



МОБИЛЬНЫЙ КРИМИНАЛИСТ ДЕСКТОП

Ведущий российский разработчик программного обеспечения для проведения компьютерно-технической экспертизы мобильных устройств, дронов, облачных сервисов и персональных компьютеров.

МОБИЛЬНЫЙ КРИМИНАЛИСТ ДЕСКТОП

3

ОСНОВНЫХ
ПРЕИМУЩЕСТВА
ПРОДУКТА

- ВЫСОКАЯ
СКОРОСТЬ
ИЗВЛЕЧЕНИЯ
И АНАЛИЗА
ИНФОРМАЦИИ
- ПОРТАТИВНЫЙ
ИНСТРУМЕНТ
- ПРОСТОЙ
И УДОБНЫЙ
ИНТЕРФЕЙС

Многофункциональный инструмент, позволяющий извлекать, расшифровывать и анализировать ключевые данные из персональных компьютеров, ноутбуков на операционных системах Windows, macOS, GNU/Linux.

ПОЧЕМУ ВЫБИРАЮТ «МК ДЕСКТОП»:

- Продукт для извлечения и исследования критически важных данных из персональных компьютеров.
- Быстрая обработка всей извлеченной информации.
- Большой набор аналитических инструментов для проведения расследования.
- Регулярное обновление функционала в соответствии с самыми современными ИТ-технологиями.
- Постоянный доступ к видео-урокам, инструкциям и вебинарам для получения навыков работы с продуктом.



Учетные данные и токены



Сообщения, контакты и медиа-файлы



Письма и контакты



Данные веб-браузеров:

учетные записи, данные форм автозаполнения, история посещения сайтов, загрузки файлов и поисковых запросов, закладки и cookies



Данные секретных хранилищ
Keychain и Windows Vault



Wi-Fi точки доступа и пароли к ним



Резервные копии iTunes



Информация о системе ПК



Данные о действиях пользователя
на компьютере



История действий с файлами
и документами



Сведения о всех подключениях
к компьютеру через USB-порт

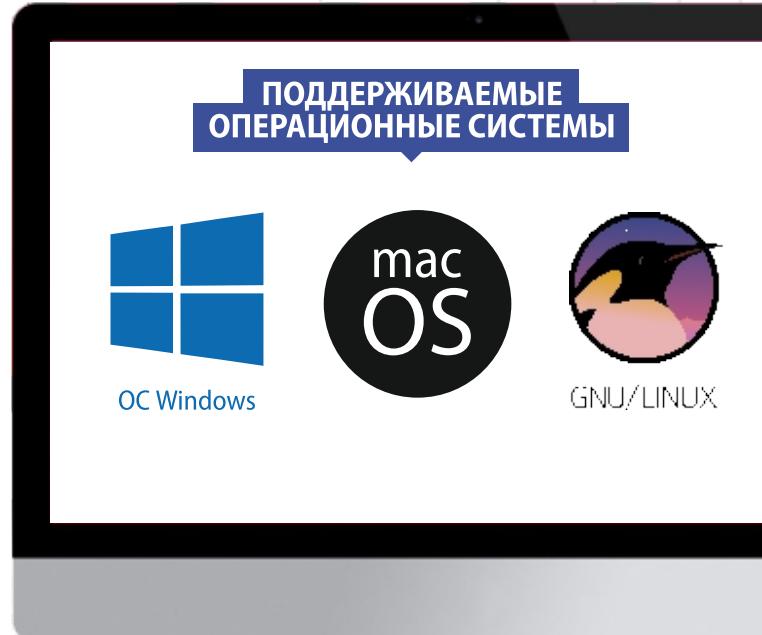
ПОДДЕРЖИВАЕМЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ



ОС Windows



GNU/LINUX



ДЛЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

«МК Десктоп» обладает широким спектром решаемых задач и является незаменимым помощником в работе правоохранительных органов, помогая извлечь и проанализировать данные за короткий промежуток времени, провести первичную экспертизу данных и сформировать портрет владельца ноутбука или персонального компьютера.

ПОЛИЦИЯ

НАМ ДОВЕРЯЮТ:



[DATA PROTECTION]



ИЗВЛЕЧЕНИЕ МАССИВА КРИМИНАЛИСТИЧЕСКИ ВАЖНЫХ ДАННЫХ ЗА КОРОТКОЕ ВРЕМЯ

«МК Десктоп» извлекает различную информацию, например, учетные данные, токены, переписку, контакты, вложения, данные Keychain и Windows Vault, системные артефакты и многое другое.

Программа обладает высокой скоростью работы благодаря современному движку программы.



ПРОВЕДЕНИЕ ПЕРВИЧНОЙ ЭКСПЕРТИЗЫ ДАННЫХ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ

Одним из важных моментов при расследовании является возможность извлечения основного массива данных за короткое время. «МК Десктоп» легко справляется с поставленной задачей, подготавливая найденную информацию к импорту в необходимом формате и количестве для последующего анализа, освобождая времени исследователя для других задач.



БЫСТРЫЙ АНАЛИЗ ПОЛУЧЕННОЙ ИНФОРМАЦИИ

«МК Десктоп» позволяет быстро провести анализ критически важных данных с помощью большого набора аналитического функционала. Для применения доступны 9 основных инструментов: «Статистика», «Граф Связей», «Контакты», «Звонки», «Сообщения», «Лента Событий», «Файлы», «Важное» и «Поиск».



ФОРМИРОВАНИЕ ОБЩЕГО ПРЕДСТАВЛЕНИЯ О ДАННЫХ НА КОМПЬЮТЕРЕ И ПОРТРЕТА ЕГО ВЛАДЕЛЬЦА

Благодаря детальному анализу информации с помощью продукта «МК Десктоп», можно составить портрет владельца персонального компьютера.

Использование аналитических инструментов в совокупности дает целостное представление о круге общения владельца ПК, о его привычках, о том, что ему нравится, чем он интересуется и увлекается. Инструменты «Статистика» и «Граф Связей» позволяют выявить наиболее частые контакты владельца компьютера, прямые и непрямые связи, а также в каких мессенджерах больше всего происходит активное взаимодействие владельца ПК с другими людьми. А об интересах и привычках можно узнать из истории посещений и просмотров в браузере или сохраненных сообщениях/фотографиях из разных источников.



РАБОТА С ПОЛУЧЕННЫМИ ДАННЫМИ БЕЗ ИТ-СПЕЦИАЛИСТОВ

Любой исследователь сможет быстро извлечь и проанализировать всю необходимую информацию из ноутбука или ПК без помощи ИТ-специалиста. Интерфейс «МК Десктоп» интуитивно понятен и прост в использовании, поэтому не потребует каких-либо специальных технических навыков по работе с ним.



ДЛЯ КОРПОРАТИВНЫХ КЛИЕНТОВ

Для специалистов служб безопасности коммерческих компаний открываются возможности для расследования и предотвращения различных видов корпоративных инцидентов, таких как кража интеллектуальной собственности, раскрытие инсайдерства, утечка конфиденциальных данных и многое другое.

«МК Десктоп» является ключевым инструментом для проведения аудита системы информационной безопасности.

НАМ ДОВЕРЯЮТ:





АУДИТ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МК «Десктоп» содержит в себе уникальную особенность – поддержка анализа данных нескольких устройств. Для удобства вся полученная информация импортируется в программу для анализа в одно дело.



РАСКРЫТИЕ ИНСАЙДЕРСТВА

При подозрении какого-либо сотрудника в инсайдерстве, можно легко узнать, совершались ли неправомерные действия со стороны сотрудника. Например, просмотреть полный список подключенных устройств через USB-порт и доказать связь между компьютером и картой памяти. Или обнаружить следы открытия файла и его выбора при отправке через мессенджер / браузер / почтовый агент / облако конкуренту. Даже если в самом приложении информация, относящаяся к данному действию, была удалена.



ОБНАРУЖЕНИЕ КРАЖИ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Одним из частых корпоративных инцидентов является кража интеллектуальной собственности.

Для того, чтобы выявить преступника и доказать его причастность, изучите историю действия владельца учетной записи на ПК. Например, узнайте, с какими файлами или приложениями работал пользователь, а также какие устройства подключал через USB-порт.



УСТАНОВЛЕНИЕ КАНАЛОВ УТЕЧКИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

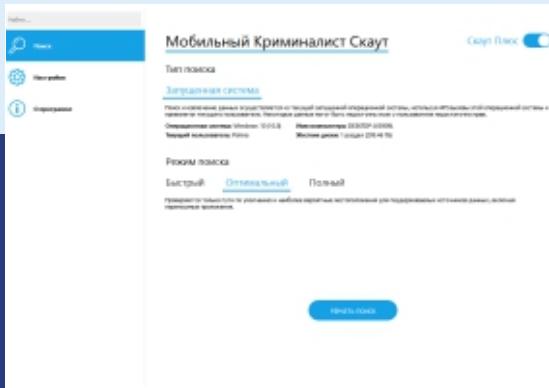
При обнаружении утечки коммерческой тайны из компании, «МК Десктоп» поможет установить ее источник. Для установления возможного канала утечки проанализируйте системные артефакты. Благодаря этому можно узнать, например, что было установлено шпионское ПО или вредоносная программа, которая передает информацию из компьютера на сторонний ресурс.



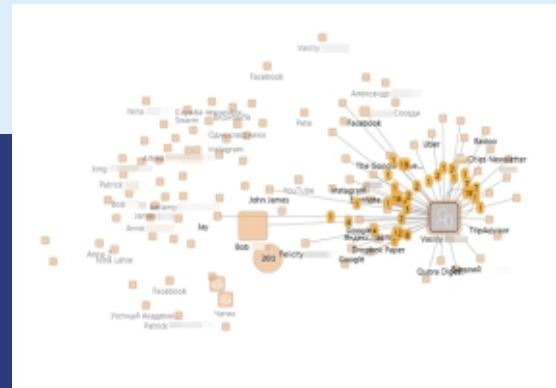
ВЫЯВЛЕНИЕ НЕЦЕЛЕВОГО ИСПОЛЬЗОВАНИЯ РАБОЧЕГО ВРЕМЕНИ

Для руководства компании важным моментом в оценке эффективности работы сотрудника, является целевое использование рабочего времени. Многие сотрудники на работе могут заниматься личными делами, посещая интернет-магазины, общаясь в социальных сетях или просматривая сайты, которые им интересны. Для решения этой задачи можно воспользоваться «Матрицей активности», с помощью которой вы просмотрите активность за нужный период времени.

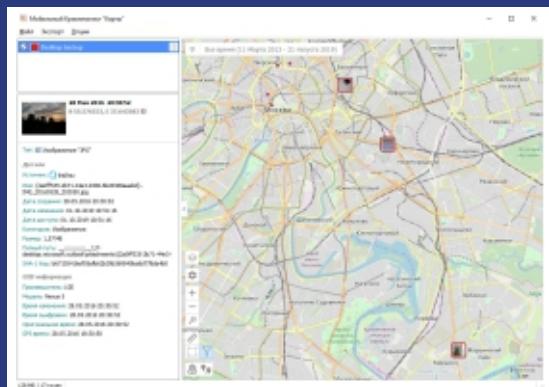
ПРОГРАММНЫЕ МОДУЛИ



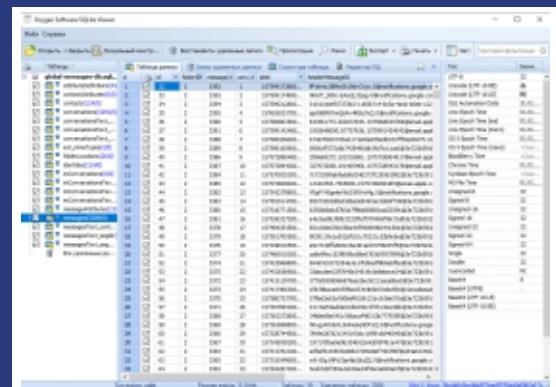
СКАУТ



АНАЛИТИЧЕСКИЙ
ФУНКЦИОНАЛ



КАРТЫ



SQLITE ПРОСМОТРЩИК



СКАУТ

Извлекает данные из исследуемых ПК и ноутбуков – от логинов/паролей и токенов до переписки в мессенджерах и почтовых агентах.

Имя	Ссылка	Последнее обновление
Браузеры	Браузеры	
Несколько сайтов	Несколько сайтов	12 часов назад
Сайты с изображениями	Сайты с изображениями	1 час назад
Помощник сайта	Помощник сайта	Помощник сайта
Рекомендованное	Рекомендованное	Помощник сайта
Скачанные	Скачанные	Скачано: 1,38 ГБ
Бесплатные программы	Бесплатные программы	Скачано: 0 ГБ
Сайты с изображениями	Сайты с изображениями	Скачано: 0 ГБ
Маршрутная система	Маршрутная система	Скачано: 0 ГБ
Паспортные	Паспортные	Скачано: 0 ГБ
О программе	О программе	Скачано: 0 ГБ
Internet Explorer	Internet Explorer	Помощник сайта
Google Chrome	Google Chrome	Помощник сайта: 0,11 МБ
Firefox	Firefox	Помощник сайта: 0,11 МБ
Thunderbird	Thunderbird	Помощник сайта: 0,11 МБ
Unigram	Unigram	Помощник сайта: 0,11 МБ
Opera	Opera	Помощник сайта: 0,03 ГБ



ПАРОЛИ И ТОКЕНЫ

The screenshot shows the 'File Manager' interface with the title bar 'Мой компьютер' (My Computer) and the window title 'Файлы' (Files). The left sidebar contains icons for 'Новый' (New), 'Папка' (Folder), 'Задачи' (Tasks), 'Маркеры и пакеты' (Markers and packages) with 24 items, 'Программы' (Programs) with 8 installed, 'Библиотеки' (Libraries) with 2 installed, 'Изображения' (Images) with 2 selected, 'Музыка' (Music) with 1 selected, 'Фильмы' (Movies) with 1 selected, 'Фотографии' (Photos) with 2 selected, 'Скачанные' (Downloads) with 15 selected, 'История' (History) with 15 selected, 'Журнал ошибок' (Error Log) with 1 selected, 'Настройки' (Settings), and 'О программе' (About program). The main pane displays a file list with columns for 'Файл' (File), 'Размер' (Size), and 'Дата' (Date). The list includes files like '000' (100B), '001' (100B), 'PhoneInfo' (100B), '00204' (100B), '0074' (100B), 'FableFox4DCH.RU' (100B), '01' (100B), 'N421_5' (100B), 'N421_5' (100B), 'N421_5' (100B), 'N421_5' (100B), 'N421_5' (100B), 'event' (100B), 'GericPhone' (100B), 'Assimilator' (100B), 'Android_2019' (100B), 'Android_2019' (100B), and 'Android_2019' (100B). The bottom status bar shows '15/15'.

Название	Берро DC	Время	Размер	Путь
iPhone Xs [iPhone X]	11.0.2	2018-11-19 16:34:24+04:00	11.16	C:\Users\Oleg\Downloads\iPhone Xs [iPhone X]
iPhone Xs [iPhone X]	11.1	2019-09-29 12:54:19+04:00	0.16	C:\Users\Oleg\Downloads\iPhone Xs [iPhone X]



РЕЗЕРВНЫЕ КОПИИ



АНАЛИТИЧЕСКИЙ ФУНКЦИОНАЛ

Позволяет исследовать коммуникации владельца компьютера, анализировать порядок его действий, в деталях изучить полученные файлы и др.

-  СТАТИСТИКА
-  ГРАФ СВЯЗЕЙ
-  КОНТАКТЫ
-  ЗВОНИКИ И СООБЩЕНИЯ
-  ЛЕНТА СОБЫТИЙ
-  ФАЙЛЫ
-  ВАЖНЫЕ УЛИКИ
-  ПОИСК

демонстрирует статистику по коммуникациям владельца ПК.

показывает прямые и косвенные связи между владельцем ПК и его контактами.

представляет подробную информацию о всех контактах в извлечении, а также объединяет их по индивидуальным настройкам.

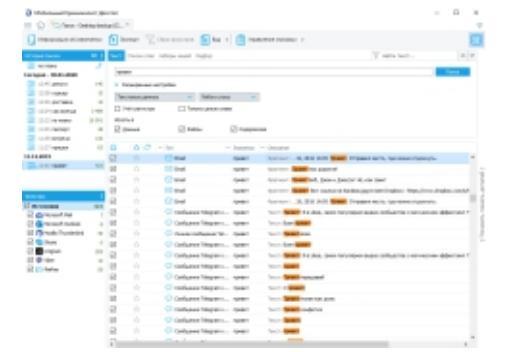
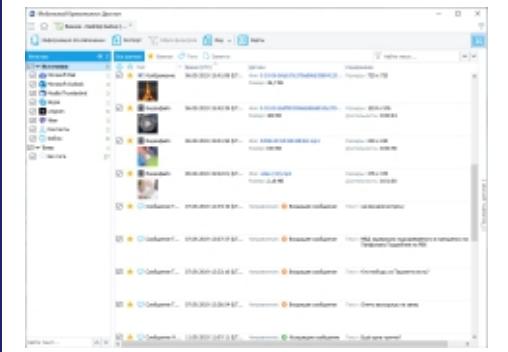
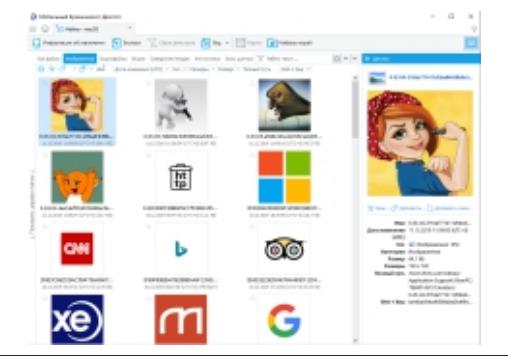
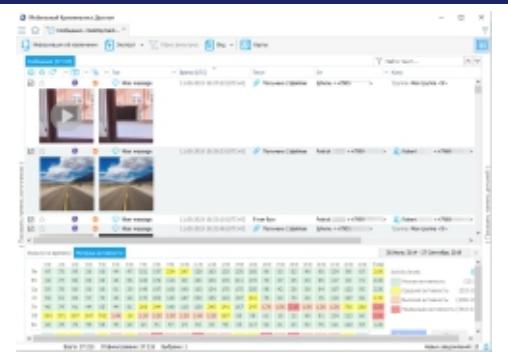
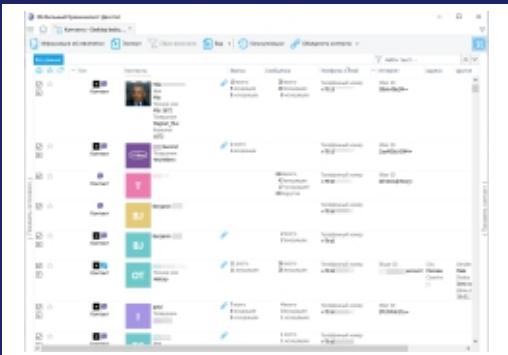
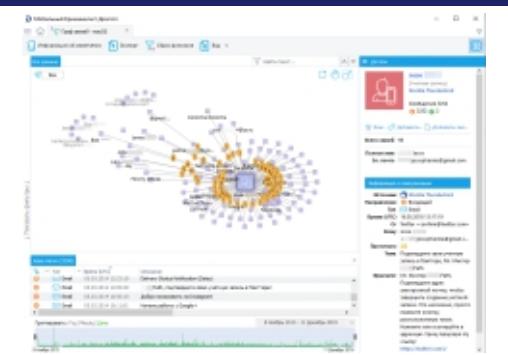
содержат все звонки и сообщения извлечения, а также предоставляют подробную информацию о них.

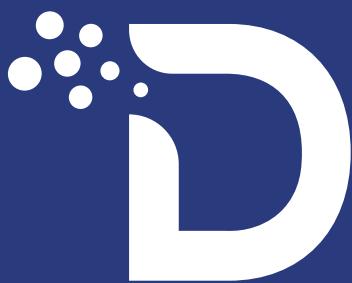
выстраивает все действия владельца ПК в хронологическом порядке.

позволяет одновременно анализировать все файлы извлечения. Каждый тип данных расположен в отдельной вкладке.

объединяет в себе все артефакты, выделенные исследователем в процессе анализа данных.

производит поиск необходимых данных как внутри всего извлечения, так и внутри отдельно взятых документов.





МОБИЛЬНЫЙ КРИМИНАЛИСТ ДЕСКТОП

ООО «ОКСИДЖЕН СОФТВЕР»
РФ, 105064, МОСКВА,
НИЖНИЙ СУСАЛЬНЫЙ ПЕР., д. 5, СТР. 8Б
+7-495-909-9278

- ✉ support@oxygensoftware.ru
- 🌐 www.oxygensoftware.ru
- VK vk.com/mkriminalist
- TG t.me/oxygensoftware
- FB www.facebook.com/MKriminalist