Elcomsoft Cloud Explorer 2.10: извлечение данных Google Drive без пароля

Москва, Россия – 17 мая 2018 - Компания «Элкомсофт» обновляет Elcomsoft Cloud Explorer, криминалистический инструмент для извлечения и просмотра данных, доступных в учётных записях Google Account. В версии 2.10 появилась возможность извлечения информации из файлового хранилища Google Drive, в том числе в случаях, когда пароль от учётной записи неизвестен. Для аутентификации без пароля с компьютера подозреваемого извлекается специальный маркер аутентификации. Возможность аутентификации без пароля доступна и для других типов данных. Новый функционал доступен как в Windows редакции, так и в редакции для Mac.

Elcomsoft Cloud Explorer 2.10 доступен как в виде отдельного продукта, так и в составе криминалистического набора Elcomsoft Mobile Forensic Bundle.

Извлечение данных из файлового хранилища Google Drive

Google Drive – популярное «облачное» хранилище, в котором пользователи хранят файлы и документы, а приложения, работающие в телефонах под управлением ОС Android, могут сохранять собственные данные и резервные копии (такие, как резервные копии WhatsApp).

В новой версии Elcomsoft Cloud Explorer добавлена возможность извлечения данных из файлового хранилища Google Drive. Встроенная поддержка Google Drive позволяет использовать Elcomsoft Cloud Explorer в качестве единственного инструмента, извлекающего всю доступную информацию из учётных записей Google.

Для входа в Google Drive может использоваться как стандартный способ с вводом логина и пароля, так и маркер аутентификации, извлечённый из браузера Google Chrome. Кроме того, доступен дополнительный способ авторизации, при котором извлекается специальный маркер аутентификации, создаваемый на компьютере пользователя приложением Google Backup and Sync. Маркеры, созданные приложением Google Backup and Sync, могут использоваться только для доступа к файловому хранилищу, в то время как маркеры из браузера Chrome открывают доступ к многочисленным категориям данным, включающим в себя и файловое хранилище Google Drive.

ELCOMSOFT
PROACTIVE SOFTWARE

Вход в Google Account без пароля

В Elcomsoft Cloud Explorer 2.10 появилась возможность извлекать многие типы данных из «облака» Google даже тогда, когда пароль от учётной записи неизвестен. Для доступа в «облако» без пароля программой используются маркеры аутентификации. Маркер аутентификации – это файл, который сохраняются браузером Chrome в тот момент, когда пользователь входит в учётную запись Google Account при попытке воспользоваться одним из сервисов компании.

Для автоматического извлечения и использования маркеров аутентификации в состав Elcomsoft Cloud Explorer включён новый инструмент под названием Google Token Extractor (GTEX). GTEX сканирует компьютер пользователя и извлекает найденные маркеры аутентификации, позволяя программе успешно подключаться к «облаку» Google. При помощи маркеров для скачивания доступны следующие категории данных: Chrome (история, закладки и пароли), календари, Dashboards, файлы из хранилища Google Drive и Hangouts.

Возможность использования маркеров аутентификации существенно расширяет сферу применения продукта и позволяет обойти дополнительную защиту по методу двухфакторной аутентификации.

О программе Elcomsoft Cloud Explorer

Elcomsoft Cloud Explorer извлекает многие типы данных, включая файлы из хранилища Google Drive, 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. Elcomsoft Cloud Explorer – единственный продукт на рынке, предлагающий встроенную поддержку всех видов двухфакторной аутентификации от Google Prompt до аппаратных ключей FIDO включительно.

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 редакциях для Windows и Mac. Стоимость каждой 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.

Системные требования

Elcomsoft Cloud Explorer в редакции для Windows совместим с 32- и 64-разрядными версиями Windows 7, Windows 8, 8.1, Windows 10, Windows 2008 – 2016 Server. Elcomsoft Cloud Explorer для Mac поддерживает Mac OS X 10.7 и более новые версии системы вплоть до macOS High Sierra.

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» расположен в Москве. Для получения более подробной информации посетите http://www.elcomsoft.ru