Аналитический обзор

eDiscovery. Основы, методы и техники досудебной идентификации электронных доказательств

group-ib.ru

GROUP IB

ОГЛАВЛЕНИЕ

Что такое eDiscovery?

eDiscovery (досудебная идентификация электронных доказательств, поиск электронной информации, обнаружение электронных данных) – это процесс обнаружения, идентификации, юридически правильного закрепления цифровых данных, способных выступать доказательствами в судебном разбирательстве.

Типовыми объектами eDiscovery являются: электронные письма, информация из базы данных, сообщения голосовой почты, сведения о чатах из программ обмена мгновенными сообщениями, графические файлы, видеофайлы, информация из социальных сетей и т.д.

Основные задачи eDiscovery

Задача eDiscovery - обеспечить взаимодействие технических специалистов, предоставляющих результаты исследования цифровых доказательств, с клиентом и его юристами.

1 — Технические специалисты обеспечивают закрепление цифровых доказательств, чтобы у противоположной стороны в судебном процессе не имелось оснований для выдвижения обвинений, что эти доказательства были как-то изменены, подброшены или уничтожены в ходе получения доказательственной базы, или получены с нарушением процессуальных норм.

2 — Искомые цифровые доказательства часто находятся в огромном массиве слабоструктурированных данных, размещенных в различных источниках: на серверах компании, в облаках, базах данных, архивных копиях данных, IoT-устройствах и т.д. Обнаружить требуемые данные неподготовленному юристу практически невозможно. Технические специалисты помогают выделить из массы разнородных данных только ту информацию, которая будет актуальна для интересующего клиента или его юристов случая. Тем самым, они помогают компании сократить время, которое та тратит на проведение аудита или внутренних расследований.

3 — Юристы, судьи, адвокаты слабо разбираются в технической терминологии. Задача специалистов - объяснить им суть использованных процессов и методов для обнаружения, закрепления и изъятия цифровых доказательств, а также важность обнаруженной информации понятным языком.

Почему важна eDiscovery?

Деятельность человека в современном мире, независимо от его желания, порождает огромное число цифровых следов.
Эти следы, в том или ином количестве, могут обнаружить и процессуально закрепить технические специалисты для дальнейшего использования клиентом или его адвокатом в ходе судебных заседаний против другой стороны.

eDiscovery обеспечивает безопасный и мгновенный доступ к бизнес-информации клиента в соответствии со строгой моделью доступа, возможностью поиска, просмотра и анализа данных, юридического закрепления обнаруженных документов, релевантных запросу клиента.

В рамках осуществления процесса eDiscovery технические специалисты помогают:

- **Произвести обнаружение этих следов, их процессуально правильное закрепление и анализ;**
- **Оценить и подготовить представление этих материалов в суде;**
- **Разработать модель правильного представления собранных цифровых доказательств в суде, привести юридически обоснованные аргументы, выстроить линию защиты, используя обнаруженные данные и документы.**

Модель обнаружения и закрепления электронных доказательств

eDiscovery подразумевает использование совокупности процессов и технологий и включает девять основных этапов

ЭТАП 1

Подготовительный этап

На этом этапе изучаются политики, процедуры, процессы электронного оборота у клиента. Определяется круг источников, задействованных в информационных процессах клиента: рабочие станции, сервера, облака, мобильные устройства, системы хранения данных, виртуальные хранилища и т.д.

ЭТАП 2

Идентификация

Осуществляется поиск источников, которые потенциально могут содержать релевантные запросу клиента данные.

ЭТАП 3

Защита информации

После определения потенциальных источников данных проводятся процедуры, направленные на защиту содержащейся в них информации от случайного или намеренного изменения, повреждения или уничтожения.

ЭТАП 4

Сбор информации

Собираются такие метаданные, как дата создания и размер файла, его криптографический хэш. В дальнейшем эти данные позволяют подтвердить, что собранная информация не подвергалась модификации.

ЭТАП 5

Обработка информации

Фаза обработки включает подготовку собранной информации для анализа. Как правило, для обработки применяется специальное криминалистическое программное обеспечение. Во время обработки файлы могут быть извлечены из каталогов и криминалистических копий, удалены бессмысленные и системные файлы, дубликаты. Информация может быть преобразована в более понятный вид для просмотра клиентом и его адвокатами.

ЭТАП 6

Оценка результатов

Специалисты по компьютерной криминалистике совместно с клиентом или его адвокатами проводят анализ полученных результатов для обнаружения релевантных, нерелевантных и наиболее важных документов, полученных в ходе выполнения предыдущего этапа. Для ускорения проведения такого анализа все чаще применяется искусственный интеллект.

ЭТАП 7

Анализ

Данный этап является вариацией шестого этапа. Он направлен на более глубокий поиск контента и контекста в анализируемой информации и документах, включая использование поисковых шаблонов, ключевых тем, данных о людях и обсуждение обнаруженных результатов.

ЭТАП 8

Производство

В этой фазе определяются документы и информация, которые будут использованы как потенциальные доказательства клиентом и его адвокатами, а также производится подготовка документов для клиента.

ЭТАП 9

Презентация результатов

Представление результатов анализа клиенту и его адвокатам.

Форматы представления результатов

В ходе выполнения eDiscovery результаты работы специалистов могут быть представлены в следующих форматах:

Графический формат

Обнаруженные файлы преобразуются в графические файлы, как правило, в формате .tiff.

Бумажный формат

Все обнаруженные электронные доказательства распечатываются на бумаге.

Нативный формат

Файлы сохраняются в формате, в котором они были созданы изначально. Например, документ формата .docx сохраняется в .docx; электронное письмо, содержащееся в файле .eml, сохраняется в этом же формате .eml и т.д.

Подобный формат

Файлы извлекаются или преобразуются в другой формат, отображение данных в котором максимально схоже с нативным форматом, но для отображения сведений требуется применение специализированного программного обеспечения. Также в нем удобно производить поиск информации (по ключевым словам или используя специальные запросы). Например, информация из электронных писем сохраняется в формат .htm, .mht или .rtf, базы данных сохраняются в текстовых файлах или файлах формата .csv.

Часто встречающие кейсы

Популярным типом eDiscovery кейсов является установление того, какие действия осуществлял работник в период, предшествующий его увольнению: какие документы он удалял, переносил на внешние накопители, отправлял ли на свои личные адреса электронной почты конфиденциальные документы компании.

Даже когда работодатель имеет полную информацию о хищении бывшим работником данных, составляющих коммерческую тайну компании (например, работодатель может получить эту информацию из DLP-системы предприятия), ему нужно юридически закрепить ее, чтобы потом обратиться с претензией к бывшему работнику в суде.

Типовыми кейсами для данной услуги являются:

- **Заверение контента отдельного чата;**
- **Заверение контента сайта;**
- **Установление факта получения или отправки электронного письма;**
- **Обнаружение факта редактирования документа на конкретном компьютере и истории его редактирования;**
- **Отслеживание истории посещения Интернета пользователем компьютера или ноутбука;**
- **Установление последовательности совершения пользователем различных действий.**

eDiscovery: кейсы от Group-IB

Кейс №1. «Недобросовестный работник»

Профиль клиента

Крупная компания по производству промышленных роботов, один из лидеров рынка, где работает более 2000 сотрудников.

Ситуация

Компания заподозрила одного своего бывшего сотрудника, занимавшего руководящую позицию, в краже сведений, составляющих коммерческую тайну, таких как техническая документация на производимое оборудование, сведения о постоянных клиентах и т.д. Подозрение в краже было обусловлено тем, что бывший сотрудник создал свою компанию с аналогичным профилем работы, и от Заказчика нашего исследования стали уходить клиенты в его новую компанию.

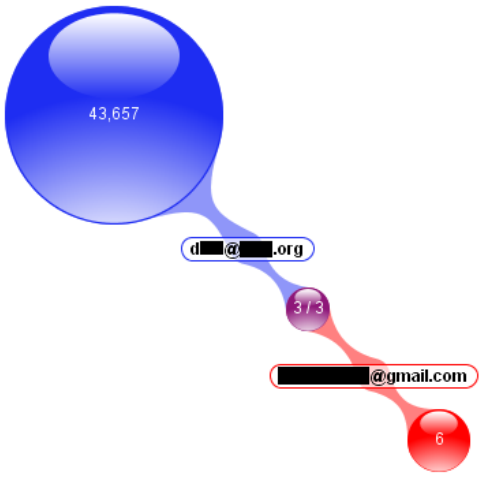
На исследование были представлены: служебные ноутбук и смартфон бывшего сотрудника.

Действия

В ходе проведения работ по этому кейсу специалисты Group-IB обнаружили цифровые следы в исследуемых устройствах, указывающие на копирование конфиденциальных данных и технической документации Заказчика на внешние USB-носители. Также было выявлено шесть фактов пересылки технической документации компании со служебного электронного ящика бывшего сотрудника на его личный почтовый ящик, расположенный на одном из бесплатных почтовых серверов.

Результат

Обнаруженные электронные доказательства были юридически закреплены, что позволило Заказчику обратиться в суд с претензией к бывшему работнику о возмещении понесенных им убытков.



Электронные письма, отправленные с рабочего почтового ящика сотрудника на его личный почтовый ящик

Кейс №2. «Недобросовестный работник страховой компании»

Профиль клиента

Крупная компания, входящая в ТОП-10 российских страховых компаний, у которой свыше 10 региональных офисов, расположенных по всей стране.

Ситуация

Из регионального подразделения страховой компании в головной офис поступило заявление о возмещении страховки КАСКО на пострадавший в ДТП автомобиль, который не подлежал восстановлению. Стоимость компенсации составляла несколько миллионов рублей. Исследуя материалы страхового дела, у сотрудника компании возникли подозрения, что фотографии автомобиля, на который была оформлена страховка, являются поддельными.

Действия

Во время исследования, проведенного экспертом Group-IB, были изучены эти фото и ноутбук страхового агента, оформлявшего страховку. В результате исследования временных меток файлов установлено, что эти фотографии сделаны уже после совершения ДТП (для изготовления фото при оформлении страховки был использован другой автомобиль схожей марки и цвета, а сама страховка была оформлена задним числом).

Результат

Собранные доказательства позволили страховой компании обратиться в правоохранительные органы по факту мошенничества, совершенного сотрудником компании.

Кейс №3 «Кража интеллектуальной собственности»

Профиль клиента

Транснациональная ИТ-компания, предоставляющая более 50 сервисов в интернет пространстве, где работает свыше 8500 человек.

Ситуация

В компании произошёл инцидент, связанный с утечкой конфиденциальных данных. Система DLP (Data Leak Protection) клиента зафиксировала факт передачи по сети информации, содержащей коммерческую тайну.

Действия

Специалист Group-IB выехал к клиенту и сделал копию НЖМД подозреваемого в передаче информации, выгрузил журналы DLP и опросил сотрудников. При исследовании НЖМД и журналов DLP удалось выяснить следующее.

Сотрудник компании Петренко (фамилия изменена) использовал облачное хранилище Dropbox для хранения некоторых файлов, подпадающих под коммерческую тайну. Доступ к облачному хранилищу Петренко предоставлял своим друзьям, таким образом осуществляя их незаконное распространение.

Из переписки, обнаруженной на диске, удалось установить, что Петренко совместно с друзьями организовал компанию, основная деятельность которой заключалась в предоставлении помещений в аренду на территории г. Москва. Используя полученные незаконным путем сведения, а именно алгоритмы ранжирования, они продвигали сайт своей компании на первые места в системе поисковой выдачи. При этом и Петренко, и его знакомые осознавали, что нарушают закон.

Результат

В ходе дальнейшего расследования была полностью выявлена преступная группа, использующая интеллектуальную собственность клиента в корыстных целях. Доказана непосредственная причастность Петренко к передаче информации, составляющей коммерческую тайну, третьим лицам. У фигурантов дела проведены обыски, изъяты носители информации, при последующем исследовании которых подтвердились первоначальные выводы и дополнена картина преступления.

В данный момент Петренко осужден.

Кейс №4 «Внутреннее расследование»

Ситуация

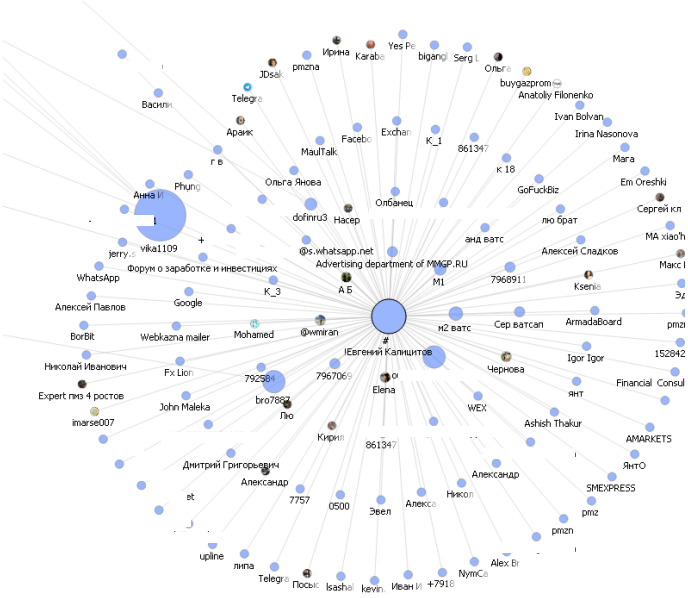
В крупном региональном банке группа сотрудников планировала совершить хищение денежных средств, замаскировав эти действия под атаку хакеров. Большую часть обсуждения задуманного плана они осуществляли с помощью корпоративной почты.

Действия

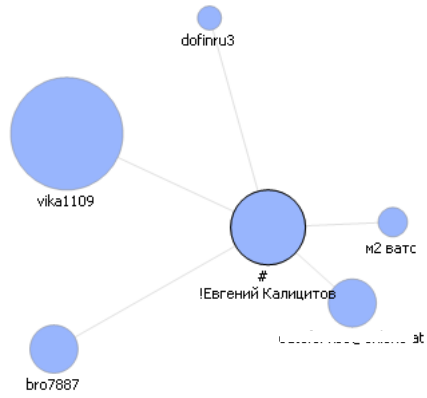
Наши специалисты выгрузили и провели анализ почтовой базы сервера банка. В ходе проведения исследования были отделены электронные письма, которыми обменивались эти сотрудники.
С использованием техник «Big Data» были установлены все сотрудники банка, причастные к этому инциденту.

Результат

Произведено юридическое закрепление обнаруженных доказательств, что позволило руководству банка обратиться в правоохранительные органы.



Круг общения абонента



Близкий круг общения абонента

О компании Group-IB

Group-IB – один из ведущих мировых разработчиков решений для детектирования и предотвращения кибератак, выявления фрода и защиты интеллектуальной собственности в сети.

15 лет практического опыта	**1000+** расследований по всему миру	**$300 млн** было возвращено клиентам благодаря нашей работе	**300+** специалистов и разработчиков

Многолетний опыт Group-IB воплощен в системе раннего обнаружения киберугроз – линейке высокотехнологичных продуктов для мониторинга, выявления и предупреждения киберугроз, основанной на самых актуальных данных киберразведки и глубоком анализе реальных хакерских атак.

Наши продукты

- **Threat Intelligence**
- **Threat Detection System (TDS)**
- **Secure Bank**
- **Secure Portal**
- **Brand Protection**

INTERPOL EUROPOL

Официальный партнёр EUROPOL и INTERPOL

IDC GARTNER FORRESTER

Threat Intelligence от Group-IB – в числе лучших мировых систем согласно рейтингам IDC, Gartner, Forrester

OSCE

Рекомендована Организацией по Безопасности и Сотрудничеству в Европе

Аудит и Оценка рисков

- Тестирование на проникновение
- Исследование уязвимостей
- Выявление фактов компрометации
- Имитация целевых атак (Red Teaming)
- Проверка готовности к реагированию на инциденты (Pre-IR)
- Оценка соответствия

Threat Hunting и Реагирование

- Проактивное выявление угроз
- 24/7 мониторинг и реагирование
- Реагирование “по подписке” *(целевые атаки, утечки и др.)*

Криминалистика

- Криминалистическое исследование
- Анализ вредоносного кода

Расследования

- Целевые атаки
- Инциденты информационной безопасности
- Финансовые и корпоративные преступления

Свяжитесь с нами, чтобы узнать больше

+7 (495) 984 33 64 info@group-ib.ru www.group-ib.ru

GROUP IB