая логика

Разделяйте четыре этапа: acquisition (получение), processing (обработка), analysis (анализ) и reporting (представление результатов). Завершение одного этапа не гарантирует полноту следующего.

Официальные страницы:

what_is_belkasoft_x

belkasoft_x_tasks

belkasoft_x_workflow

# 2. Криминалистические принципы

## Сохранение исходных данных

Официальная справка указывает, что при dead-box анализе Belkasoft X не должен записывать данные на исследуемый носитель и совместим с write-blocker и образами. Тем не менее используйте проверенный аппаратный блокиратор записи, работайте с копией и документируйте все подключения.

## Хэширование

Фиксируйте контрольные суммы исходного и рабочего образов. При добавлении источников доступны SHA-1, SHA-256 и MD5. В документации отмечены риски коллизий MD5; для проверки целостности предпочтителен SHA-256 либо утверждённая политика лаборатории.

## Время

Часовой пояс задаётся при создании дела. Для источников из разных регионов учитывайте отдельные часовые пояса устройств. Не смешивайте UTC, локальное время устройства и время рабочей станции без пояснения.

## Документирование

Записывайте кто, когда, каким инструментом и с какими настройками выполнял каждую операцию. Отделяйте факт от интерпретации и гипотезы.

Официальные страницы:

forensically_sound_software

when_belkasoft_x_uses_internet

# 3. Подготовка и установка

## Подготовка

Подготовьте выделенную рабочую станцию, достаточный объём RAM и хранилища. Разделите системный диск, исходные образы, рабочие дела и резервные копии. Проверьте системные требования актуальной версии и совместимость лицензии.

## Установка

Получите дистрибутив из официального источника или через авторизованного поставщика. Проверьте цифровую подпись/целостность, запустите установщик и следуйте мастеру. Зафиксируйте версию, сборку, ОС и дату установки.

### Особенности Windows

Официальная справка рекомендует по возможности запуск с административными правами и отключение гибернации до работы: переход системы в гибернацию может потребовать перезапуска Belkasoft X.

Официальные страницы:

installing_belkasoft_x

trial-limitations

# 4. Лицензирование и активация

### Электронная лицензия

Запустите мастер активации, введите полученные лицензионные данные и выполните онлайн-активацию. Для изолированной станции используйте официальный офлайн-процесс через отдельный компьютер с Интернетом. Сохраните сведения об активации.

### USB-ключ (dongle)

Подключите ключ, укажите файл лицензии, если это требуется, нажмите Next и дождитесь подтверждения. Для работы на другой станции повторите процедуру с тем же ключом согласно условиям лицензии.

### Пробная версия

Trial-редакция может иметь ограничения. До реального исследования проверьте, доступны ли необходимые методы получения и экспорта в вашей версии.

Официальные страницы:

activating_belkasoft_x

electronic-license-activation

dongle-license-activation

# 5. Интерфейс

### Home

Начальный экран для создания нового дела или открытия существующего.

### Dashboard

Сводка по делу, источникам, задачам, действиям и статистике.

### Рабочие области

Artifacts — извлечённые артефакты; File System — дерево файлов; Timeline — события по времени; Connection Graph — контакты и связи; Bookmarks — сохранённые находки; Tasks — фоновые операции.

Официальные страницы:

user_interface

home_screen

dashboard

# 6. Создание дела

### Порядок

Нажмите Create case. Заполните Name, Folder, Time zone, Investigator и Description. Нажмите Create и перейдите к добавлению источников.

### Папка дела

Выбирайте диск с запасом места: дела могут быть большими, а каталог хранения нельзя просто изменить после создания. Рекомендуется заранее спланировать структуру хранения.

### Часовой пояс

По умолчанию используется часовой пояс компьютера. Если источники происходят из разных часовых зон, настройте их отдельно, где это предусмотрено, и опишите метод нормализации времени.

Официальные страницы:

creating_case
home_screen_full

# 7. Добавление источников данных

## Поддерживаемые типы

Образы компьютеров и мобильных устройств, физические и логические диски, съёмные носители, дампы памяти и папки. Добавление доступно при создании дела, через Actions → Add data source или кнопку «+» на Dashboard.

## Папки

Existing files — анализ существующих файлов; Recursive — включение подпапок; Nested data sources — поиск внутренних источников, например образов виртуальных машин, pagefile, hibernation, мобильных backup и DMG.

## Дамп памяти

В зависимости от сценария доступны Carve all space и Extract processes. Эти параметры определяют поиск артефактов по сигнатурам и извлечение сведений о процессах.

## Параметры обработки

Различайте Analysis type (анализ с опорой на файловую систему) и Carving type (поиск по сигнатурам). Могут быть доступны анализ существующих файлов, вложенных источников, NTFS shadow copies и сведений о корзине.

## Хэши

Можно выбирать SHA-1, SHA-256 и MD5. Проверьте настройки для крупных файлов: документация указывает, что в конфигурации по умолчанию файлы свыше 200 МБ могут не получать хэш.

Официальные страницы:
adding_data_source
hashset_database

# 8. Компьютеры и диски

## Рекомендуемый сценарий

По возможности создайте образ с write-blocker, затем добавьте его в дело как Image. Live acquisition используйте только после оценки риска изменения состояния системы.

## Шаги

Подключите носитель через блокиратор; убедитесь, что выбран правильный физический диск; задайте отдельный каталог назначения; зафиксируйте формат, ошибки чтения и хэши; добавьте образ в дело; выберите типы анализа и carving.

## Ограничения

Доступность физического извлечения зависит от интерфейса, шифрования, состояния накопителя, контроллера и оборудования.

Официальные страницы:
acquiring_data_source
acquiring_disk_drive

# 9. Получение данных с iOS

## iTunes backup

Требуется iTunes на рабочей станции. Разблокируйте устройство либо укажите путь к lockdown-файлу, задайте Target path и запустите получение. Зашифрованная резервная копия может содержать больше данных.

### Agent backup

Проверьте требования к Интернету и учётной записи Apple ID. Разблокируйте iPhone/iPad, подключите USB, подтвердите Trust this computer, укажите целевую папку и запустите операцию.

### Checkm8

Поддерживается только для определённых моделей и версий iOS; в справке указана Windows 10 с актуальным iTunes. Перед работой проверьте актуальный список совместимости.

### Предостережение

Методы с jailbreak/exploit требуют оценки допустимости и возможного влияния на состояние устройства. Не экспериментируйте на единственном оригинале без плана и резервной стратегии.

Официальные страницы:

iOS

## 10. Получение данных с Android

### ADB backup

Подключите и разблокируйте устройство, включите USB debugging, подтвердите разрешение на компьютере и на устройстве выберите Back up my data, если диалог доступен.

### Agent backup

Программа может установить временный агент для передачи данных; по описанию производителя после получения он удаляется. Разблокируйте смартфон, разрешите USB debugging и запустите операцию.

### Filesystem copy и physical dump

В документации эти методы указаны для rooted-устройств. Физический образ не гарантирует расшифровку пользовательских данных.

### MTP/PTP

Выберите режим передачи файлов на устройстве, подключите его и выберите смартфон в мастере. MTP/PTP не является полным физическим образом.

### MTK / Qualcomm EDL

Специальные методы для отдельных платформ. Требуют проверки совместимости, драйверов и технической квалификации. Не выполняйте аппаратные манипуляции без подготовленного специалиста.

### APK downgrade

Документация предупреждает о риске потери данных приложений. Используйте только после оценки риска и отдельного разрешения.

Официальные страницы:

android

## 11. Облачные источники

### Общий порядок

Проверьте правовое основание и доступ к учётной записи; уточните поддержку конкретного сервиса в актуальной версии; безопасно передайте учётные данные; зафиксируйте время, аккаунт, метод входа, диапазон и ограничения API; добавьте полученный результат в дело.

### Ограничения

Наличие пункта Cloud не означает поддержку любого сервиса или гарантированное получение всех данных аккаунта. Проверяйте список сервисов и лицензионные условия.

Официальные страницы:

cloud

# 12. Обработка и задачи

## Контроль задач

В Tasks проверяйте статус каждой операции. Разбирайте ошибки и недостающие данные; частично завершённую обработку нельзя считать полной. Не отключайте источники до окончания операций, которые используют их напрямую.

## Профили анализа

Analysis profiles позволяют адаптировать обработку к задаче. Фиксируйте выбранный профиль и ручные изменения, поскольку они влияют на состав извлечённых данных.

Официальные страницы:

tasks

task_statuses

analysis_profiles

# 13. Артефакты и файловая система

## Artifacts

Группирует найденные данные по типам: сообщения, почта, браузерная активность, документы, изображения и другие категории. Проверяйте свойства объекта, исходный путь, источник и связанные элементы.

## File System

Показывает дерево файлов и папок. Используйте его для перехода от артефакта к исходному файлу и проверки расположения и метаданных.

## Hashset

Сопоставление по хэшам помогает классифицировать файлы. Проверяйте происхождение базы, алгоритм и значение совпадения: совпадение не доказывает контекст или происхождение файла.

Официальные страницы:

artifacts_full

file_system_full

hashset_database

# 14. Поиск и фильтры

## Поиск

Задайте ключевые слова или фразы, ограничьте категории и источники, используйте регулярные выражения при необходимости. Проверяйте контекст совпадения: источник, путь, время, приложение и связанные объекты.

## Фильтрация

Добавляйте критерии постепенно и проверяйте логику AND/OR. Слишком узкий фильтр может скрыть важные данные.

## Ограничение

Отсутствие результата не доказывает отсутствие данных: объект мог не попасть в образ, быть зашифрован, повреждён или не поддерживаться парсером.

Официальные страницы:

searching_artifacts

regular_expression_syntax

filtering_data

adding_multiple_criteria

# 15. Временная шкала и геолокация

## Timeline

Объединяет события в хронологическую последовательность. Учитывайте часовой пояс, точность временных меток и возможное смещение часов устройства.

## Геолокация

Belkasoft X позволяет просматривать геолокационные артефакты и GPS-данные изображений, использовать Offline Map Server и экспортировать координаты в KML.

## Проверка

Сопоставляйте координаты с источником и временем. Учитывайте точность GPS, EXIF, кэш карт и возможную подмену геоданных. В отчёте указывайте диапазон и происхождение координат.

Официальные страницы:

timeline_full
offline-maps
geolocation_data
pictures_with_gps
geolocation_on_maps
exporting_geolocation_to_kml

# 16. Граф связей

## Анализ

Connection Graph визуализирует отношения между контактами, сущностями и объектами. Изучайте тип связи, направление, частоту, временной диапазон и исходные артефакты.

## Интерпретация

Графическая близость сама по себе не доказывает личные отношения или участие в событии. Подтверждайте вывод первичными данными и контекстом.

Официальные страницы:

connection_graph_full
contacts_and_entities
graph_pane
contact_or_connection_properties

# 17. Низкоуровневые просмотрщики

## Hex Viewer

Просмотр байтов, смещений и шестнадцатеричного/текстового представления. Применяется для проверки структуры, сигнатур и данных, не разобранных парсером.

## SQLite Viewer

Исследование таблиц и записей SQLite. Учитывайте схему, WAL/SHM, транзакции и возможность фрагментов удалённых записей.

## Plist Viewer

Просмотр структурированных Apple Property List, часто содержащих настройки и метаданные.

## Registry Viewer

Исследование ключей и значений Windows Registry. Интерпретируйте их с учётом версии Windows и времени изменения.

Официальные страницы:

hex_viewer
sqlite_viewer
plist_viewer
registry_viewer

# 18. Закладки

## Фиксация находок

Сохраняйте важные артефакты, файлы, контакты и события в Bookmarks. Добавляйте комментарий, почему объект важен и какую гипотезу он поддерживает.

## Проверка

Перед отчётом проверьте список закладок, свойства каждого объекта и связь с исходным источником. Не подменяйте первичный объект одним скриншотом.

Официальные страницы:

bookmarks
bookmarks_window
bookmarks_pane
bookmarked_artifacts_list
selected_artifact_properties

# 19. Incident Investigation

## Сценарий

Определите цель: первичный triage, установление точки входа, анализ вредоносной активности или сбор доказательств. Сохраните volatile data до выключения системы, если это допустимо.

## Практика

Не запускайте лишние утилиты на подозрительной системе без оценки влияния. Сопоставляйте процессы, системные события, сетевые следы, файлы и действия пользователей. Документируйте временную последовательность.

Официальные страницы:

incident_investigation

# 20. Отчёты и Evidence Reader

## Создание

На Dashboard выберите Actions → Create report. Для отдельного артефакта или папки используйте контекстное меню → Create report. Выберите формат, Target folder, при необходимости Open report when done и Advanced Options.

## Содержание

Включайте цель и объём исследования, идентификацию источников, методы получения, версии ПО, хэши, параметры обработки, результаты, ограничения, часовые пояса и приложения. Разделяйте факты и интерпретации.

## Карта и граф

Добавляйте карту и Connection Graph, если они поясняют результаты. Указывайте легенду, временной диапазон и происхождение данных.

## Evidence Reader

Portable Case позволяет передавать дело или его содержимое для просмотра на другой машине. Проверьте состав экспорта и ограничения лицензии.

Официальные страницы:

creating_reports
report_options
map_to_report
graph_to_report
reader

# 21. Сквозной сценарий

## Этапы

1) Законное основание и план; 2) подготовка станции и блокиратора; 3) создание дела; 4) получение образа/backup и хэширование; 5) добавление источника; 6) обработка; 7) поиск и анализ; 8) проверка низкоуровневых данных; 9) закладки и временная шкала; 10) отчёт и экспорт; 11) архивирование.

## Критерий качества

Другой квалифицированный специалист должен понимать, какой источник исследовался, каким способом получены данные, какие настройки применялись и как сформирован вывод.

Официальные страницы:

belkasoft_x_workflow

# 22. Контроль качества и ошибки

## Перед началом

Проверьте правовое основание, идентификаторы источников, защиту от записи, свободное место, часовой пояс, версию ПО и лицензию.

## Перед завершением

Проверьте статусы задач, ошибки, хэши, временные метки, контекст находок, полноту отчёта и сохранность исходных образов.

## Типичные ошибки

Работа с оригиналом без защиты; неверный часовой пояс; предположение, что физический дамп расшифрует данные; игнорирование ошибок парсеров; слишком узкие фильтры; устаревшая совместимость; принятие автоматической классификации за экспертный вывод.

# 23. Справочник всех пунктов оглавления Help

На исходной странице Help обнаружено 84 ссылки оглавления/навигации. Ниже приведены все тематические пункты, сгруппированные по разделам. Официальная страница с актуальными переходами: belkasoft.com/help.

## Введение

- What is Belkasoft X and who are its users?
- Types of tasks Belkasoft X is used for
- Typical Belkasoft X workflow
- Forensically sound software
- When Belkasoft X uses the Internet
- Why Belkasoft X?

## Quick start

- Installing Belkasoft X
- Belkasoft X Trial version limitations
- Activating Belkasoft X license
- Electronic license activation
- Floating (dongle) license activation
- Home screen
- Creating a report
- Dashboard
- Artifacts
- File System

- Timeline
- Connection Graph
- Incident Investigation
- Reattach a disconnected data source

## Редакции и интерфейс

- X Forensic
- X Corporate
- Belkasoft X user interface
- Home screen
- Creating a case
- Other options and functions on Home

## Dashboard и источники

- Dashboard
- Case properties
- Actions
- Automatic searches
- Data sources
- Application types
- Artifacts
- Adding data source
- Look for matches from a hashset database

## Окна анализа

- Artifacts window
- File System window
- Timeline window
- Connection Graph window
- Contacts and entities
- Graph pane
- Contact or connection properties pane
- Hex Viewer window
- SQLite Viewer window
- Plist Viewer window
- Registry Viewer window

## Настройки

- Settings
- General settings
- Appearance settings
- Analysis profiles
- Bookmark settings
- Carving settings
- Picture settings
- Video settings

## Закладки и задачи

- Creating a bookmark

- Bookmarks window
- Bookmarks pane
- Bookmarked artifacts list
- Selected artifact properties
- Tasks window
- Task statuses
- Entering missing data
- Filtering tasks

## Поиск, геолокация, фильтры

- Searching artifacts
- Regular expression syntax
- Search Results window
- Belkasoft Offline Map Server
- Reviewing geolocation data
- Pictures with GPS
- Showing geolocation artifacts on Open Street Maps or Google Earth
- Exporting geolocation artifacts to KML format
- Filtering data
- Adding multiple criteria

## Отчёты, acquisition, export

- Creating reports
- Report options
- Including a map to a report
- Including a connection graph to a report
- Acquiring data source
- Acquiring disk drive
- Acquiring iOS device
- Acquiring Android device
- Acquiring cloud
- Portable case with Belkasoft Evidence Reader
- Hashcat brute-force options

Перечень отражает названия пунктов исходной страницы; некоторые ссылки ведут на обзорные страницы и подпункты, а не на отдельные операции. Для актуальной навигации используйте официальный Help Contents.

# 24. Глоссарий

| Термин | Значение |
|---|---|
| Acquisition | Получение / извлечение данных с устройства или из облака. |
| Artifact | Цифровой артефакт — данные, имеющие аналитическое значение. |
| Carving | Поиск данных по сигнатурам, в том числе вне обычной структуры файловой системы. |
| Case | Дело / проект исследования. |
| Data source | Источник данных: образ, диск, папка, дамп памяти и т. п. |
| Dead-box analysis | Исследование выключенного или отдельно подключённого носителя/образа. |
| Hash | Контрольная сумма для проверки целостности и сопоставления. |
| Image | Криминалистический образ носителя или устройства. |
| Logical acquisition | Логическое извлечение доступных файлов и данных. |
| Physical acquisition | Получение физического образа памяти/разделов, если метод поддерживается. |
| Triage | Первичная сортировка и выделение значимых данных. |
| Write blocker | Средство предотвращения записи на исследуемый носитель. |

# 25. Источники и примечания

Основной источник — официальная страница Belkasoft X Help и её дочерние материалы. Руководство систематизирует и объясняет пользовательские сценарии; при расхождении приоритет имеет актуальная документация установленной версии.

https://belkasoft.com/help
https://belkasoft.com/what_is_belkasoft_x
https://belkasoft.com/belkasoft_x_workflow
https://belkasoft.com/forensically_sound_software
https://belkasoft.com/adding_data_source
https://belkasoft.com/iOS
https://belkasoft.com/android
https://belkasoft.com/cloud
https://belkasoft.com/creating_reports
https://belkasoft.com/reader

Ограничения: интерфейс и функции меняются между сборками. Специальные методы мобильного извлечения зависят от моделей, версий ОС, аппаратных платформ и условий лицензии. Руководство не является заверением производителя о поддержке любой конкретной конфигурации.