Подготовил:

Холопов Алексей Васильевич - кандидат юридических наук, доцент, советник юстиции.

Заведующий криминалистической лабораторией Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации

Научно-технические средства и методы цифровой криминалистики

В Окинавской хартии глобального информационного общества, принятой в 2000 г., отмечено, что развитие информационных технологий, компьютерных информационно-коммуникационных систем революционным образом воздействует на образ жизни людей, их образование и деятельность, взаимодействие правительств и гражданского общества, то есть того, что именуется средой обитания. Все это с логической неизбежностью приводит (и уже привело) к значительным изменениям во всех сферах и областях жизни, в том числе как в преступности, так и в методах борьбы с ней[1].

В докладе правительству РФ о деятельности прокуратуры за 2016 год генеральный прокурор Ю.Я. Чайка отметил, что есть проблемы с противодействием киберпреступности. Он отмечает резкий рост и крайне малый процент раскрытия преступлений, совершенных с помощью использования IT-технологий. За прошлый год было раскрыто всего 8% мошеннических действий.

Также генеральный прокурор России Юрий Чайка заявил, что в России с 2013 по 2016 год количество случаев киберпреступности выросло в шесть раз — до 66 тыс. Данное заявление генпрокурор сделал на встрече

[1] Окинавская хартия глобального информационного общества. Принята на о. Окинава 22 июля 2000 г. // Дипломатический вестник. 2000 № 8 С. 51–56. См.: Бангкокская декларация “Партнёрство во имя будущего” (принята в г. Бангкоке 21.10.2003) // Дипломатический вест-ник. 2003; Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895) // СПС ГАРАНТ.

руководителей прокурорских служб стан БРИКС, посвященной вопросам противодействия киберпреступности. Встреча прошла в Бразилии.

Термин "forensics" является сокращенной формой "forensic science", дословно "судебная наука", то есть наука об исследовании доказательств — именно то, что в русском именуется криминалистикой. Русский термин "форензика" означает не всякую криминалистику, а именно компьютерную.

Некоторые авторы разделяют компьютерную криминалистику (computer forensics) и сетевую криминалистику (network forensic).

Основная сфера применения форензики — анализ и расследование событий, в которых фигурируют компьютерная информация как объект посягательств, компьютер как орудие совершения преступления, а также какие-либо цифровые доказательства[2].

В США и в западной Европе данная область знаний называется digital forensics, что очень часто переводят как цифровая криминалистика. Digital forensics или computer forensics в первую очередь ориентированы на поиск, извлечение, проверку подлинности уголовно релевантных электронных данных, то есть на то, что в отечественной криминалистике называется использованием знаний о механизмах следообразования, и, во вторую очередь, на придание полученным электронным данным формы доказательства. При этом различие уголовно-процессуальных подходов в государствах англосаксонской правовой системы и в нашей стране приводит к тому, что предмет исследования digital forensics в нашем представлении о предмете криминалистики сужается только до методов судебной компьютерно-технической экспертизы и использования специальных (в основном технических) знаний в уголовном процессе[3].

Киберпреступление – это общественно опасное деяние, совершаемое в киберпространстве, посягающее на общественную безопасность,

---

[2] См.: Компьютерная криминалистика (форензика) // URL: https://habr.com/company/pentestit/blog/338378/ (дата обращения 25.05.2018)

[3] См.: Мещеряков В.А. Цифровая криминалистика // Библиотека криминалиста. Научный журнал. - М.: Юрлитинформ, 2014, № 4 (15). - С. 231-241.

собственность, права человека, другие охраняемые законом отношения, необходимым элементом механизма подготовки, совершения, сокрытия и отражения которого является компьютерная информация, выступающая в роли предмета или средства преступления[4].

Классификация киберпреступлений.

Конвенция Совета Европы о киберпреступности[5] говорит о четырех типах компьютерных преступлений «в чистом виде», определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

1. Незаконный доступ — ст. 2 (противоправный умышленный доступ к компьютерной системе либо ее части);
2. Незаконный перехват — ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);
3. Вмешательство в данные — ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);
4. Вмешательство в систему — ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

Классификация по уровню квалификации пользователя (субъекта преступления) и его возможности в выборе «криминальных информационных технологий»[6]:

---

[4] Шевченко, Е. С. О криминалистической трактовке понятия «киберпреступность» // Информационное право. 2014. № 3 (39). С. 29 – 32

[5] См.: «Конвенция о компьютерных преступлениях" (ETS N 185) [рус., англ.] (заключена в г. Будапеште 23.11.2001) с изм. от 28.01.2003

[6] См.: Шевченко, Е. С. Тактика производства следственных действий при расследовании киберпреступлений : Диссертация на соискание ученой степени кандидата юридических наук. Специальность 12.00.12 - криминалистика ; судебно-экспертная деятельность ; оперативно-розыскная деятельность / Е. С. Шевченко ; науч. рук. Е. П. Ищенко. -М., 2016. - 249 с.

1) Преступления, совершённые пользователем с применением простейших информационных технологий, когда информационно-телекоммуникационные технологии используются примитивно. Противоправное деяние может быть совершено даже «случайным» пользователем, т. е. не требует наличия у преступника криминальных навыков и профессиональных знаний в области информационно-телекоммуникационных технологий:

- незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, совершённые с использованием сети Интернет (в случае получения информации при официально разрешённом доступе к ней); незаконное собирание или распространение информации о частной жизни лица, составляющей его личную или семейную тайну, в том числе персональных данных, совершённое с использованием сети Интернет;
- возбуждение ненависти либо вражды, а равно унижение человеческого достоинства, совершённые с использованием сети Интернет;
- нарушение авторских и смежных прав, совершённое с использованием сети Интернет (в данном случае – незаконное использование экземпляров компьютерных программ, баз данных, аудиовизуальных и литературных произведений);
- мошенничество, совершённое с использованием фиктивных брачных интернет-агентств; незаконное предпринимательство в сфере предоставления услуг Интернет;
- вымогательство, совершённое с использованием сети Интернет;
- кибертерроризм (спонсирование, пропаганда террористической деятельности).

2) Преступления, совершённые опытным пользователем с применением информационных технологий среднего уровня. Преступление способен совершить профессиональный непрограммирующий пользователь, т. е.

совершение противоправного деяния предполагает владение преступником некоторыми профессиональными знаниями или криминальными навыками:

- неправомерное подключение к сети оператора эл. связи с целью уйти от оплаты полученных услуг Интернет;
- незаконное изготовление, хранение, распространение, рекламирование и (или) публичная демонстрация информации, запрещённой к свободному обороту, совершённые с использованием сети Интернет;
- нарушение тайны переписки, телефонных переговоров, почтовых или иных сообщений, передаваемых по сети Интернет;
- нарушение авторских и смежных прав, совершённое с использованием сети Интернет (незаконное распространение экземпляров компьютерных программ, баз данных, аудиовизуальных и литературных произведений);
- продажа несуществующих товаров, оказание фиктивных услуг и предложение фиктивной надомной работы, совершённые с использованием Интернет-магазинов или рекламных электронных сообщений;
- привлечение средств на ложные (в том числе несанкционированные) благотворительные цели;
- мошенничество в интернет-казино, букмекерских конторах (на тотализаторах), розыгрышах лотереи и на аукционах;
- финансовые «интернет-пирамиды»;
- кибертерроризм.

3) Преступления, совершённые пользователем-специалистом с применением сложных информационных технологий, предполагающие использование информационно-телекоммуникационных технологий и методов: их адаптация либо модификация применительно к целям преступной деятельности при наличии у преступников высокой квалификации, глубоких профессиональных знаний, умений и навыков в

рассматриваемой сфере. Такое преступление способен совершить исключительно пользователь-профессионал:

- неправомерное получение и использование чужих учётных данных (логинов и паролей) для доступа в сеть Интернет;
- частичная подмена собственных учётных данных чужими (MAC и IP-адреса) для неправомерного доступа в сеть Интернет;
- создание, использование и распространение сетевых вредоносных компьютерных программ;
- незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, совершённые с использованием сети Интернет (в случае получения информации без официально разрешённого доступа к ней);
- нарушение авторских и смежных прав, совершённое с использованием сети Интернет (в данном случае – незаконное создание экземпляров компьютерных программ, баз данных, аудиовизуальных и литературных произведений);
- мошенничество в электронных платёжно-расчётных системах сети Интернет;
- хищение электронных реквизитов и сбыт поддельных кредитных либо расчётных карт;
- вымогательство, совершённое с использованием сети Интернет (с использованием вредоносных программ);
- кибертерроризм.

Киберпространство – это область взаимодействия информационных систем различного уровня, включающих следующие элементы: компьютерные системы, сети (как глобальные, так и локальные), компьютерные программы пользователей, а также данные, циркулирующие в перечисленных элементах.

Структура «кибернетического пространства»:

1. Глобальная информационная сеть (например, Интернет)
2. Локальная сеть (система ЭВМ)
3. Средства вычислительной техники (персональный компьютер, большая ЭВМ, специализированное вычислительное устройство)
4. Элемент средства вычислительной техники как отдельный носитель информации
5. Информационная структура первого уровня (логический носитель информации)
6. Информационная структура второго уровня (файл)
7. Информационная структура третьего уровня (запись файла)
8. Элементарная информационная группа (слово - 16, 32, 64 или более бит, размещенных рядом друг с другом, байт, бит).

Особенности преступлений, совершаемых в киберпространстве.

– повышенная скрытность совершения преступлений, что становится возможным благодаря специфике сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т. п.);

– трансграничный характер сетевых преступлений, когда преступник, объект криминального посягательства, потерпевший могут находиться на территориях разных государств;

– высокая квалификация преступников в области компьютерных технологий, интеллектуальный характер преступной деятельности;

– нестандартность, сложность, многообразие и динамичное обновление способов совершения преступлений и применяемых специальных средств;

– возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно, возможность объединять относительно слабые ресурсы многих отдельных компьютеров в мощное орудие совершения преступления;

– многоэпизодичный характер криминальных действий с множеством потерпевших;

– неосведомлённость потерпевших о том, что они подверглись преступному посягательству (воздействию);

– дистанционный характер преступных посягательств, отсутствие физического контакта преступника и потерпевшего; невозможность предотвращения и пресечения преступлений данного вида традиционными криминалистическими средствами[7].

Виртуальные следы – это данные о совершении действий в информационном пространстве технических устройств, их сетей и систем, такие как: создание, включение, удаление, внесение изменений, активация, открывание.

Виды виртуальных (кибер) следов.

1. Сетевые виртуальные следы – это данные, сохраненные провайдером (информация о сеансе связи, статистические или динамические IP-адресные журналы регистрации провайдера в сети Интернет, телефонные номера, скорость передачи сообщения, исходящие сеансы связи, типы использованных протоколов и т. д.), LOG-файлы.
2. Локальные виртуальные следы – следы, остающиеся на компьютерах, используемых для совершения преступных действий, либо через которые проходит или поступает информация (таблицы размещения файлов FAT, NTFS и др., системные реестры операционных систем, отдельные кластеры магнитного носителя информации, файлы и каталоги хранения сообщений электронной почты, файлы конфигурации программ удаленного доступа и иное)[8].

Источники виртуальных следов.

[7] Осипенко, А. Л. Сетевая компьютерная преступность: теория и практика борьбы: Монография. Омск: Омск. акад. МВД России, 2009. С. 109 – 110.

[8] См.: Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. 2002. № 1. С. 4–12

1. Электронный почтовый ящик. Здесь могут быть оставлены виртуальные следы в виде переписки по вопросам финансирования терроризма.

2. Интернет-сайт. Обычно это популярные ресурсы в сети Интернет.

3. Профиль в социальных сетях. В ходе анализа уголовных дел по финансированию терроризма было выявлено, что информация, находящаяся в социальной сети («ВКонтакте», «Одноклассники» и др.), чаще становится объектом преступного посягательства по мотивам мести, из хулиганских побуждений, нежели в корыстных целях. Это выделяет ее среди остальных видов.

4. Счет в электронных платежных системах («Qiwi-кошелек», «Яндекс.Деньги», Perfect Money и др.).

5. База данных (абонентов операторов связи, ГИБДД и др.).

6. Локальная сеть. Возможность доступа к ресурсам (программам, файлам, папкам и др.) всех соединенных между собой посредством кабелей (телефонных линий, радиоканалов) компьютеров.

7. Сетевые устройства (роутеры, маршрутизаторы и т.д.).

8. Компьютер. Жесткий диск содержит информацию о его включении, применении разных материалов, отправке счетов, выполнении иных манипуляций. Благодаря работе памяти компьютера сведения об активности ресурсов операционной системы сохраняются, поэтому их можно использовать как источник доказательств в уголовном процессе.

9. Устройства хранения компьютерной информации (флешки, мобильные винчестеры и т.д.)

10. Средства мобильной связи (как правило, применяются операционные системы Android и Apple в силу обширной распространенности). Лица, причастные к финансированию терроризма, могут оставить следы

использования мобильных устройств в виде информации о соединениях между абонентами и (или) абонентскими устройствами[9].

Запись с камер системы видеонаблюдения в случае обнаружения места совершения неправомерных действий субъекта киберпреступления.

Сокрытие виртуальных следов.

Анонимайзеры.

Средства анонимизации и работа с интернет-сервисами через прокси-серверы. Это требует определенной настройки компьютера и чаще всего приводит к замедлению скорости обмена данными, отключает определенные функции (например, не будут работать Flash-анимация и ActiveX-содержимое) и ограничивает активность пользователя (в браузере нельзя будет открывать файлы для просмотра и загружать их через встроенный менеджер закачек) из-за необходимости соблюдения приватности. Кроме того, вполне вероятно, что работа под прокси будет недолгой: адреса этих серверов активно блокируются для предотвращения массовых рассылок спама, DDoS-атак, несанкционированных проникновений и т. д.

Альтернатива анонимайзерам.

VPN Whoer.net лишен всех перечисленных выше недостатков анонимайзера: VPN работает быстро, не режет скорость вашего провайдера, не показывает рекламу, стабильно работает, обладает списком IP-адресов разных стран, шифрует весь трафик в обе стороны и не записывает логи.

Tor, децентрализованная сеть прокси-серверов. В составе программы есть анонимайзер TCP/IP-трафика и прокси-фильтр содержимого веб-страниц, который дополнительно обеспечивает анонимность. Весь трафик шифруется, и его невозможно перехватить на стороне провайдера, поскольку маршруты пересылки пакетов делятся на цепочки переходов между узлами сети,

[9] Абрамова Алёна Алексеевна Значение виртуальных следов в расследовании финансирования терроризма // Общество: политика, экономика, право. 2017. №4. URL: https://cyberleninka.ru/article/n/znachenie-virtualnyh-sledov-v-rassledovanii-finansirovaniya-terrorizma (дата обращения: 27.05.2018).

которые постоянно изменяются (каждые десять минут). В настоящее время Tor функционирует за счет порядка 2500 распределенных серверовнодов, к которым производится попеременное «многослойное» подключение с шифрованием.

Дарк нет (англ. DarkNet, с англ. — «скрытая сеть», «тёмный интернет», «теневой интернет», также — Dark Web) — скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов. Анонимная «сеть», не связанных между собой, виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

Даркнет отличается от других распределённых одноранговых сетей, так как файлообмен происходит анонимно (поскольку IP-адреса недоступны публично), и, следовательно, пользователи могут общаться без особых опасений и государственного вмешательства.

Многие теневые сети требуют установки специального программного обеспечения для получения доступа к сети.

Существуют такие популярные теневые сети как:

Tor — это одна из самых популярных программ для анонимных сетей, которая также используется для доступа в даркнет.

I2P

RetroShare

Freenet

GNUnet (при использовании опции «топология F2F»)

Аппаратные средства уничтожения компьютерной информации. Программно-аппаратные комплексы экстренного удаления данных с физических носителей компьютерной информации.

Противодействие анонимайзерам.

Осенью 2016 года полиция Швеции совместно с коллегами из других стран провела международную операцию «Титан». Результат? Поймано 3000 покупателей наркотиков в сети Tor.

Основатель крупнейшей даркнет-площадки Silk Road попался из-за своей забывчивости. Росс Ульбрихт прекрасно скрывался и шифровался, но однажды использовал тот же ник, что и на старых форумах, где ранее разместил вакансию в поисках сотрудника на другой проект.

Ульбрихта арестовали в библиотеке, где он сидел с ноутбука на Silk Road под аккаунтом администратора. Также вычислили посылку с девятью поддельными документами, которые Ульбрихт планировал использовать для аренды серверов для Silk Road, и установили его место жительства.

Чаще всего пользователей даркнета ловят на внешней активности. Которая начинается в Tor и заканчивается в реальном мире.

Но пользователя даркнета поджидают и другие угрозы конфиденциальности.

1. Взлом аккаунтов на сайтах даркнета

Взломать аккаунт на сайте в даркнете в среднем проще, чем на площадках вроде e-Bay или Amazon. Хакеры (и белые, и черные) пользуются этим. Они получают контроль над аккаунтом и некоторое время работают от имени его прежнего владельца.

Тот даже может не успеть никого предупредить, ведь сообщения, отправленные с «левого» аккаунта, в даркнете смотрятся особенно подозрительно. А другие каналы связи в этой сфере используются нечасто.

К тому же после взлома аккаунта хакер получает доступ к старой переписке владельца. Так что установка кодовых фраз или просьба привести факты из прежнего общения не спасает.

Фактически, крадётся личность пользователя, и от её лица можно наделать многое.

Реальный владелец аккаунта не способен ничего доказать без деанонимизации. Не покажет же он личную фотку, номер телефона или профили в соцсетях.

2. Загрузка вирусов и вредоносных скриптов

Сайты даркнета могут заражать вирусами. Почему бы и нет? Они ничем особо не отличаются от обычных веб-сайтов. Например, вредоносный скрипт позволит узнать реальный IP-адрес пользователя или перехватить его трафик без взлома аккаунта.

Преимущество заражения сайтов – массовость атаки. Если аккаунты обычно ломают по одному, то здесь можно получить сразу весь трафик или IP-адреса пользователей, заходивших на сайт в определённый промежуток времени.

Методы выявления незаконных действий в киберпространстве[10].

- **Перехват и исследование трафика**

  В работе ИТ-специалистов анализ сетевого трафика – один из основных методов диагностики и поиска неисправностей. Возможности этого метода велики. Поэтому и в правоохранительной деятельности он должен использоваться как можно шире. На основе анализа содержимого, а также статистики сетевого трафика можно определить и доказать совершение пользователем многих действий в сети, а также получить информацию об устройстве программ, информационных систем и сетей.

- **Исследование статистики трафика**

  Статистика прошедшего трафика собирается на многих устройствах. Все без исключения маршрутизаторы, а также многие иные коммуникационные устройства имеют встроенные функции для сбора разнообразной статистики.

- **Исследование логов веб-сервера**

[10] См.: Федотов Н.Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – 432 с.

Лог – это журнал автоматической регистрации событий, которые фиксируются в рамках какой-либо программы. Обычно каждому событию соответствует одна запись в логе. Обычно запись вносится сразу же после события (его начала или окончания). Записи эти складываются в назначенный файл самой программой либо пересылаются ею другой, специализированной программе, предназначенной для ведения и хранения логов. Как понятно из определения, в логах могут регистрироваться абсолютно любые события – от прихода единичного ethernet-фрейма до результатов голосования на выборах президента. Форма записи о событии также целиком остается на усмотрение автора программы. Формат логаможет быть машинно-ориентированным, а может быть приспособлен для чтения человеком.

- **Исследование системных логов**

  Логирование событий в операционной системе является одной из трех составляющих безопасности. Имеется в виду модель «AAA» – authentication, authorization, accounting – аутентификация, авторизация, аудит. Запись всех событий, связанных прямо или косвенно с безопасностью системы, и составляет сущность аудита. Логирование само по себе не препятствует злоумышленнику получить несанкционированный доступ к информационной системе. Однако оно повышает вероятность его выявления, а также последующего нахождения и изобличения злоумышленника. Также логирование способствует выявлению уязвимостей защищаемой системы.

- **Исследование логов мейл-сервера и заголовков электронной почты**
- **Установление принадлежности и расположения IP-адреса**

  Почти в каждом уголовном деле, связанном с сетью Интернет, присутствовала такая задача: по известному IP-адресу установить использующий его компьютер и местоположение этого компьютера.

  Как правило, цепочка доказательств выглядит именно таким образом:

(преступление) – (IP-адрес) – (компьютер) – (человек)

При помощи различных технических средств фиксируется IP-адрес, с которого осуществлялась криминальная деятельность. Затем устанавливается компьютер, который использовал данный IP-адрес, факт такого использования закрепляется экспертизой. Затем следует доказать, что этим компьютером в соответствующее время управлял подозреваемый.

Вторая из упомянутых задач – найти компьютер по его IP-адресу – и будет предметом рассмотрения в данной главе.

- **Установление принадлежности доменного имени**
- **Принадлежность адреса электронной почты**
- **Кейлогеры.**

Клавиатурный почерк - поведенческая биометрическая характеристика, которую описывают следующие параметры:

Скорость ввода - количество введенных символов разделенное на время печатания

Динамика ввода - характеризуется временем между нажатиями клавиш и временем их удержания

Частота возникновение ошибок при вводе

Использование клавиш - например, какие функциональные клавиши нажимаются для ввода заглавных букв.

Движение мыши и т.д.

Первоначальный этап обнаружения незаконных действий в киберпространстве должен обнаруживаться и фиксироваться специальным программами, обеспечивающими кибербезопасность страны, предприятия и т.д.

Классификация научно-технических средств цифровой криминалистики:

Аппаратные средства:

Устройства для клонирования жестких дисков и других носителей (в том числе в полевых условиях).

Специализированная переносная лаборатория "RM3" Мульти-интерфейсное средство извлечения и анализа данных в условиях выезда на место расследования.

Функциональность. Исследователь может анализировать данные НЖМД (Накопитель на жёстких магнитных дисках), с помощью любого специального программного обеспечения, установленного на RM3. Устройство поддерживает любые программы просмотра и любые специальные программы анализа, такие как Encase, FTK, ILOOK и др.

Извлечение файлов любой ОС. Устройство извлечет файлы любой ОС и любые типы разделов с НЖМД. Устройство гарантирует выполнение передачи бит за битом всего, что есть на исследуемом НЖМД, включая удаленные файлы, свободные области и файловое пространство. Конвертер Link MASSter IDE-USB/Firewire может быть использован для извлечения областей HPA НЖМД стандарта ATA.

Совместимость Копирования и Анализа. Может копировать и изучать в среде Windows исследуемый НЖМД или НЖМД, на котором находятся извлеченные данные.

Копирование НЖМД. Устройство будет копировать НЖМД, использующие интерфейсы P-ATA (с адаптером), SCSI, SATA, USB, 1394B и SAS. Возможность горячей замены НЖМД. Поддерживается горячая замена НЖМД. НЖМД можно заменять во время включенного электропитания устройства.

Методы извлечения данных. Возможно извлечение данных с одного или, одновременно, с двух исследуемых НЖМД методом Single Capture (посекторного копирования) и методом Linux DD (

копирование блоками). Дополнительно возможны не специальные (не для проведения расследования) быстрые методы копирования (IQCOPY, MultiMASSter), когда выполняется быстрое копирование только файлов данных.

Информация о Деле. Записывается информация о Деле и исследователе, проводящем анализ.

Очистка НЖМД Wipe Out. Очистка НЖМД, подключенного на место НЖМД исследователя, проводится по спецификации DOD для очистки НЖМД, или по определенному пользователем шаблону.

Отчет о копировании. Печатает или сохраняет отчет о ходе копирования на любом принтере или на любом устройстве хранения данных.

ImageMASSter Solo-3 Forensic Kit - комплект технических средств для копирования данных.

Комплект аппаратных блокираторов записи "ForensicPC Ultimate Write Block Kit" – специально разработанный портативный комплект аппаратных блокираторов записи, используемых при проведении судебного дублирования различных накопителей.

Переносные компьютеры с комплексом программных и аппаратных средств, ориентированных на исследование компьютерной информации в полевых условиях.

Специализированная переносная лаборатория FREDDIE. Сервер для криминалистов FREDDIE снабжен устройством UltraBay 3 Write Protected Imaging Bay для получения образа исследуемого диска в режиме "защиты от записи". Комплекс FREDDIE представляет из себя гибкую масштабируемую систему для получения и анализа компьютерных улик.

Аппаратные и программные средства для исследования мобильных телефонов (SIM-карт), навигаторов, плееров и т.д.

UFED 4PC – универсальный аппаратно-программный комплекс для криминалистических исследований, дающий возможность извлекать, декодировать и анализировать цифровые данные, полученные из мобильных устройств, на существующем ПК или ноутбуке. Комплекс поставляется с набором приложений UFED, периферийными устройствами и принадлежностями, нужными для успешного проведения исследований. UFED 4PC может работать как автономно, так и со сторонним программным обеспечением.

UFED Touch Ultimate представляет собой наиболее мощное решение для извлечения, декодирования, анализа данных и составления отчетов, специально сконструированное с учетом поддержки высокопроизводительных устройств. Комплекс позволяет выполнить извлечение данных на физическом, логическом уровнях и на уровне файловой системы, а также восстановление паролей (даже удаленных) с самых разнообразных устройств, включая устаревшие и мобильные телефоны, смартфоны, портативные устройства GPS и планшетные компьютеры. Благодаря собственному аппаратному оборудованию, встроенному аккумулятору, интуитивно понятному графическому интерфейсу и сенсорному экрану, UFED Touch Ultimate ускоряет процесс расследования и полностью отвечает требованиям мобильной криминалистики.

XRY - комплекс исследования информации с мобильных устройств, таких как мобильные телефоны, смартфоны различных производителей, GPS навигаторы, планшеты и 3G модемы.

Eclipse Screen Capture Kit предназначен для фиксации пользовательской информации с экранов мобильных телефонов, GPS навигаторов, Tablet PC и других портативных устройств, экраны которых могут быть сфотографированы.

Аппаратные средства для исследования локальных сетей.

Fluke Networks WiFi AirCheck - анализатор Wi-Fi сети.

Функциональные возможности WiFi AirCheck:

- Автоматическое тестирование одной кнопкой
- Вывод списка точек доступа в каждом канале в полосах частот 2,4 и 5 ГГц
- Сведения о точке доступа
- Статус авторизации точки доступа
- Обнаружение местонахождения точек доступа и клиентов по уровню сигнала
- Вывод списка сетей
- Тестирование возможности подключения к беспроводной сети
- Проверка соединений
- Использование канала и помехи в нем
- Подробности о клиенте

Стационарные программно-аппаратные комплексы.

Forensic Workstation - программно-аппаратный комплекс для компьютерно-технических исследований.

- представляет мощную вычислительную систему, построенную на базе новейших компьютерных технологий, с широким набором интерфейсов для съема информации с блокировкой записи (IDE/SATA, SAS, USB), с встроенным RAID-массивом большой емкости;
- используется для криминалистического исследования компьютерных носителей информации, и мобильных устройств специализированным программным обеспечением, таким как Encase, Passware Kit Forensic и и многое другое.

Аппаратные средства восстановления данных.

Visual NAND Reconstructor - является универсальной платформой для Chip-Off восстановления данных и криминалистического анализа информации с поврежденных накопителей с флэш памятью.

Программные средства.

Программы поиска и обнаружения виртуальных следов в киберпространстве.

Программа X1 Social Discovery - поиск и сбор данных из социальных сетей и Web ресурсов. Программный продукт собирает вместе в одно целое детальный медиа контент из соц.сетей и Web данные. Решение X1 Social Discovery экономит экспертам огромное количество времени благодаря автоматизированной и одновременной работе по сбору информации из различных акканутов в социальных сетях.

Работает со следующими ресурсами:

Facebook, Twitter, Instagram, YouTube, Tumblr, Web pages & websites, Gmail, YahooMail, Outlook.com, AOL Mail, Internet Message Access Protocol (IMAP).

Passware Recovery Kit Forensic включает в себя более 30 модулей восстановления паролей, объединённых в единый пользовательский интерфейс. Для восстановления сложных паролей используются передовые методы ускорения.

Программа Defacto - это решение предназначенное для экспресс-инвентаризации программного обеспечения, фактически установленного на жестком диске компьютера. Результаты представляются в виде таблицы, в которую сведены сведения об авторе, названии программы, ее рыночной стоимости, статусе (коммерческая, условно-бесплатная, бесплатная). Бесплатные программы отображаются зеленым цветом, платные — красным, пробные (shareware) — фиолетовым.

NetAnalysis программа для восстановления и анализа артефактов интернет-браузера. NetAnalysis также имеет уникальную функцию для быстрой идентификации возможных сайтов детской порнографии, критерии поиска, введенные пользователем, паролями и именами пользователей и доступом к онлайн-хранилищу.

Network E-mail Examiner - программный продукт предназначен для экспертного анализа архивов электронной почты в корпоративной сети.

Porn Detection Stick представляет собой флэш-накопитель, с помощью которого происходит поиск картинок и видео порнографического содержания на вашем компьютере. По окончании процесса сканирования создается отчет с перечнем файлов с предполагаемым порнографическим содержанием. Porn Detection Stick также сканирует удаленные картинки и удаленную кэш память интернет-браузеров, поэтому не удастся скрыть какую-либо интернет активность.

Мобильный криминалист - универсальный программный комплекс для исследования мобильных устройств, извлечения данных из облачных хранилищ и анализа биллингов операторов сотовой связи. Программа позволяет обходить блокировку экрана, находить пароли на зашифрованные резервные копии, извлекать данные из самых надежных приложений, а также восстанавливать удаленную информацию. Данные из мобильных устройств, облачных хранилищ и биллинги операторов показаны вместе в удобном для использования интерфейсе с возможностью их глубокого анализа во встроенных аналитических секциях программы.

XAMN Аналитическое программное обеспечение для выявления взаимосвязей между данными, извлеченными из мобильных устройств Это комплект аналитического программного обеспечения, разработанный исключительно для сопоставления данных, извлеченных из смартфонов, планшетов и других мобильных устройств посредством экспертных инструментов. Дает возможность распознавания соединений, объединения отчетов и предоставления их в хронологическом формате, создания логических схем и нанесения геопозиционных данных на карту.

Программы для проведения компьютерно-технических экспертиз.

X-Ways Forensics – это интегрированный комплекс, позволяющий оперативно решать практически весь спектр задач компьютерной экспертизы и расследования ИТ инцидентов, от съема данных до

составления отчетов. Благодаря этому повышается эффективность работы экспертов, существенно сокращаются сроки проведения исследований.

Основные функции и возможности X-Ways Forensics

- Съем и восстановление данных
- Просмотр и анализ данных
- Поиск и индексирование
- Хэширование

Forensic Toolkit® (FTK®) является признанным мировым стандартом в области компьютерной экспертизы. Одобренная судами программная платформа для проведения расследования осуществляет расширенный анализ информации с криминалистической точностью, дешифрует и взламывает пароли. Программа FTK создана для проведения быстрого анализа данных с возможностью масштабирования для использования в больших компаниях.

EnCase ® Forensic это локальное программное обеспечение для проведения компьютерно-технической экспертизы, являющееся по сути международным стандартом поиска цифровых улик и предоставления данных в суд. EnCase ® Forensic позволяет экспертам получать данные с помощью широкого спектра готовых фильтров и модулей, выявлять потенциальные доказательства путем криминалистического анализа информации, содержащейся на жестком диске, и подготавливать полные отчеты о полученных результатах, сохраняя при этом надежность и целостность полученных доказательств.

Belkasoft Evidence Center облегчает получение, поиск, анализ, хранение и передачу цифровых улик, находящихся внутри компьютеров и мобильных устройств. Программа быстро извлечет цифровые улики из различных источников путем анализа жестких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий iOS, Blackberry и Android, UFED, JTAG и chip-off дампов. Evidence Center автоматически проанализирует источник данных и представит наиболее

значительные улики для обзора, подробного изучения или включения в отчет.

Позволяет обнаружить более 800 типов артефактов, включая более 100 мобильных приложений, все основные форматы документов, браузеры, email-клиенты, дюжины графических и видеоформатов, программы обмена мгновенными сообщениями, социальные сети, системные файлы, файлы реестра, P2P приложения, приложения для обмена файлами и т. д. Извлекает данные из всех основных операционных систем, как компьютерных, так и мобильных: Windows, Linux, macOS, iOS, Android, Windows Phone, Blackberry.

Camera Ballistics выявляет аномалии в каждом изображении и использует эту информацию для создания описания сенсора устройства. Сенсор является частью каждой цифровой камеры, собирая свет в миллионы пикселей и преобразуя его в изображение. Из-за различий в размерах и материале, каждый пиксель может вести себя по-разному, делая каждый датчик уникальным. Это верно даже между устройствами той же марки и модели. Именно эти различия, генерируемые сенсором, позволяют создать неповторимый отпечаток и связать его с конкретной камерой.

Таким образом, обеспечение кибербезопасности и расследование киберпреступлений с помощью цифровой криминалистики возможно только с использованием специальных знаний и научно-технических средств.