Elcomsoft Cloud eXplorer 1.30: извлечение текстовых сообщений SMS, поддержка расширенных картографических служб из «облака» Google

Москва, Россия – 26 апреля 2017 - Компания «Элкомсофт» обновляет Elcomsoft Cloud eXplorer, криминалистический инструмент для извлечения и просмотра данных, доступных в учётных записях Google Account. В версии 1.30 появилась возможность извлечения текстовых сообщений SMS из «облачных» резервных копий смартфонов Google Pixel, а также устройств под управлением Android O (в предварительной версии). Теперь из «облака» извлекается полная история переписки пользователе посредством текстовых сообщений, отправленных и полученных на всех устройствах, резервные копии которых присутствуют в учётной записи пользователя.

Кроме того, в новой версии продукта история местоположения пользователя отображается в привязке к маршрутам пользователя и к картографическим объектам («дом», «работа», название заведения или организации и т.п.), что помогает существенно ускорить и упростить следственные действия.

На текущий момент резервные копии текстовых сообщений способны создавать устройства Google Pixel и Pixel XL, работающие под управлением Android 7 и более новых версий, а также все устройства, на которых установлена предварительная версия Android O.

Elcomsoft Cloud eXplorer 1.30 доступен как в виде отдельного продукта, так и в составе криминалистического набора Elcomsoft Mobile Forensic Bundle.

Извлечение SMS из «облачных» резервных копий Android

Автоматическое резервное копирование появилось в Android только в версии 6.0. В то же время, даже в Android 7.1.2, являющейся последний на настоящий момент официальной версией Android, механизм резервного копирования далёк от совершенства в сравнении с iOS. Google постепенно исправляет ситуацию, и в предварительной версии Android O (а также на устройствах Google Pixel и Pixel XL, работающих на любой версии Android) появляется резервное копирование SMS в «облако» Google. , а сейчас пока это только на Pixel (но подчеркнуть что N/7).

В отличие от журнала звонков, который синхронизируется с «облаком» с минимальной задержкой, текстовые сообщения сохраняются лишь в составе резервных копий, которые создаются конкретным устройством. Как правило, свежая резервная копия создаётся телефоном не чаще одного раза в сутки во время подзарядки, если устройство подключено к сети Wi-Fi.

В Elcomsoft Cloud eXplorer 1.30 добавлена возможность извлечения текстовых сообщений SMS, которые сохраняются в «облачных» резервных копиях смартфонов Android. Сообщения извлекаются из резервных копий всех совместимых устройств, представленных в «облаке» Google Account. Это позволяет экспертам извлекать потенциально больший объём данных по сравнению с тем, что доступно при исследовании единственного устройства. Доступен сквозной поиск по текстовым сообщениям SMS, извлечённым из всех устройств, зарегистрированных в учётной записи пользователя.

Для доступа к учётной записи Google Account требуется аутентификация посредством логина и пароля пользователя. В Elcomsoft Cloud eXplorer 1.30 поддерживаются в том числе и учётные записи, для которых включена защита по методу двухфакторной аутентификации; в таких случаях потребуется доступ к дополнительному фактору (доверенному устройству, приложению-аутентификатору или доверенному телефонному номеру для получения одноразового кода).

Возможность извлечения и анализа SMS на основе данных Google Account уникальна для Elcomsoft Cloud eXplorer и не встречается в сторонних коммерческих решениях. В настоящее время создавать резервные копии текстовых сообщений способны устройства Google Pixel и Pixel XL, работающие под управлением Android 7 и более новых версий, а также все устройства, на которых установлена предварительная версия Android O.

Привязка к картографическим объектам

В новой версии инструментария представлены существенные улучшения в области обработки данных местоположения. В ECX 1.30 история местоположения пользователя привязывается к маршрутам и данным о картографических объектах. Встроенными инструментами из «облака» Google Account извлекаются маршруты пользователя и делается привязка координат к объектам на карте.

Привязка к картографическим объектам существенно упрощает анализ перемещений пользователя. Без дополнительных усилий эксперт может составить объективное представление об активности пользователя в течение заданного временного промежутка; к примеру, можно увидеть маршрут в формате «Дом – поездка в общественном транспорте – работа – поездка – название ресторана». Такое представление истории местоположения заметно удобнее в процессе расследования в сравнении с традиционным набором цифровых координат, даже если координаты накладываются на карту.

Маршруты

Ещё одним нововведением в ECX 1.30 является поддержка маршрутов пользователя. В версии 1.30 поддерживаются не просто наборы координат, привязанные к карте, а полноценные маршруты с указанием вида транспорта, остановок и посещаемых объектов.

Другие нововведения

В ECX 1.30 существенно улучшена работа раздела Media. Если в предыдущих версиях продукта скачивались только фотографии, то теперь продукт научился извлекать и видеоролики. Полные дубликаты обнаруживаются и удаляются автоматически (полными дубликатами считаются фотографии, попавшие в несколько альбомов, если информация о принадлежности ко всем альбомам сохраняется). Увеличилось количество данных, которые извлекаются EXIF, а на базе данных ориентации изображения программа теперь автоматически разворачивает фотографии. Ускорена генерация уменьшенных изображений в галерее, значительно улучшены фильтры.

ELCOMSOFT
PROACTIVE SOFTWARE

О программе Elcomsoft Cloud eXplorer

Elcomsoft Cloud eXplorer извлекает многие типы данных, включая профиль пользователя, сообщения Hangouts, контакты (в том числе с мобильных устройств), заметки Google Keep, историю поисковых запросов включая историю перехода по найденным ссылкам. Доступны все данные браузера Google Chrome, включая закладки, пароли и сохранённые данные веб-форм; фотографии, календари, данные из Dashboard. Продукт извлекает историю местоположения пользователя, включая данные из всех мобильных устройств, зарегистрированных под исследуемой учётной записью, а также некоторые данные из мобильных устройств под управлением Android.

В состав продукта входит удобный инструмент для просмотра и анализа извлечённых данных. Все двоичные форматы файлов автоматически обрабатываются и выводятся на экран в максимально удобном для просмотра виде. Доступны функции поиска и фильтрации.

Для скачивания доступна бесплатная пробная версия продукта. В бесплатной версии присутствует ряд ограничений: отображаются только 10 записей из каждой категории, а сохранённые пароли маскируются специальными символами.

Стоимость и редакции

Продукт выпускается в стандартной редакции. Стоимость редакции – 129,995 рублей. Продукт доступен как в виде самостоятельного приложения, так и в составе набора Elcomsoft Mobile Forensic Bundle. В состав набора входит ряд продуктов «Элкомсофт» для криминалистического анализа мобильных устройств под управлением Apple iOS, Windows Phone / Windows 10 Mobile и BlackBerry 10. Стоимость набора – 199,995 рублей.

Системные требования

Elcomsoft Cloud eXplorer совместим с 32- и 64-разрядными версиями Windows 7, Windows 8, 8.1, Windows 10, Windows 2008 - 2016 Server.

О компании «ЭлкомСофт»

Компания «ЭлкомСофт» – российский разработчик программного обеспечения и поставщик услуг в области восстановления паролей и данных. Решения компании «ЭлкомСофт» используются корпорациями, входящими в список Fortune 500, а также правительственными организациями, правоохранительными органами и спецслужбами по всему миру. Компания «ЭлкомСофт» является членом Российской Криптологической Ассоциации, имеет статус сертифицированного партнера Microsoft (Microsoft Gold Certified Partner) и Intel (Intel Software Partner). Компания основана в 1990 году, головной офис «ЭлкомСофт» находятся в Москве. Для получения более подробной информации посетите http://www.elcomsoft.ru