УДК 616-78: 343.98 https://doi.org/10.33619/2414-2948/55/21

ОБЗОР ТЕХНИК КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКИ

©Ваценко А. А., *ORCID: 0000-0002-6681-1872, SPIN-код: 8905-1450,*
Национальный исследовательский Томский государственный университет,
г. Новосибирск, Россия, vatsenkoandrey@gmail.com

DIGITAL FORENSICS TECHNIQUES OVERVIEW

©Vatsenko A., *ORCID: 0000-0002-6681-1872, SPIN-code: 8905-1450,*
National Research Tomsk State University,
Novosibirsk, Russia, vatsenkoandrey@gmail.com

Аннотация. В данной статье рассматривается важный вопрос применения криминалистической техники в компьютерной криминалистике. Рассматриваются основные существующие на сегодняшний день техники компьютерной криминалистики, такие, как отслеживание в режиме реального времени, песочница, восстановление данных и пароля и так далее. Приводятся достоинства и недостатки существующих методов и даются рекомендации по развитию техник компьютерной криминалистики в будущем. Формируются выводы по проблеме применения криминалистической техники в компьютерной криминалистике.

Abstract. This article discusses the important issue of the use of forensic technology in computer forensics. The basic techniques of computer forensics existing today, such as real-time tracking, sandboxing, data and password recovery, and so on, are examined. The advantages and disadvantages of existing methods are given and recommendations are made on the development of computer forensics techniques in the future. Conclusions are drawn up on the problem of using forensic technology in computer forensics.

Ключевые слова: криминалистика, компьютерные технологии, восстановление, методы.

Keywords: forensics, computer technology, recovery, methods.

Введение

Во всем мире в целом и в Российской Федерации в частности особую актуальность приобретает проблема преступлений в компьютерной сфере. При этом преступники все чаще используют информационные технологии в преступных целях, совершают квалифицированные «бесконтактные» преступления, говоря компьютерным языком, удаленным доступом. В таких ситуациях значительно уменьшается количество традиционных трасологических следов, но в то же время появляется большое количество цифровых следов преступления. В этой связи общество и государство должны предпринимать упреждающие шаги на предотвращение, пресечение, раскрытие и расследование информационных преступлений на новой технологической базе.

Центральным звеном в таком противодействии должна стать компьютерная криминалистика как отрасль знаний, умений и навыков, набор компетенций, обеспечивающих деятельность по выявлению информационных преступлений, криминалистическому исследованию электронной доказательственной информации. Для любого специалиста по компьютерной криминалистике крайне важно изучить как можно

Т. 6. №6. 2020
https://doi.org/10.33619/2414-2948/55

больше методов криминалистической техники. Это не только максимизирует шансы справиться с широким спектром ситуаций, но также позволяет быстрее находить решения.

Результаты и обсуждение

Рассмотрим основные техники компьютерной криминалистики.

Live Response. Используется при обнаружении, контроле и устранении угрозы в работающей системной среде. В традиционной компьютерной криминалистике берутся снимки памяти и накопителей в качестве образов и выполняем анализ этих образов в изолированной среде. Конечно, это может привести к засорению конвейера анализа, поскольку создание изображений далеко не является эффективным по времени процессом. Это где живая криминалистика вступает в игру. В отличие от традиционной компьютерной криминалистики, криминалистическая экспертиза имеет дело с активными угрозами во время выполнения. Вы можете думать о судебной экспертизе как об активном ответе, в отличие от пассивной природы традиционной криминалистики [1]. Живая экспертиза полезна, если необходимо бороться с угрозой на месте. Следует отметить, что разница между традиционной криминалистикой и живой криминалистикой заключается только во времени отклика; вам все равно придется выполнить те же шаги по выявлению, количественной оценке и устранению угрозы. Живая экспертиза обеспечивает практически мгновенный доступ к разделам реестра, системным учетным записям пользователей, действующим соединениям и объектам памяти. Сценарии живой криминалистики недолговечны. Таким образом, чтобы добиться успеха, нужно сосредоточиться на сужении источника угрозы. Это означает, что вместо того, чтобы грубо форсировать ваш путь к выявлению проблемы, вы должны искать в системе «обычные подозрительные» файлы, такие как каталоги TEMP. В Windows хорошим способом инициирования оперативной криминалистики является пик в каталоге APPDATA активного пользователя, особенно в папке ROAMING. Распространенным примером живой криминалистики является анализ системной памяти. Выделив некоторые подозрительные процессы, можно приступить к анализу кода указанных процессов.

Восстановление данных. Это один из наиболее типичных параметров, с которыми может столкнуться криминалист. Поскольку наша жизнь становится все более управляемой данными, большинство не может позволить себе потерять эти данные навсегда. Сюда могут входить личные данные, включая семейные фотографии и видео, или профессиональные данные, такие как документы, конфиденциальная информация о компании и тому подобное. Восстановление данных обычно принимает одну из двух форм: восстановление на месте, где можно использовать инструменты для восстановления данных путем исправления ошибок дисков; или восстановление только для чтения, которое не исправляет ошибки в исходной точке отказа, а хранит восстановленные файлы в другом месте на диске [2]. Довольно много людей случайно удаляют свои файлы. Но удаленные файлы редко удаляются навсегда; система хранит их на диске до тех пор, пока не потребуется место для нового файла. Это означает, что в течение определенного периода времени вы можете восстановить удаленные файлы. Обычно для этого требуется утилита, аналогичная TestDisk.

Восстановление пароля. Пароль может обеспечить надежную защиту конфиденциальных данных или информации. Но в не столь редком случае, когда он теряется или администратор забывает об этом, пароль также может быть неприятным. В таких случаях восстановление пароля — ваш лучший выбор для восстановления ваших файлов [1]. Восстановление пароля может быть достигнуто путем взлома пароля с помощью грубой силы, которая пробует все возможные комбинации, разрешенные для этого пароля. В

Т. 6. №6. 2020
https://doi.org/10.33619/2414-2948/55

большинстве случаев это может занять много времени. Можно использовать более разумные методы, чтобы существенно сократить количество возможных паролей. Проблема может усугубиться, если файлы также зашифрованы. Во время уголовных расследований правоохранительные органы часто видят защищенные паролем файлы в системе подозреваемого. Доступен широкий спектр утилит для открытия таких файлов. Среди них — Passware, инструмент, используемый правоохранительными органами для взлома файлов, защищенных паролем.

Вскрытие файлов. Это метод криминалистики, который использует содержимое файла, а не метаданные файла, чтобы найти или восстановить указанный файл. Как обсуждалось выше, когда файл удаляется, это не обязательно означает, что он был удален с диска. Обычно операционная система просто теряет свой дескриптор файла, иначе называемый метаданными файла. Таким образом, вы не можете получить доступ к файлу через файловую систему, так как теперь он не знает о существовании самого файла. Восстановление таких файлов на основе их содержимого называется разделением файлов. Вырезание файла извлекает значимые структурированные данные из неструктурированной, нераспределенной части диска. Это наиболее полезно, когда записи файла или каталога повреждены или отсутствуют.

Фильтрация файлов. Распространенный метод криминалистической экспертизы, используемый для поиска только релевантных файлов путем фильтрации не относящихся к делу артефактов. *Обзор.* В своей карьере криминалисты часто сталкиваются со значительным объемом данных, совершенно не имеющих отношения к существу дела. Часто ищутся конкретные файлы, что означает просеивание множества несвязанных артефактов. Известная фильтрация файлов делает это легко; вместо того, чтобы исключать все файлы, которые не имеют отношения к делу, вы начинаете с некоторых известных данных соответствующего файла. Это делает процесс исключения намного быстрее. Известная фильтрация файлов использует популярные криптографические хеши MD5 или SHA1 в сочетании со значениями хеш-файлов установочных файлов приложения. Затем он ищет соответствующий хеш в файловой системе. Основным недостатком известной фильтрации файлов является то, что она может работать, только если хэши полностью совпадают. Это означает, что, если соответствующие файлы даже слегка повреждены, этот метод становится бессильным [3]. *Пример.* Известный файловый фильтр (KFF) используется в утилитах компьютерной экспертизы, таких как Forensic Toolkit (FTK). Он использует криптографический хэш MD5. Используемые хэши либо генерируются пользователем, либо взяты из Национальной справочной библиотеки программного обеспечения (NSRL), поддерживаемой NIST. KFF используется для поиска известных файлов.

Поиск строки и ключевого слова. В цифровой криминалистике используется поиск по строкам и ключевым словам, который может помочь идентифицировать соответствующие данные, а также источник потенциальных угроз. *Обзор:* этот метод предшествовал самой компьютерной криминалистике. Задолго до того, как у нас появились цифровые файлы, специалисты-криминалисты анализировали бумажные документы, чтобы найти специальные фразы или слова, имеющие отношение к их запросу. Сегодня мы называем эти строки и ключевые слова. Поиск этих специальных последовательностей символов может значительно ускорить судебные расследования, особенно если набор данных достаточно велик. Важным моментом здесь является выбор хороших ключевых слов и строк. Например, если вы хотите найти файл, содержащий инструкции по рисованию портретов, избегайте использования термина «инструкции» в своем поиске; вместо этого сосредоточьтесь на «портрете», поскольку у вас могут быть другие файлы, содержащие слово «инструкции», в то время как

Т. 6. №6. 2020
https://doi.org/10.33619/2414-2948/55

очень немногие файлы включают «портрет» [2]. *Пример:* поиск по ключевым словам является одним из основных методов, используемых в анализе вредоносных программ, так как он может помочь классифицировать происхождение вируса. Вообще говоря, мы используем поиск по строкам и ключевым словам все время, чтобы сузить объекты, представляющие интерес, например, в случае поиска Google, поиска видео на YouTube и так далее.

Анализ заголовка. Позволяет исследователям анализировать заголовки электронной почты, которые могут указывать на IP-адрес исходного электронного письма, а также исправлять задержки при доставке электронной почты. *Обзор:* почтовые клиенты могут использоваться для проникновения в чью-либо систему, если принимающая сторона не проявляет осторожности. Большинство клиентов делают похвальную работу по выявлению таких подозрительных электронных писем сами, которые они затем могут либо перенести в раздел спама, либо полностью удалить с сервера. Тем не менее, есть вероятность заражения вирусом по электронной почте. В прискорбных случаях, таких как эти, анализ заголовка используется в качестве первого средства определения, откуда пришло электронное письмо. Заголовок электронного письма содержит некоторые полезные метаданные, такие как IP-адрес источника, а также имя компьютера. Этот IP-адрес может быть использован для отслеживания преступника [4]. *Пример:* специалисты-криминалисты просматривают почтовый ящик жертвы, если они считают, что источник вируса находится там. Затем инструменты, доступные онлайн, используются для анализа заголовков подозрительных электронных писем, так как ручное определение заголовков является трудоемким. Почтовые клиенты имеют разные способы доступа к заголовкам, которые вы можете найти здесь, а также, посмотрев руководство Google по заголовкам сообщений.

Анализ временной шкалы. Анализ событий в хронологическом порядке, которые либо привели, либо последовали за основным исследуемым событием. *Обзор:* плохие события не происходят в вакууме. Существует цепь событий, предшествующих плохому происшествию, и часто бывает полезно выяснить, что это были за события. Анализ временной шкалы обеспечивает именно это, он использует временные метки и другие описательные по времени артефакты для отображения всех событий, происходящих в системе, в хронологическом порядке. Это позволяет экспертам-криминалистам определить причинно-следственную связь, что крайне важно для выявления источника проблемы [5]. *Пример:* многие инструменты судебной экспертизы включают анализ графика времени, чтобы поддержать их продукты. Например, Autopsy имеет инструмент анализа временной шкалы на основе графического интерфейса, который использует веб-артефакты и прочие извлеченные данные для построения временной шкалы событий.

Анализ графического изображения. Извлечение информации, такой как метаданные и геотеги, из изображений для исследовательских целей. В мире, который становится все более зависимым от визуальных данных, анализ изображений можно без преувеличения считать важнейшим навыком для криминалистов. Большинство изображений, помимо очевидных данных о пикселях, также содержат различные другие информационные фрагменты. Анализ графических изображений представляет собой совокупность различных методов, используемых для извлечения значимой информации из таких изображений. Эта информация может представлять собой метаданные изображения, тип MIME и т. Д. Иногда в метаданных изображения фотографий можно найти геотеги — данные о локализации на основе GPS, которые сообщают вам долготу и широту места, где была сделана фотография. Вы также можете определить, было ли подделано изображение, с помощью анализа уровня ошибок (ELA). Этот метод сканирует изображение на предмет уровней сжатия; две области,

Т. 6. №6. 2020
https://doi.org/10.33619/2414-2948/55

имеющие существенно разные результаты, указывают на то, что изображение было отредактировано [6]. В связи с растущей популярностью анализа изображений в цифровой криминалистике, вы можете найти ряд онлайн-инструментов, предназначенных для профессионалов. Одним из таких инструментов является автоматический анализатор изображений Ghiro. Это бесплатно, но вы не можете использовать его для пакетного анализа. Анализ изображений считается ключевым навыком для криминалистов и экспертов в области безопасности, который используется для исследования видеоматериалов CCTV, спутниковых изображений и даже инфракрасных изображений.

Корреляция событий. Анализ журналов активности сети для установления цепочки событий. Корреляция событий является одним из наиболее широко используемых методов цифровой криминалистики. Это потому, что это часто первый шаг в судебных расследованиях. По сути, специалистам по безопасности поручено анализировать журналы активности конкретной сети (каждая сеть содержит файлы журналов, детализирующие веб-трафик). Это говорит им обо всем, что им нужно знать о сетевом трафике и о том, какие события произошли до критического сбоя или нарушения безопасности. Корреляция событий часто используется в качестве начального шага в отслеживании источника взлома. Поскольку журналы содержат полную хронологическую временную шкалу событий, зарегистрированных в сети, они могут помочь в определении причины нарушений безопасности.

Криптоанализ / Стегоанализ. Расшифровка данных, которые были скрыты с помощью криптографии или стеганографии. Расшифровка данных является одним из старейших исследовательских подходов, намного предшествовавших появлению компьютеров. Однако в цифровую эпоху современные методы сокрытия данных с использованием криптографии и стеганографии возродили интерес к этой области. Криптоанализ — это процесс расшифровки данных, которые были зашифрованы с использованием шифров. Точно так же, стеганализ — это исследование поиска скрытых данных в обычных сообщениях или файлах. Разница между ними заключается в способе кодирования сообщений; данные, скрытые с помощью криптографии, не имеют смысла, что означает, что можно определить, было ли сообщение зашифровано. С другой стороны, стеганография скрывает данные в несекретных сообщениях. Это могут быть текстовые файлы, аудиофайлы или, чаще всего, изображения [4]. Криптоанализ распространен при попытке расшифровки сообщений, которые были перехвачены правоохранительными органами. Типичные методы включают в себя дешифрование методом «грубой силы» и атаки «человек посередине». Вы можете найти список популярных инструментов криптоанализа здесь.

Песочница. Запуск подозрительных программ или кода в изолированной среде. Песочницы — это безопасные виртуальные среды, которые можно использовать для тестирования программ из непроверенных источников. Использование песочницы может помочь в сдерживании угроз, которые поставляются в комплекте с ненадежным программным обеспечением. Песочницы обычно назначают часть аппаратных ресурсов для запуска виртуальных машин, включая ядра процессора, память и дисковое пространство; можно подумать о песочнице как об особом случае виртуализации. Ключевое различие между ними заключается в том, что, в отличие от виртуализации, «песочница» сильно ограничивает сетевой доступ к гостевой операционной системе, что ограничивает возможности программы по распространению любых вирусов, которые она может содержать [6]. Инструменты песочницы, такие как Sandboxie, используются судебно-медицинскими экспертами для выявления и сдерживания потенциально враждебных программ. Он эмулирует довольно элементарную операционную систему на базе Windows.

Т. 6. №6. 2020
https://doi.org/10.33619/2414-2948/55

Вы можете безопасно запускать любые программы внутри Sandboxie и, если в какой-либо из них будет обнаружено вредоносное ПО, ваша операционная система не будет подвержена его влиянию.

Сетевой анализ. Захват и анализ пакетов, поступающих и проходящих через определенную сеть. Сетевой анализ или анализ пакетов — это метод, используемый исследователями для захвата пакетов данных, передаваемых по сети. Эти пакеты затем регистрируются и анализируются. Инструменты, используемые для таких целей, известны как анализаторы сети или, просто, анализаторы. Снифферы перехватывают пакеты данных и, в зависимости от их возможностей, могут открывать эти пакеты, чтобы обнаружить необработанные данные, передаваемые внутри. Теоретически, можно отслеживать полный трафик сети, используя инструменты сниффинга. Одним из самых популярных сетевых анализаторов является Wireshark. Он доступен бесплатно, и разработчики даже сделали его исходный код доступным. Wireshark делает все: захват пакетов, регистрацию трафика и анализ отдельных пакетов.

Сбор данных. Использование криминалистических методов на необычно больших наборах данных для поиска значимых закономерностей [2]. Компании, большие и маленькие, начинают двигаться в направлении оцифровки своих операций. Это означает, что объем данных, которые они содержат, быстро увеличивается. И с увеличением объема данных увеличивается и сложность их анализа. Интеллектуальный анализ данных означает манипулирование большими объемами данных для извлечения из них полезной информации. Несмотря на то, что он широко используется для распознавания тенденций в бизнесе, интеллектуальный анализ данных также нашел свое применение в компьютерной экспертизе. При изучении чрезвычайно подробных наборов данных судебно-медицинские специалисты должны сначала идентифицировать соответствующие данные с помощью таких методов интеллектуального анализа данных, как сокращение, кластеризация и т. д. Хотя интеллектуальный анализ данных не может рассматриваться как чисто криминалистический метод сам по себе, он может использоваться в качестве механизма экономии времени при работе с неуправляемо большими объемами данных. Знание методов интеллектуального анализа данных может помочь судебным экспертам в проведении срочных расследований.

Визуализация доказательств. Визуализация судебных доказательств с целью выявления ценных моделей в ходе расследования. Расширение анализа временной шкалы (обсуждается в части 1 данной статьи), визуализация доказательств пытается представить доказательства в визуальном формате. Поскольку изображения более интуитивны, чем текст, визуализация доказательств может значительно ускорить процесс расследования, в дополнение к выявлению новых подходящих моделей. Это косвенно связано с извлечением данных, так как оно также работает лучше всего, когда количество доказательств слишком велико для регулярного судебного анализа. Специалисты-криминалисты начали воспринимать визуализацию как важную судебно-медицинскую практику. Инструменты цифровой криминалистики, такие как EnCase, используются для сбора судебных доказательств, и затем эти свидетельства передаются в механизм распознавания образов (пример: SKLean для Python). Наконец, результаты от движка передаются в библиотеку визуализации или построения графиков, которая представляет визуальное представление свидетельства.

Выводы

Таким образом, при компьютеризации процесса расследования преступлений следователь, анализируя меняющуюся следственную ситуацию, должен переработать огромный массив информации, выделить из нее криминалистически значимую и не

Т. 6. №6. 2020
https://doi.org/10.33619/2414-2948/55

допустить при этом ошибок. При расследовании конкретного дела в компьютер в диалоговом режиме вводятся сведения о составе и способе преступления, предмете преступного посягательства, потерпевшем и др. После обработки на экран выдаются рекомендации, которые могут быть использованы в планировании расследования, позволяют выбрать данные по эпизодам и по участникам, подсказывают, как осуществить конкретное следственное действие, произвести поиск и сопоставление эпизодов, фамилий, дат и прочее.

Список литературы:

1. Колесникова Д. А., Селезнев А. В. Особенности технико-криминалистического исследования документов // Современная наука: теория и практика: мат. I междунар. науч.-практ. конф. Т. 2., Ч. 1. Общественные науки. Ставрополь, 2011. С. 103-106.

2. Пастухов П. С., Лосавио М. Использование информационных технологий для обеспечения безопасности личности, общества и государства // Вестник Пермского университета. Юридические науки. 2017. №36. С. 231-236.

3. Федотов Н. Н. Форензика - компьютерная криминалистика. М.: Юридический мир, 2007. С. 28.

4. Алабужев И. Г., Зезянов В. П., Соснин К. В. Об объективизации и визуализации информации, получаемой в результате производства следственных действий // Криминалистика, криминология и судебные экспертизы в свете системно-деятельностного подхода. 2003. С. 53-60.

5. Аверьянова Т. В, Белкин Р. С, Корухов Ю. Г, Российская Е. Р. Криминалистика. М.: Норма, 2001. С. 959.

6. Алабужев И. Г. Визуализация показаний допрашиваемого посредством компьютерного моделирования: автореф. дисс. ... канд. юрид. наук. Ижевск, 2004. 30 с.

References:

1. Kolesnikova, D. A., & Seleznev, A. V. (2011). Osobennosti tekhniko-kriminalisticheskogo issledovaniya dokumentov. *In Sovremennaya nauka: teoriya i praktika: Mat. I mezhdunar. nauch.-prakt. konf. V. 2. Part 1. Obshchestvennye nauki, Stavropol, 103-106*. (in Russian).

2. Pastukhov, P. S., Losavio, M. (2017). Ispol’zovanie informatsionnykh tekhnologii dlya obespecheniya bezopasnosti lichnosti, obshchestva i gosudarstva. *Vestnik Permskogo universiteta. Yuridicheskie nauki,* (36), 231-236. (in Russian).

3. Fedotov, N. N. (2007). Forenzika – komp’yuternaya kriminalistika. Moscow. (in Russian).

4. Alabuzhev, I. G., Zezyanov, V. P., & Sosnin, K. V. (2003). Ob ob”ektivizatsii i vizualizatsii informatsii, poluchaemoi v rezul’tate proizvodstva sledstvennykh deistvii. *In Kriminalistika, kriminologiya i sudebnye ekspertizy v svete sistemno-deyatel’nostnogo podkhoda, 53-60*. (in Russian).

5. Averiyanova, T. V, Belkin, R. S, Korukhov, Yu. G, & Rossiiskaya, E. R. (2001). Kriminalistika. Moscow. (in Russian).

6. Alabuzhev, I. G. (2004). Vizualizatsiya pokazanii doprashivaemogo posredstvom komp'yuternogo modelirovaniya: autoref. J.D. diss. Izhevsk, 30. (in Russian).

Работа поступила
в редакцию 08.05.2020 г.

Принята к публикации
11.05.2020 г.

Ссылка для цитирования:

Ваценко А. А. Обзор техник компьютерной криминалистики // Бюллетень науки и практики. 2020. Т. 6. №6. С. 167-174. https://doi.org/10.33619/2414-2948/55/21

Cite as (APA):

Vatsenko, A. (2020). Digital Forensics Techniques Overview. *Bulletin of Science and Practice, 6*(6), 167-174. (in Russian). https://doi.org/10.33619/2414-2948/55/21