ELCOMSOFT QUICK TRIAGE (EQT)

Программное обеспечения для быстрого сбора информации с компьютерных систем

Руководство пользователя

ЭлкомСофт
2026

1. ВВЕДЕНИЕ

Назначение продукта

Elcomsoft Quick Triage (EQT) – специализированный программный инструмент для быстрого извлечения, агрегации и предварительного анализа критически важных данных с исследуемых компьютеров (ОС Windows 10 и Windows 11) и подключённых накопителей.

Целевая аудитория и возможности

Продукт предназначен для экспертов в области цифровой криминалистики, сотрудников правоохранительных органов и специалистов по информационной безопасности, выполняющих сбор цифровых доказательств как на месте происшествия (на выезде), так и в лабораторных условиях.

В основе работы EQT лежит концепция «триажа» – оперативного сбора наиболее значимых артефактов до проведения глубокого криминалистического анализа. Инструмент позволяет извлекать образ оперативной памяти, системные и пользовательские артефакты, историю браузеров, переписку и файлы из сотен различных источников, автоматически объединяя разрозненные данные.

Предупреждение о рисках

EQT поддерживает работу в режиме анализа авторизованной сессии непосредственно на компьютере подозреваемого. Запуск любого программного обеспечения на «живой» (загруженной) операционной системе несёт риски изменения цифровых доказательств. При работе в таком режиме специалисту необходимо строго документировать каждый шаг процесса сбора данных и обязательно фиксировать в итоговом отчёте точную версию используемой программы (доступно в меню Помощь -> О программе).

2. ПРИНЦИП РАБОТЫ

Для минимизации вмешательства в исследуемую систему и обеспечения неизменности цифровых доказательств, EQT запускается специалистом в портативном режиме с внешнего накопителя.

Для успешного сбора данных с загруженной системы требуется выполнение двух условий:

1. Наличие активной, аутентифицированной пользовательской сессии (экран компьютера должен быть разблокирован).
2. Наличие у активного пользователя прав локального администратора.

В процессе работы создаётся **Проект** – набор файлов, размещаемых на внешнем накопителе специалиста. Собранные артефакты и извлечённая информация сохраняются в этот проект. Основной массив данных упаковывается в контейнер открытого формата **VHDX**. Использование открытого формата исключает привязку к конкретному разработчику: собранные данные можно монтировать и исследовать как с помощью самого EQT, так и средствами сторонних криминалистических программ, включая решения с открытым исходным кодом.

3. СИСТЕМНЫЕ ТРЕБОВАНИЯ

Для обеспечения корректной работы программного комплекса Elcomsoft Quick Triage (EQT) как на рабочем компьютере специалиста (в лаборатории), так и на исследуемом ПК, необходимо соблюдение следующих аппаратно-программных условий:

- **Операционная система:** Windows 10 или Windows 11.
- **Процессор и оперативная память:** Минимальные требования к центральному процессору (CPU) и объему оперативной памяти (RAM) полностью совпадают с базовыми системными требованиями, заявленными разработчиком ОС (Microsoft) для установленной версии Windows 10 или Windows 11. Дополнительных вычислительных мощностей для работы самой утилиты не требуется.
- **Аппаратные интерфейсы и накопители:** Специфические требования к встроенному дисковому пространству исследуемого компьютера отсутствуют. Необходим внешний портативный накопитель (флеш-диск или внешний жесткий диск) с объемом свободного места, достаточным для сохранения извлекаемого массива данных. Для обеспечения штатной скорости сбора и записи информации настоятельно рекомендуется наличие хотя бы одного свободного порта стандарта USB 3.0 или выше.

4. УСТАНОВКА, УДАЛЕНИЕ, РЕГИСТРАЦИЯ И СОЗДАНИЕ ПОРТАТИВНОЙ ВЕРСИИ

Установка на компьютер специалиста

Первоначальная установка Elcomsoft Quick Triage производится на рабочий компьютер эксперта (в лаборатории). Процесс установки стандартен и выполняется через Мастер установки.

Ввести лицензионный ключ можно непосредственно в диалоговом окне во время установки либо позже, выбрав в главном меню пункт Помощь -> Регистрация EQT.

Удаление установленного ПО

Для удаления Elcomsoft Quick Triage с компьютера специалиста воспользуйтесь стандартным механизмом Windows по удалению (деинсталляции) установленного ПО через Панель Управления Windows.

Удаление ПО с исследуемого компьютера не требуется, т. к. продукт по определению запускается только с портативного внешнего накопителя – и не устанавливается на исследуемый компьютер.

Устранение проблем (Windows Defender)

Эвристические алгоритмы Защитника Windows (Windows Defender) могут ошибочно идентифицировать компоненты криминалистического ПО как вредоносные и переместить их в карантин (ложноположительное срабатывание). В этом случае необходимо:

1. Открыть приложение **Безопасность Windows** (Windows Security).
2. Перейти в раздел «Защита от вирусов и угроз» -> «Журнал защиты».
3. Найти заблокированный компонент EQT, отменить карантин и выбрать действие «Восстановить» (или «Разрешить на устройстве»).

Создание портативной версии

В целях сохранения целостности улик EQT **не рекомендуется** устанавливать на исследуемый компьютер. Запуск должен осуществляться исключительно с внешнего накопителя.

Для создания портативной версии:

1. Скопируйте папку с установленной программой (по умолчанию: C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft Quick Triage) с компьютера эксперта на подготовленный внешний диск или флеш-накопитель.
2. Подключите внешний накопитель к целевому компьютеру и запустите исполняемый файл EQT из скопированной директории.

5. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ: РЕЖИМ СБОРА ДАННЫХ

Напоминание: Работа с внешнего накопителя на загруженном компьютере подозреваемого (анализ авторизованной сессии) всегда несёт риски изменения системных данных. Тщательно документируйте свои действия.

Шаг 1. Создание проекта

Запустите портативную версию EQT. На главном экране нажмите кнопку **Создать** или перейдите в меню Файл -> Создать новый проект. Укажите путь для сохранения файла проекта. *Внимание:* Путь должен вести строго на ваш внешний накопитель, а не на локальные диски исследуемого ПК.

Шаг 2. Добавление источника данных

В дереве проекта кликните правой кнопкой мыши по названию созданного проекта и выберите **Добавить источник данных**. Введите понятное название источника (например, «начальный_сбор_ноутбук»).

Программа предложит выбрать тип источника:

- **Текущий компьютер:** для сбора данных с активной («живой») системы.
- **Логический диск:** для сбора данных с заранее снятого образа диска (обычно выполняется в лаборатории).
  Примечание: далее в этом разделе рассматривается работа в режиме «Текущий компьютер».

Шаг 3. Аутентификация и работа с DPAPI

EQT попросит выбрать учётную запись пользователя, от имени которой будет выполняться сбор, и запросит ввод её пароля. Пароль необходим для расшифровки пользовательских данных, защищённых системным механизмом Windows DPAPI (сохранённые пароли браузеров, токены, почтовые базы и т. д.).

- Если пароль неизвестен, программа может попытаться подобрать его автоматически, однако на практике вероятность успеха встроенного перебора невелика.

- Процесс сбора можно продолжить и без пароля. В этом случае артефакты будут скопированы, но данные, зашифрованные DPAPI, останутся нечитаемыми.

Шаг 4. Экспорт хэш-сумм паролей

Если пароль неизвестен, вы можете воспользоваться функцией **Экспорт хэшей**. Она позволяет сохранить хэш-суммы учётных записей ОС в отдельные файлы. В дальнейшем эти файлы можно загрузить в специализированный программный комплекс *Elcomsoft Distributed Password Recovery* для проведения высокопроизводительной атаки по восстановлению пароля на мощном лабораторном оборудовании.

Шаг 5. Выбор артефактов

После этапа авторизации программа перейдёт к интерфейсу выбора конкретных артефактов и категорий данных, которые необходимо собрать.

6. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ: ТИПЫ ИЗВЛЕКАЕМЫХ ДАННЫХ

Концепция сбора артефактов

Программный комплекс Elcomsoft Quick Triage (EQT) осуществляет автоматизированный поиск, извлечение и структурирование значимых элементов файловой системы и операционной системы – цифровых артефактов. Данные артефакты позволяют специалисту установить факты активности в системе, выявить хронологию действий пользователя и реконструировать события, предшествующие инциденту.

Внутренняя архитектура продукта классифицирует извлекаемую информацию по форматам представления:

- **Двоичные блоки данных:** фрагменты данных в их оригинальном формате и состоянии («сырые» данные), скопированные с накопителя «как есть».
- **Извлечённые структуры данных (артефакты):** информация, полученная в результате автоматического разбора (анализа) сложных системных баз данных и файлов специализированными модулями EQT.
- **Файлы:** целостные документы и системные файлы, для которых предусмотрены средства просмотра.
- **Текстовые данные:** информация, проиндексированная и доступная для сквозного полнотекстового поиска внутри проекта.

Для удобства анализа и навигации все собираемые артефакты разделены на две глобальные категории: **Системные артефакты** и **Пользовательские артефакты**.

Группа 1: Системные артефакты

Системные артефакты отражают глобальное состояние операционной системы, аппаратного обеспечения и сетевого окружения. Эти данные не привязаны к конкретному профилю пользователя, но важны для понимания общей картины работы устройства и могут помочь установить факт запуска вредоносного программного обеспечения, подключения внешних носителей или несанкционированного изменения системных конфигураций.

1.1 Файловые артефакты операционной системы

В данную подгруппу входят файлы баз данных, системные журналы работы и служебные записи Windows, которые извлекаются из хранилища исследуемого компьютера. Модули EQT осуществляют их независимое чтение и автоматический разбор.

Наиболее значимые системные файловые артефакты:

- **Файлы баз данных Amcache и Shimcache (AppCompatCache):** позволяют установить факт присутствия и времени первого запуска исполняемых файлов в системе, даже если сами файлы были впоследствии удалены.
- **База данных SRUM (System Resource Utilization Monitor):** содержит детализированную статистику об использовании сетевых ресурсов, процессора и батареи конкретными приложениями.
- **Файлы Prefetch (*.pf):** используются для ускорения запуска программ, однако в контексте исследования они позволяют установить факт запуска приложения, путь к исполняемому файлу и хронологию его активности.
- **Журналы событий Windows (Windows Event Logs - .evtx):* системные журналы, фиксирующие широкий спектр событий (аутентификация пользователей, старт и остановка служб, ошибки оборудования).
- **Данные Защитника Windows (Windows Defender) и сторонних антивирусов:** EQT собирает журналы работы, истории обнаружения угроз и данные из карантина множества защитных продуктов (включая Kaspersky, ESET, McAfee, Symantec, Avast, Bitdefender и др.).
- **Системные журналы IIS, DHCP, DNS и логи установки (Setupapi.log):** позволяют выявить сетевую активность и историю обновления драйверов и компонентов.
- **Образ оперативной памяти (Memory Dump):** программа позволяет извлечь файлы pagefile.sys, swapfile.sys, hiberfil.sys, а также сохранить текущий снимок оперативной памяти (в режиме активной сессии), что необходимо для выявления скрытых процессов и извлечения ключей шифрования.

1.2 Реестр Windows (Глобальные настройки)

EQT использует штатный системный механизм VSS для независимого чтения кустов реестра (таких как SYSTEM, SOFTWARE, SAM, SECURITY), что позволяет обходить блокировки файлов операционной системой. Из системного реестра программа автоматически извлекает следующие данные:

- Списки когда-либо подключённых к компьютеру USB-накопителей, Bluetooth-устройств, жёстких дисков и принтеров (позволяет установить факт использования конкретных внешних носителей).
- Конфигурации сетевых интерфейсов и список сетей, к которым подключался компьютер.
- Списки установленных программ, обновлений драйверов и служб.
- Общая информация об операционной системе, включая параметры часовых поясов, статус защиты ОС и списки задач Планировщика Windows.

Группа 2: Пользовательские артефакты

В отличие от системных данных, пользовательские артефакты извлекаются из профиля конкретного пользователя (например, из директорий AppData, Documents и пользовательского куста реестра NTUSER.DAT). Они позволяют установить факты

конкретных действий человека: с кем он общался, какие сайты посещал, какие документы редактировал и какие пароли сохранял.

2.1 Интернет-браузеры

Современные браузеры хранят огромный массив информации о цифровой жизни пользователя. EQT поддерживает сбор и автоматический анализ данных из более чем 60 различных браузеров, разделяя их по используемым платформам:

- **На базе Chromium:** Google Chrome, Microsoft Edge, Yandex Browser, Opera, Vivaldi, Brave, Chromium и десятки других.
- **На базе Mozilla:** Mozilla Firefox, Waterfox, Pale Moon, SeaMonkey.
- **Прочие:** Apple Safari.

Для каждого найденного профиля EQT извлекает: историю посещений (History), сохранённые учётные данные и пароли (Login Data), информацию о загрузках, файлы cookie, данные автозаполнения форм, закладки, локальные хранилища (Local Storage / IndexedDB) и снимки открытых сессий.

2.2 Недавно открытые файлы и каталоги

Данные артефакты позволяют установить, с какими документами пользователь работал непосредственно перед исследованием:

- **Файлы ярлыков (LNK Files) и списки переходов (JumpLists):** автоматически создаваемые операционной системой структуры, которые указывают на расположение локальных и сетевых файлов, к которым обращался пользователь. EQT осуществляет разбор этих структур для извлечения метаданных (дат создания, путей и характеристик целевых файлов).
- **История проводника Windows:** данные о недавних файлах, поисковых запросах в Проводнике и корзине конкретного пользователя.

2.3 Активность приложений (Мессенджеры, Облака, Утилиты)

EQT собирает локальные базы данных, файлы конфигураций и журналы работы для широкого спектра пользовательского программного обеспечения. Это позволяет установить факт использования определённых сервисов и собрать локальные копии пользовательских данных:

- **Мессенджеры и корпоративные чаты:** извлекаются локальные профили, базы данных сообщений, кэши изображений и журналы из Telegram Desktop, Skype, WhatsApp, Viber, Microsoft Teams, Slack, Discord и Signal.
- **Облачные хранилища:** сбор метаданных, списков синхронизации и локальных файлов кэша из Dropbox, Google Drive, OneDrive, MegaSync, pCloud.
- **Программы для работы с файлами и сетью:** извлекаются конфигурации, история подключений и сохранённые сессии FTP/SSH-клиентов (FileZilla, WinSCP, OpenSSH), менеджеров загрузок (BitTorrent, uTorrent), программ удалённого доступа (TeamViewer, AnyDesk, RDP) и файловых менеджеров (Total Commander).

2.4 Виртуальные машины

Наличие виртуальных машин может указывать на попытки скрыть активность или изолировать рабочую среду. EQT автоматически выполняет поиск данных виртуализации:

- Конфигурационных файлов и образов дисков классических гипервизоров (VMware – *.vmdk, *.vmem; VirtualBox – *.vbox, *.vdi; Microsoft Hyper-V – *.vhd, *.vhdx).
- Файлов образов дисков формата.vhdx, используемых подсистемой Windows для Linux (WSL), включая дистрибутивы Ubuntu, Debian, Kali Linux и openSUSE.

2.5 E-мейл клиенты (Электронная почта)

В рамках сбора пользовательских данных инструмент обнаруживает и копирует локальные почтовые базы, позволяющие анализировать переписку в специализированных криминалистических программах. Поддерживается извлечение:

- Локальных хранилищ Microsoft Outlook (файлы *.pst, *.ost, *.nst).
- Профилей и баз данных клиента Mozilla Thunderbird (файлы.sqlite и другие объекты локального хранилища).
- Универсального хранилища встроенных приложений Windows Mail / Calendar.

2.6 Реестр Windows (Пользовательские данные)

Из файла пользовательского куста реестра NTUSER.DAT и файла UsrClass.dat модули программы извлекают специфичные для конкретной учётной записи следы:

- Списки недавно запущенных программ (через ветки BAM и UserAssist), что позволяет установить точные даты активности.
- Историю открытых и сохранённых файлов через стандартные диалоговые окна Windows (Open/Save MRU).
- Списки смартфонов, планшетов и других мобильных устройств, которые подключал именно данный пользователь.
- Информацию о документах, недавно открытых в Microsoft Office, Adobe Acrobat и архиваторах.

7. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ: СОХРАНЕНИЕ И БЫСТРЫЙ АНАЛИЗ ДАННЫХ

Фоновый сбор и отображение в реальном времени

Процесс извлечения улик, инициированный на предыдущем этапе, выполняется в фоновом режиме. Сохранение массива информации может занять продолжительное время, что напрямую зависит от совокупного объема извлекаемых данных и пропускной способности (скорости записи) используемого внешнего накопителя.

Ожидать полного завершения процедуры не обязательно: уже обработанные и сохраненные артефакты незамедлительно появляются в древовидной структуре в левой части интерфейса EQT. Специалист может сразу приступить к их просмотру и изучению, что существенно ускоряет первичный анализ инцидента.

Структура файлов проекта

В целях оптимизации последующего анализа программа распределяет извлеченную информацию по специализированным файлам и директориям внутри созданного проекта:

- **Образ оперативной памяти:** сохраняется в виде единого обособленного файла в корневой директории проекта.
- **Учетные данные ОС:** метаданные локальных учетных записей экспортируются в файл hashes.pwdump. Данный файл аппаратно независим, и его можно открыть в специализированном комплексе *Elcomsoft Distributed Password Recovery* для проведения высокопроизводительной атаки по восстановлению паролей доступа к Windows.
- **Поисковый индекс:** текстовая информация и служебные связи артефактов индексируются и помещаются в локальную базу данных db.sqlite.

Организация хранилища (VHDX-контейнеры)

Основной массив извлекаемых файлов (файловая система, документы, базы данных) помещается в подкаталог container текущего проекта. Для хранения используется открытый формат виртуальных дисков VHDX. При этом EQT создаёт не один монолитный файл, а модульную структуру:

1. Data.vhdx — содержит непосредственно скопированные блоки данных (сами файлы).
2. Meta.vhdx — содержит системные метаданные (атрибуты файлов, временные метки создания/модификации/доступа, права доступа и списки контроля доступа).

Мгновенный доступ к контейнерам

Для удобства работы специалиста непосредственно в каталоге проекта создаются системные ярлыки в виде виртуальных папок Data и Meta. Они ведут напрямую к содержимому соответствующих VHDX-контейнеров. Это позволяет оперативно «зайти» в контейнер средствами стандартного Проводника Windows и просмотреть его содержимое без выполнения дополнительных операций по ручному монтированию виртуальных дисков.

По завершении процедуры фонового сбора специалист может либо продолжить экспресс-анализ непосредственно на месте работы с исследуемым компьютером, либо выполнить безопасное извлечение внешнего накопителя для проведения углубленного исследования материалов в лабораторных условиях.

8. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ: ПОДРОБНЫЙ АНАЛИЗ СОБРАННЫХ ДАННЫХ

После доставки внешнего накопителя с результатами криминалистического сбора в лабораторию, эксперту доступны три основных сценария работы с полученным проектом.

Способ 1. Анализ средствами комплекса EQT

Оптимальный метод для быстрого поиска, фильтрации и навигации по структурированному дереву артефактов. Для загрузки собранных материалов необходимо запустить EQT на лабораторном компьютере и выполнить команду главного меню: Файл -> Открыть проект/дело, после чего указать путь к файлу проекта на накопителе.

Способ 2. Монтирование контейнера через интерфейс EQT

Специалист может смонтировать виртуальный диск в операционную систему лаборатории, используя встроенные инструменты программы.

- Для подключения контейнера в виде логического диска используется команда главного меню: Контейнер -> Смонтировать контейнер.
- Для корректного завершения работы с диском применяется команда: Контейнер -> Размонтировать контейнер.
- В случае непредвиденного повреждения файловой структуры виртуального диска (например, из-за внезапного отключения питания при первоначальном сборе), в программе предусмотрен механизм восстановления целостности: Контейнер -> Восстановить контейнер.

Способ 3. Использование стороннего программного обеспечения

Поскольку результаты сбора упаковываются в контейнеры открытого стандарта VHDX, полученные образы можно открыть, смонтировать и детально проанализировать в любом стороннем криминалистическом программном обеспечении, поддерживающем работу с данным форматом.

Примечание к архитектуре контейнеров

Необходимо учитывать, что механизм сбора EQT физически разделяет сами файлы и их метаданные на два независимых образа (Data.vhdx и Meta.vhdx). На текущий момент полностью корректное слияние (бесшовное объединение) этих контейнеров для отображения оригинальных атрибутов осуществляет только сам EQT. Тем не менее, разработанные компанией Elcomsoft спецификации механизма разделения являются полностью открытыми. Это предоставляет сторонним разработчикам криминалистического ПО возможность интеграции аналогичной логики объединения контейнеров в свои программные продукты.

9. ПРИЛОЖЕНИЯ: ОГРАНИЧЕНИЯ И ОСОБЕННОСТИ РАБОТЫ

Для корректного функционирования программы в режиме «живой» системы обязательным предварительным условием является наличие активной, разблокированной сессии пользователя, обладающего правами локального администратора. Работа в данном режиме сопряжена с неотъемлемыми рисками изменения цифровых следов в исследуемой операционной системе, что требует строгой фиксации действий специалиста. Важно учитывать, что в портативном режиме комплекс не производит модификацию целевых накопителей, не устанавливает системные службы и не осуществляет обход паролей на вход в систему или снятие полнодискового шифрования в обход загруженной ОС. Полнота извлекаемой информации напрямую зависит от уровня привилегий активной сессии, а при отсутствии корректного пароля пользователя защищённые системным механизмом DPAPI данные будут извлечены, но останутся криптографически нечитаемыми.

Скорость сбора данных и формирования образа оперативной памяти ограничивается исключительно пропускной способностью интерфейсов подключения и скоростью записи используемого специалистом внешнего накопителя. Также необходимо принимать во внимание архитектурную особенность формирования результатов: извлечённые файлы и их системные метаданные физически разнесены в независимые виртуальные образы Data.vhdx и Meta.vhdx. На данный момент бесшовное слияние этих контейнеров для

отображения оригинальных атрибутов при анализе гарантированно поддерживается только внутренними средствами комплекса EQT, тогда как стороннее программное обеспечение может обрабатывать и монтировать их лишь по отдельности.

10. ТИПОВЫЕ ОШИБКИ И ДИАГНОСТИКА

Программа не запускается с внешнего носителя

Убедитесь, что запуск исполняемого файла осуществляется от имени администратора. Проверьте, не заблокированы ли порты или запуск неизвестного ПО корпоративными политиками безопасности исследуемого компьютера.

Отсутствуют права локального администратора

Сбор данных в рамках текущей сессии невозможен. Необходимо авторизоваться под учётной записью с соответствующими привилегиями либо использовать альтернативные методы исследования (изъятие накопителя для лабораторного анализа).

Недостаточно свободного места на внешнем носителе

Процесс формирования VHDX-контейнера будет остановлен во избежание повреждения файловой системы. Требуется подключить накопитель большей ёмкости, создать новый проект и запустить процедуру сбора заново.

Смонтированный VHDX-контейнер не открывается или повреждён

Воспользуйтесь штатной функцией программы: перейдите в меню Контейнер и выберите Восстановить контейнер. Если сбой был вызван внезапным отключением питания или извлечением диска во время записи, часть последних файлов может быть утрачена.

Пароль DPAPI неизвестен или введён неверно

Продолжите процедуру сбора, оставив поле пароля пустым; зашифрованные данные скопируются в исходном виде. Выполните экспорт хэш-сумм паролей для последующего проведения атаки на лабораторном оборудовании.

Антивирусное ПО или Windows Defender удалил компонент программы

Откройте интерфейс управления антивирусной защитой на исследуемом компьютере и перейдите в раздел журнала или карантина. Найдите заблокированный файл комплекса EQT, отмените помещение в карантин и выберите действие «Восстановить» (или «Разрешить на устройстве»).

11. ИНФОРМАЦИЯ О РАЗРАБОТЧИКЕ И ТЕХНИЧЕСКОЙ ПОДДЕРЖКЕ

Программный комплекс Elcomsoft Quick Triage (EQT) разработан и поддерживается компанией ООО «Элкомсофт».

Юридический и фактический адрес: Российская Федерация, 129085, г. Москва, Звездный бульвар, д. 21, офис 615.

Техническая поддержка: При возникновении технических сбоев или вопросов по эксплуатации продукта, решения для которых не описаны в разделе «Типовые ошибки и диагностика», специалист может обратиться в службу технической поддержки разработчика следующими способами:

- По электронной почте: support@elcomsoft.ru
- По телефону +7 495 974-11-62