

5. Компьютерно-техническая экспертиза

Место и роль КТЭ

Общее

С точки зрения места в раскрытии и расследовании уголовного дела компьютерно-техническая экспертиза (КТЭ) ничем не отличается от других видов экспертиз.

Компьютерная информация, являющаяся объектом или средством совершения компьютерного преступления, хотя и может быть предназначена для обычных людей, но исследовать ее могут только специалисты. Практически любое обращение с компьютерной информацией требует специальных знаний. А источником таких знаний, согласно закону, может быть только специалист или эксперт. Устанавливать факты, касающиеся компьютерной информации, можно только на основании экспертизы. Отсюда и особая роль КТЭ при расследовании.

Несведущим людям может показаться, что многие действия над компьютерной информацией не требуют специальных знаний. Действительно, современные компьютеры и ПО предназначены для широкого круга пользователей. И пользователи (в том числе малоквалифицированные) успешно выполняют на них обычные задачи, такие как редактирование текстов, отправка и получение электронной почты, создание и распечатка рисунков. Зачем же тут специальные знания?

Чтобы найти ответ, давайте немного вспомним историю развития вычислительной техники. В 1960-х годах для работы на ЭВМ следовало не просто иметь специальные знания, но и быть программистом. Затем были созданы программы для решения некоторых типовых задач, и навык программиста перестал быть обязательным. Но управление работой ЭВМ по-прежнему было недоступно для неспециалиста. В 1980-х годах появились первые персональные компьютеры, научиться работать с которыми мог обычный человек. Обучение тем не менее все же требовалось. И это ограничивало рынок сбыта персональных компьютеров. Но ПО стремительно развивалось. И одним из главных направлений его развития являлось обеспечение простого, наглядного и относительно привычного интерфейса для неквалифицированного пользователя. Ориентация на массового покупателя — залог успеха для коммерческого ПО. Некоторые современные ОС делают освоение персонального компьютера довольно простой задачей, поскольку сводят «многомерное» управление к выбору из списка действий, а вместо технических терминов оперируют менее

адекватными, но более привычными для простого человека аналогами: «документ» вместо «файл», «папка» вместо «каталог», «отправка сообщения» вместо «установление SMTP-сессии» и так далее. Многие операции автоматизированы за счет снижения функциональности. Многие другие операции просто скрыты от пользователя. Все это стало возможным благодаря развитию программного обеспечения. Биты в современных компьютерах точно такие же, как и 40 лет назад. И набор арифметическо-логических операций процессора мало изменился. Кажущаяся простота — это не более чем поднятие пользователя на более высокий уровень абстрагирования от технической реализации операций. Такое поднятие вовсе не означает понимания. Напротив, простота управления достигается за счет снижения понимания сути производимых действий.

Приведем простую аналогию. В начале XX века управление автомобилем было неразрывно связано с его техобслуживанием (довольно трудоемким) и починкой. В течение нескольких десятилетий вождение автомобиля оставалось профессией, которой положено было учиться. По мере развития техники автомобиль превратился в потребительский товар, доступный самому широкому кругу. Ездить на машине перестало означать ее обслуживать. У некоторых современных моделей даже не открывается капот, поскольку пользователю это не нужно. В автошколах уже перестали учить устройство двигателя. Нужны ли специальные знания для современного автолюбителя? Почти нет. А для проведения экспертизы автотехники?

Для пользования современным компьютером специальные знания действительно не требуются. Это происходит благодаря высокой степени отчуждения пользователя от технической реализации обработки информации. Между «верхним слоем», то есть графическим интерфейсом пользователя, и «нижним слоем», то есть битовыми массивами данных, лежит много промежуточных «слоев» из форматов, протоколов, драйверов, API, системных функций и прикладных программ. На каждом из них остаются следы. Каждый «слой» вносит свою лепту в изменение компьютерной информации, в образование цифровых следов. Для поиска и изучения этих следов специальные знания нужны. Из-за отчуждения пользователя от реализации большая часть информации от него скрыта. Почти все процессы происходят не так, как они представляются пользователю.

Кто может быть экспертом?

Неоднократно автору приходилось сталкиваться с вопросами на эту тему. Причем вопросы задавали следователи. А у вас есть лицензия на производство экспертизы? А ваше предприятие имеет сертификат экспертного учреждения? А у вас есть допуск на ознакомление с материалами уголовных дел?

Ответы на все подобные вопросы содержатся в Уголовно-процессуальном кодексе. «Эксперт — лицо, обладающее специальными знаниями и назначенное в порядке, установленном настоящим Кодексом, для производства судебной экспертизы и дачи заключения» (ст. 57 УПК). Как видно из этого определения, в законе отсутствуют требования о наличии определенного образования, опыта работы, какой-либо сертификации или лицензирования. Это, конечно же, не означает, что экспертом может быть любой. Специальные знания необходимы, но их наличие определяется следователем самостоятельно. Если следователь признал какое-либо лицо экспертом, поручив ему проведение экспертизы, то подозреваемый или потерпевший может лишь заявить отвод эксперту (ст. 198 УПК) и не более.

Когда эксперт или экспертное учреждение являются государственными, то они руководствуются также законом «О государственной судебно-экспертной деятельности в Российской Федерации» (№73-ФЗ). В нем предусматривается аттестация экспертов из государственных экспертных учреждений.

На деятельность иных, то есть негосударственных экспертов и экспертных учреждений действие этого закона распространяется частично. Какого-либо лицензирования, обязательной сертификации или аттестации для негосударственных экспертов не предусмотрено.

Какое же учреждение является экспертным, а какое — нет? Кодекс говорит, что «экспертное учреждение — государственное судебно-экспертное или иное учреждение, которому поручено производство судебной экспертизы в порядке, установленном настоящим Кодексом» (ст. 5 УПК). То есть любое негосударственное учреждение, которому следователь или суд счел возможным поручить проведение экспертизы (поручить на законных основаниях, естественно), автоматически становится экспертным.

Ни в УПК, ни в упомянутом законе, не содержится никаких отдельных упоминаний компьютерно-технической экспертизы, поэтому КТЭ производится по общим принципам.

По традиционным видам судебной экспертизы авторитет государственных экспертных учреждений и квалификация их экспертов редко подвергаются сомнению. Но по новому, всего 5-7 лет назад возникшему виду экспертизы — КТЭ — эти экспертные учреждения либо вообще экспертиз не проводят, либо способны проводить лишь простейшие их виды. Причина известна. Специалисты в области ИТ (а тем более, квалифицированные) пока еще не подготавливаются в массовом порядке. Средняя рыночная зарплата такого специалиста намного превышает ставки, которые в состоянии предложить любое из бюджетных учреждений (а государственное экспертное учреждение, согласно закону, может финанси-

роваться только из бюджета).

Таким образом, следователь может выбрать в качестве эксперта любое лицо, в чьей компетентности он уверен. Никаких обязательных «сертификатов эксперта», лицензий и допусков не требуется. Разумеется, для оценки квалификации кандидата следователь может навести справки об образовании, опыте работы в сфере ИТ, должности. Опыт является определяющей величиной.

Когда есть выбор, автор рекомендует отдавать предпочтение гражданскому эксперту. В государственных экспертных учреждениях системы МВД (ЭКЦ, ЭКУ, ЭКО) если и имеются штатные эксперты по КТЭ, то лишь низкой квалификации, как правило, «крепостные», то есть работающие там, чтобы избежать призыва в армию. Кроме того, нагрузка на штатных экспертов МВД никак не позволяет им затрачивать на экспертизу более двух дней (обычная норма две экспертизы в день), что автор полагает неприемлемо коротким сроком для полноценного исследования.

Проблемы с пониманием

Эксперт призван дать заключение (ч. 1 ст. 57 УПК), а специалист — разъяснить вопросы (ч. 1 ст. 58). То и другое подразумевает объяснение неспециалистам фактов и обстоятельств из области специальных знаний. Но всегда ли возможно такое объяснение?

Оно возможно лишь тогда, когда некий процесс непонятен без специальных знаний, но его следствия или выводы целиком лежат в знакомой области. Например, неспециалист может не понимать, что такое отпечатки пальцев и как их снимают. Но вывод — человек касался пальцами предмета — понятен любому. Неспециалист может совершенно не разбираться в авиационной технике. Но «причиной аварии явилась ошибка пилота» — это каждому понятно. Неспециалист не может себе вообразить, как работает транзистор. Но как пользоваться радиовзрывателем — здесь нажал, там взорвалось — это понятно.

В отрасли ИТ встречаются ситуации, когда не только механизм и процесс лежат в области специальных познаний, но там же находятся следствия и выводы. Поэтому бывает так, что специалист затрудняется объяснить простыми словами не только почему, но и что, собственно, произошло.

Например, возьмем такое злодеяние, как вмешательство в процесс показа рекламных баннеров*. Специалист вряд ли сможет разъяснить суду механизм подмены адреса баннерного сервера через DNS-записи. Но и следствия этого деяния — пользователи увидят на веб-страницах рекламу, помещенную туда помимо их желания и без прямой санкции владельца веб-страницы вместо другой рекламы, которая тоже была помещена туда

помимо желания пользователей и без прямой санкции владельца веб-страницы — все целиком находится в виртуальном мире и не могут быть разъяснены без предварительного разъяснения всех сложных взаимоотношений между участниками информационного обмена.

Разъясняя вопросы, требующие специальных знаний, специалист фактически занимается переводом с одного языка на другой. Для этого он не только должен в совершенстве владеть обоими языками. Попытки перевести с технического на юридический часто наталкиваются на такое препятствие: в другом языке просто не существует соответствующего термина. Да что там термина! Соответствующего понятия не существует.

Например, нетрудно перевести с технического термин «провайдер». На юридическом это означает «оператор связи». А вот как перевести термин «доменное имя»? Это совершенно новый объект, возникший в Сети и не имеющий аналогов в офлайне*. Средство индивидуализации? Нет, под определение не подпадает. Ресурс нумерации? Тоже нет, фактически не соответствует. Приходится обходиться без перевода и вводить этот термин в юридический оборот. Но как объяснить его значение неспециалисту, если даже специалист учился несколько лет, прежде чем полностью понял, что такое доменное имя?

Еще пример. В ходе процесса судья поставил перед специалистом вопрос: идентифицирует ли IP-адрес компьютер в сети Интернет однозначным образом? Специалист ответил утвердительно. Тот же вопрос был поставлен перед экспертом. Эксперт ответил отрицательно. Оба они были правы, о чем и согласились, поговорив между собой. Дело в том, что эксперт отвечал на вопрос «теоретически», имея в виду абстрактный компьютер и любой IP-адрес. Разумеется, любой IP-адрес однозначным идентификатором не является. Специалист же был ознакомлен с материалами дела и отвечал на вопрос применительно к конкретному компьютеру и конкретному адресу. Фигурировавший в деле IP-адрес идентифицировал компьютер обвиняемого однозначно, о чем специалист и сказал.

Итак, следует признать, что для области ИТ сформулированная в УПК задача специалиста и эксперта не всегда является выполнимой. Но выполнять ее надо. Как следствие, эксперты и специалисты иногда превышают свои полномочия и не только «разъясняют вопросы», но и делают выводы.

Приемлемые вопросы

Для следователя и оперуполномоченного важно представлять, что именно может компьютерно-техническая экспертиза (КТЭ) и чего она не может. Также важно уметь верно формулировать вопросы для экспертизы.

На памяти автора следователь ни разу не поставил вопросы для КТЭ корректно. Оно и неудивительно. Чтобы правильно сформулировать вопрос, нужно знать большую часть ответа. И разбираться в терминологии. А чтобы знать специальные термины, нужно представлять, что они означают. Короче, нужно самому обладать специальными знаниями в области ИТ.

Была издана работа, содержащая перечень возможных вопросов для КТЭ [42]. Формулировки всех вопросов там заранее выверены и должны быть понятны эксперту. Следователю оставалось лишь выбрать нужный. Разумеется, ни к чему хорошему это не привело. Раньше, не имея подобной подсказки, следователь формулировал вопросы некорректно. Это приводило к объяснению между ним и экспертом. В ходе разговора вопросы уточнялись, следователь переписывал свое постановление в соответствии с рекомендациями эксперта. А пользуясь шпаргалкой, но по-прежнему не понимая значения терминов, следователь попросту выбирает из списка не те вопросы. В результате вместо плодотворного диалога получается, что эксперт просто выполняет ненужную работу. А нужную — не выполняет.

Автор полагает, что для формулировки вопросов для КТЭ всегда следует привлекать специалиста. Это может быть специально приглашенный специалист. Это может быть неофициальная консультация. В крайнем случае, сам эксперт, которому предстоит проводить КТЭ, поможет следователю верно поставить вопросы.

Автор, не желая повторять чужих ошибок, не станет приводить здесь списка возможных вопросов для КТЭ. Вместо перечня вопросов автор предпочитает дать перечень решаемых экспертизой задач с необходимыми разъяснениями.

Поиск информации

Поиск на компьютерном носителе документов, изображений, сообщений и иной информации, относящейся к делу, в том числе в неявном (удаленном, скрытом, зашифрованном) виде.

Автор рекомендует не конкретизировать вид и содержание искомой информации. Эксперт вполне может самостоятельно решить, относится ли тот или иной текст, изображение или программа к делу. В ходе поиска информации эксперту приходится просматривать глазами тысячи текстов и изображений. Понятно, что невозможно распечатать и приложить к заключению их все — с тем, чтобы потом следователь решил, что из найденного относится к делу. Эксперт в любом случае вынужден проводить первичную селекцию и принимать решение, что именно из найденного приобщать. Вынужден в силу объемов информации. Типичный объем архива электронной почты среднего пользователя — мегабайты. Для более актив-

ного — сотни мегабайт. Это не поместится ни в одно заключение (протокол). Поэтому эксперта следует ознакомить с уголовным делом или хотя бы кратко изложить его фабулу в постановлении о назначении КТЭ. И запросить у него поиск «любой информации, относящейся к данному делу».

Следы

Поиск «цифровых» следов различного рода действий, совершаемых над компьютерной информацией. Вопрос лучше формулировать не про следы, а про действия. То есть вместо «имеются ли следы создания таких-то веб-страниц?» лучше поставить вопрос так: «создавались ли на исследуемом компьютере такие-то веб-страницы?».

Когда компьютер используется как средство доступа к информации, находящейся в ином месте, и когда доступ к информации осуществляется на этом компьютере — в обоих случаях остаются «цифровые» следы, следы в виде компьютерной информации. КТЭ может определить, когда, при каких условиях и каким образом осуществлялся доступ. Кто его осуществлял, КТЭ определить не может. Лишь в некоторых случаях эксперту удастся обнаружить некоторые сведения о пользователе исследуемого компьютера.

Действия, которые оставляют следы на компьютере или на носителе информации, включают: доступ к информации, ее просмотр, ввод, изменение, удаление, любую другую обработку или хранение, а также удаленное управление этими процессами.

Программы

Анализ программ для ЭВМ на предмет их принадлежности к вредоносным, к средствам преодоления ТСЗАП, к инструментам для осуществления неправомерного доступа к компьютерной информации, к специальным техническим средствам, предназначенным для негласного получения информации. А также анализ функциональности программ, принципа действия, вероятного их источника, происхождения, автора.

Иногда необходимо более глубокое исследование программ. То есть исследование не просто их свойств и функциональности, а происхождения, особенностей взаимодействия с другими программами, процесса создания, сопоставление версий. Такое глубокое исследование подразумевает дизассемблирование программы, запуск под отладчиком (пошаговое исполнение), исследование структуры данных. Это предмет отдельной экспертизы, иногда ее называют программно-технической. Редко можно найти эксперта, сочетающего специальные знания по ИТ и по программированию. Поэтому рекомендуется проводить две отдельные экспертизы — первая изучает содержимое компьютерных носителей, а вторая особенности обнаруженных программ.

Такое более глубокое исследование программ необходимо далеко не всегда. Например, вредоносность программы — это совокупность ее функций [81, 70]. Вредоносность может установить эксперт-специалист по ИТ. А вот для сопоставления объектного* кода программы с фрагментом исходного* кода необходимо участие эксперта-программиста.

Время

Установление времени и последовательности совершения пользователем различных действий.

Благодаря наличию у компьютера внутренних энергонезависимых часов и простановке в различных местах временных меток становится возможным определить, когда и в какой последовательности пользователь производил различные действия.

Если внутренние часы компьютера были переведены вперед или назад (в том числе неоднократно), все равно имеются возможности восстановить правильное время и правильную последовательность событий. Перевод часов компьютера сам по себе оставляет следы. А если еще было и сетевое взаимодействие, то есть возможность сопоставить моменты событий, зафиксированные данным компьютером, с событиями по иным источникам и выяснить сдвиг внутренних часов.

Задача выполнима даже в том случае, если системный блок, содержащий внутренние часы, не находится в распоряжении экспертизы. Только по носителю информации (например, НЖМД*) можно получить кое-какие сведения о последовательности событий. Чем больше информации на носителе, тем полнее будет восстановлена картина.

Отмечена даже такая экзотическая задача, как подтверждение/опровержение алиби подозреваемого, который утверждает, что в определенное время работал за компьютером [43]. В этом случае, хотя речь не идет о компьютерном преступлении, для проверки алиби потребуется КТЭ.

Пользователь

Оценка квалификации и некоторых других особенностей личности пользователя исследуемого компьютера.

При достаточно интенсивном использовании компьютера человек неизбежно оставляет в нем «отпечаток» собственной личности. Документы, фотографии, музыка, переписка, настройки, оформление, закладки, временной режим работы, подбор программ — все это индивидуализирует информационное содержимое компьютера. Все это отражает интеллект пользователя, его эмоции, наклонности, способности.

Нет уверенности, что вопрос полностью лежит в сфере КТЭ. Возможно, ради более строгого подхода такая экспертиза должна быть комплексной, компьютерно-психологической. Во всяком случае, вопрос квалифи-

кации пользователя в области ИТ точно в компетенции эксперта, проводящего КТЭ. Конечно, для оценки квалификации на исследуемом носителе должны находиться соответствующие объекты, результаты интеллектуальной деятельности — написанные пользователем программы, переписка по нетривиальным техническим вопросам, сложные программные инструменты (например, отладчик).

Следует заметить, что некорректно ставить вопрос об «установлении личности пользователя компьютера». Любые выводы о личности на основе найденных на диске плодов интеллектуальной и творческой деятельности могут носить лишь предположительный характер.

Итоги

Итак, обычно перед экспертом, проводящим КТЭ, ставятся вопросы:

- о наличии на исследуемых объектах информации, относящейся к делу (в том числе в неявном, удаленном, скрытом или зашифрованном виде);
- о возможности (пригодности) использования исследуемых объектов для определенных целей (например, для доступа в сеть);
- о действиях, совершенных с использованием объектов, их времени и последовательности;
- об идентификации найденных электронных документов, программ для ЭВМ, о признаках пользователей компьютера;
- о свойствах программ для ЭВМ, в частности, о принадлежности их к вредоносным.

Неприемлемые вопросы

Контрафактность

Отдельного разъяснения требуют вопросы, связанные с контрафактностью экземпляра произведения, представленного в цифровой (электронной) форме. Недопустимо ставить перед экспертом вопрос, является ли исследуемый экземпляр произведения контрафактным. Контрафактность — это вопрос правоотношений между правообладателем и пользователем, но никак не вопрос состояния экземпляра. Один и тот же экземпляр может быть контрафактным и легальным (лицензионным), в зависимости от того, оплатил ли пользователь стоимость лицензии, истек ли ее срок, выполнены ли лицензионные условия и других обстоятельств. Иными словами, контрафактность — это юридический, а не технический факт. Устанавливать его эксперт не может [L02].

Конечно, эксперт может найти косвенные признаки контрафактности, то есть такие особенности, которые обычно (подчеркиваю — обычно!) встречаются на контрафактных экземплярах и обычно не встречаются на

лицензионных. Но прямыми доказательствами такие признаки не будут, поскольку контрафактный экземпляр легко превращается в лицензионный путем заключения договора с правообладателем или его представителем (а это сводится к уплате соответствующей суммы). И, напротив, лицензионная копия легко становится контрафактной при нарушении пользователем лицензионных условий. В обоих случаях сама копия при таких «превращениях» ни на бит не изменяется.

Перед экспертом следует ставить вопросы о наличии признаков контрафактности — любых или конкретных, которые заранее известны следователю.

Впрочем, среди юристов существует мнение, что никаких «признаков контрафактности» вообще не бывает. А признаки исполнения экземпляра произведения не должны подвергаться экспертизе, поскольку их наличие или отсутствие не связано с контрафактностью экземпляра. Согласно этой точке зрения, для доказательства нарушения авторских прав непременно следует установить изготовителя экземпляра произведения, доказать отсутствие у него разрешения от правообладателя и лишь затем проводить экспертизу изъятых экземпляров с целью установить, действительно ли они были изготовлены тем же способом, на том же оборудовании.

Предположим, в лапы правоохранительных органов попал компакт-диск с произведением. Диск имеет тип CD-R, записан с использованием ПК, обложка отпечатана на ксероксе, голограмма отсутствует. Следует ли устанавливать и закреплять с помощью экспертизы все перечисленные признаки? Обсуждаемая позиция утверждает, что нет, не следует. Поскольку отсутствует причинная связь между кустарным исполнением и отсутствием разрешения правообладателя. Следует доказывать нарушение авторских прав, что сводится к доказыванию отсутствия разрешения, то есть договора, между изготовителем (не продавцом!) диска и правообладателем, либо между изготовителем и уполномоченным представителем правообладателя, либо между изготовителем и обществом по коллективному управлению авторскими правами. А метод изготовления диска с фактом заключения такого договора никак не связан. Следовательно, признаки исполнения диска ничего не доказывают. Даже косвенно.

Впрочем, автор с изложенной позицией не согласен. И авторитеты (например, Верховный Суд) на этот счет еще не высказались.

Стоимость

Технический специалист не может определить ни стоимость программного продукта, ни ущерб правообладателю. Стоимость является предметом товароведческой или экономической экспертизы.

Ценообразование на программные продукты и цифровые фонограммы — это отдельная большая тема. Происходит оно несколько иначе, чем в отношении материальных товаров. При этом издержки производителя — далеко не самый важный фактор. Если в отношении материального товара цена на различных рынках для различных групп потребителей может отличаться и в 2, и в 3, и даже в 5 раз (больше — вряд ли), то в отношении «нематериального» программного обеспечения цена может различаться в бесконечное число раз даже в пределах одной страны. Нередки случаи, когда правообладатель передает право на использование программного продукта (лицензию) совершенно бесплатно для некоторых потребителей, а с других потребителей берет значительные суммы.

Например, в отношении золотого кольца цена в один доллар является однозначным указателем на криминальное происхождение. Покупатель не может не знать, что таких цен на такой товар не бывает. На рынке же программных продуктов встречаются вполне легальные и при этом добротные товары по цене в 1 и даже в 0 долларов. При этом их аналоги могут продаваться за сотни долларов. Поэтому покупатель не может быть уверен в контрафактности, ориентируясь на низкую цену. Даже подозрений на контрафактность может не возникнуть.

Правомерность доступа

Эксперт не может определить правомерность доступа, осуществлявшегося с исследуемого компьютера или на исследуемый компьютер. Правомерность — это, как и контрафактность, факт юридический, а не технический.

Но эксперт может определить ряд других фактов, которые позволят следствию и суду квалифицировать доступ как правомерный или неправомерный. Это следующие факты:

- к какой именно информации осуществлялся доступ (для последующего решения вопроса, является ли она охраняемой законом компьютерной информацией);
- предпринимал ли обладатель информации, к которой был осуществлен доступ, какие-либо меры для ее защиты и ограничения доступа (для решения вопроса о конфиденциальности этой информации);
- присутствует ли на электронном документе или носителе гриф «коммерческая тайна» (для решения вопроса об отнесении этой информации к коммерческой тайне [44]) или иной гриф;
- является ли данный способ доступа общепринятым способом для публичных сетевых ресурсов.

Нуждается в пояснениях последний пункт. Правомерность или неправомерность доступа определяется не только законами (каковых для Интернета не очень много) или договорами (каковые не могут быть заключены между всеми пользователями и владельцами ресурсов). Во многих

случаях правомерность определяется обычаями делового оборота (ст. 5 ГК). Например, порт 3389/tcp используется для удаленного управления компьютерами с ОС «Windows». Никаких публичных сервисов на этом порту ожидать нельзя. Поэтому попытки доступа на этот порт со стороны постороннего лица следует расценивать как неправомерные. Порт 80/tcp, напротив, в подавляющем большинстве случаев используется для публичного HTTP-сервиса. Поэтому пользователь, осуществляя попытку доступа к этому порту чужого сервера, может ожидать на нем наличия общедоступного веб-сайта. Такую попытку нельзя признать неправомерным доступом. Итак, одно и то же действие по отношению к различным портам должно квалифицироваться по-разному. При этом статус обоих упомянутых портов закреплен лишь в технических стандартах и в неписаных обычаях делового оборота сети Интернет.

Оценка содержания

Эксперт может найти на исследуемом компьютере (носителе) тексты и сообщения по определенной тематике, однако он не имеет права оценивать содержание этих текстов, их авторство.

Также эксперт не может действовать в качестве переводчика, если тексты на ином языке. Возможно, исключение составляет тот случай, когда в переписке используется жаргон или транслитерация. Хотя задача в этом случае вроде бы лингвистическая, но соответствующих специалистов среди обычных лингвистов нет. Это как раз тот случай, когда лучший переводчик — не переводчик, а специалист в предметной области. Для «перевода» текстов с жаргона или с нестандартного транслита можно назначить отдельную комплексную экспертизу — лингвистическо-компьютерную. А можно поручить эксперту в рамках КТЭ «преобразовать найденные тексты в доступную для восприятия форму без изменения их смыслового содержания, а также разъяснить используемые в текстах специальные термины и выражения».

Ниже для иллюстрации приводится реальный диалог по ICQ из одного уголовного дела. Автор специально выбрал пример попроще, с использованием кириллицы. В случае же применения собеседниками транслитерации, да к тому же транслитерации далеко не канонической, о подобный диалог читатель мог бы сломать глаза.

Слушай а ты не знаешь где можно Civilization2 скачать?(это игра)
ТЫ ЧЕ?! ДУРАК?!
СОВСЕМ ПОЕХАЛ ЧТОЛИ?!
ОНА ВЕСИТ ТО СКОЛЬКО?!
А мне пофигу! Я вчера на 56\$ сосканил!
ВОТ НЕНАВИЖУ КОГДА ТАК ОТРУБАЮТ!!!!!!
КАК?
Прлсто взяли и отрубили! Я уж думал пароль кончился....

:) Да у меня тоже такое в последнее время бывает...
 Слушай... Ты мне так и не сказал как по сети в кваку резаться.
 Здорова!!!
 Здравово!!!
 Пришол чтоли?
 Ну так...
 Здесь тебе привет от ученицы!!!
 От Сашки чтоли? :)))
 Мы тут по порно лазием!!
 :))))))))))
 Рульно!!!
 Ты где ща лазаеш?
 Дан!! Дай пасс.
 У менямои на исходе, а впереди еще вся ночь!!!!
 Я те патом по возможности отдам...
 Я простог в последнее время обленился!!! :((((:)))
 Дан!! Не молчи!!
 Ты меня слышьшь?
 Слушай UFO выйдиз инета побазарить надо!!!!!!
 Давай.... А ещё, кокой у тебя номер в Одиго?
 А как тебя туда занесло?:-)))
 А газета то МоСковская?
 А может это фсВля А-ааа...:-))))))))))))))))))))))
 Не-а...
 Ты на щёт чего??
 Слишком длинный:-)))
 Давай на кнт.ru
 Чё за инфа??
 Слушай где мне УРл короткий достать?
 Ну типа как ты говорил www.haker.net
 Чё хоть куриш та?
 Дай хоть какой нибудь сайт прикольный:-)))
 Нет...
 avt393381
 Нет ты мне дал avt239776...
 Держи на два бакса

 avt202265
 UTew8hNC

 Ладно пора спать, а то завтра хрен встану. Полтинник принесу в воскресенье
 Пока!!!!

Неподготовленный человек вряд ли поймет, что речь идет о применении вредоносных программ и неправомерном доступе к компьютерной информации, а также о сбыте результатов такого доступа.

Резюме

Итак, в рамках КТЭ нельзя ставить следующие вопросы:

- о лицензионности/контрафактности экземпляров произведений, записанных на исследуемых носителях;

- о правомерности действий, произведенных с использованием исследуемых объектов;
- о стоимости компьютеров, носителей, прав (лицензий) на содержащиеся там программы;
- о переводах найденных текстов, интерфейсов программ, переписки и т.п. (кроме разъяснения терминов и жаргона).

Объекты исследования

Оригинал или копия?

Существует мнение, что на экспертизу следует представлять только оригинал носителя компьютерной информации — НЖМД, компакт-диск, флэш-накопитель и т.д. А исследовать его копию якобы неприемлемо.

Это мнение не основано на законе. Ни в УПК, ни в законе «О государственной судебно-экспертной деятельности в Российской Федерации» (№73-ФЗ) такого требования не содержится. Более того, содержится запрет повреждать объект исследования без особого разрешения следователя.

Автор полагает (и многие исследователи с этим согласны), что исследовать в ходе КТЭ оригинал носителя вообще нежелательно. Чтобы гарантировать неизменность информации, а также оставить возможность проведения повторной или дополнительной экспертизы, надо оставить оригинал нетронутым. А все исследования проводить с его копией. Это не только надежнее, но и удобнее, поскольку копию можно сделать на таком носителе, который лучше приспособлен для имеющихся у эксперта инструментов, надежнее, быстрее.

Это относится не только к изготовлению копии носителя в ходе КТЭ, но и к копированию носителя вместо его изъятия при проведении обыска или выемки.

Например, во время обыска специалист может изъять диск сервера целиком, а может на месте скопировать все его содержимое (естественно, на низком уровне, на уровне контроллера) на свой диск. Допустимо ли это с процессуальной точки зрения? Разумно ли с технической точки зрения?

Есть следующие аргументы:

1. Некоторые методы исследования носителя непременно требуют оригинала. Другие с равным успехом работают с копией. Во время изъятия может ли специалист предположить, какие вопросы поставят перед экспертом и какие методы он станет применять? По мнению автора, может. Тем более что методы, требующие непременно оригинала, используются крайне редко.

2. Возможны ошибки при копировании диска. Их возникновение ставит под угрозу проведение экспертизы вообще. Но насколько вероятны такие ошибки? Верификация после копирования носителя разве не решит проблему? По мнению автора, решит. Кроме того, специалист должен использовать для копирования лишь проверенные средства и методы, которые не только не допускают ошибок, но и детектируют внешние ошибки.

3. Достаточно ли компетентность специалиста, участвующего в следственном действии, проводящего копирование диска? По мнению автора, найти такого специалиста несложно.

4. Поймут ли понятые суть происходящих действий? Изъятие и опечатывание оригинала диска им, безусловно, понятно. А снятие копии? Смогут ли они уверенно утверждать, что именно проделывал специалист? По мнению автора, им этого понимать и не обязательно. На то и предусмотрен специалист, чтобы проводить действия, требующие специальных знаний.

5. Может ли произойти при копировании диска утрата некоторой информации? Например, заводской номер диска, число секторов. По мнению автора, утраты не произойдет, если копировать на уровне контроллера диска, а внешние признаки оригинала записать в протокол.

6. Если применять снятие копии вместо изъятия оригинала носителя, это позволит не прерывать (или прервать ненадолго) рабочий процесс у владельца носителя. Остановить работу сервера на несколько дней ради проведения экспертизы — за что потерпевшему или непричастному провайдеру такое наказание?

7. В некоторых случаях копирование носителя страхует от потери данных вследствие недолговечности оригинального носителя. Например, в случае КПК. Лучше на месте снять копию памяти, чем до экспертизы поддерживать КПК в заряженном состоянии (не нарушая целостность печатей). Или в случае старого диска, склонного «сыпаться», то есть постоянно увеличивать количество дефектных блоков.

Методы КТЭ

Исследование файловых систем

Чтобы носитель компьютерной информации мог содержать файлы, он должен быть размечен и отформатирован под определенную файловую систему*. Разметка* состоит в создании на носителе разделов* (партиций), внутри которых могут быть образованы логические диски (тома). Форматирование логического диска (тома) состоит в создании на нем пустой файловой системы. Некоторые виды носителей способны содержать единственный раздел (партицию), например, дискеты.

Файловая система — это структура для организации хранения информации в виде файлов и доступа к ней. Файл обязательно предусматривает заголовок и тело. В заголовке содержится имя файла, другие его атрибуты и указание на расположение тела файла. В теле файла записываются данные, то есть содержимое файла. Практически все файловые системы предусматривают древовидную структуру: файлы включаются в состав директорий* (каталогов), которые, в свою очередь, могут включаться в другие директории. Минимальная единица хранения определяется параметрами носителя (например, размером сектора НЖМД) и файловой системой; обычно она именуется блоком или кластером. Тело файла всегда занимает целое число таких блоков.

Наиболее распространенные файловые системы таковы.

| Название | Макс. емкость | Комментарии |
|----------|--|--|
| FAT12 | 16 Мб | Используется только на дискетах |
| FAT16 | 2 Гб; для Windows-NT и последующих: 4 Гб | Единственная ФС для MS-DOS и ее клонов. С момента создания поддерживается ОС Юникс. Ныне считается устаревшей для компьютеров, но широко используется на иных устройствах — MP3-плеерах, камерах, флэш-накопителях |
| FAT32 | 2 Тб | Оригинальная ФС для Windows-95-OSR2 и последующих, является модификацией FAT16. Применяется в некоторых мультимедийных носителях. |
| NTFS | 16 Эб (1 Эб=2 ⁶⁰ б) | Оригинальная ФС для Windows-NT и последующих. Поддерживает сжатие и шифрование данных, а также восстановление после сбоев |
| UFS | 256 Тб–1 Йб (2 ⁸⁰ б) (UNIXFile System) | Стандартная, или «родная», ФС для всех типов UNIX, а также MacOS-X. Существует несколько модификаций под различные клоны Юникс |
| Ext2fs | 32 Тб | Оригинальная ФС для ОС Linux. Наследует свойства UFS. Предусматривает восстановление целостности после сбоев |
| Ext3fs | 32 Тб | Развитие ФС Ext2fs. Добавлено журналирование транзакций для улучшения и ускорения восстановления после сбоев |
| Ext4 | 1 Эб (1 Эб=260б) | Дальнейшее развитие ФС Ext3. Уменьшена фрагментация и повышена производительность |

| | | |
|---------------------------------|---|--|
| ISO-9660 | | Популярная ФС для компакт-дисков и DVD. Есть несколько модификаций ФС: Joliet, Rock-Ridge, ISO-13490 и др. |
| этой HPFS (High-to-File System) | 64 Гб | Оригинальная ФС для OS/2. Основана на принципах FAT с добавлением некоторых свойств по ускорению доступа и оптимизации |
| HFS | Performance | Стандартная ФС для MacOS |
| | MacOS-6 и 7 — 2 Гб MacOS-7.5 — 4 Гб; MacOS-7.5.2 и послед. — 2 Тб | |
| HFS Plus | 2 Тб | Дальнейшее развитие HFS |
| UDF (Universal Disk Format) | | ФС для DVD и некоторых CD |

С другими файловыми системами можно познакомиться в специальной литературе [W10, W11], всего их известно несколько десятков.

Как правило, каждая ОС имеет встроенную поддержку для одной или нескольких файловых систем. При помощи дополнительного ПО (драйверов) ОС может понимать и иные файловые системы.

Если работать с носителем (диском) помимо штатных функций для соответствующей файловой системы, то можно увидеть больше информации, чем доступно через файловую систему. Такая скрытая информация может быть обнаружена в четырех местах — свободных блоках, хвостах файлов, ADS и неиспользованных разделах.

Свободные блоки. При стирании файлов штатными средствами ОС блоки, содержащие тело файла, отмечаются как свободные, но сразу не перезаписываются. Запись в эти блоки может быть произведена позже, при последующих операциях. Таким образом, свободные блоки, если они хоть раз использовались, содержат фрагменты старых, удаленных или измененных файлов. Правда, не всегда можно восстановить первоначальную принадлежность и последовательность этих блоков.

Хвосты файлов. Как указывалось, тело файла должно занимать целое число блоков (кластеров) на носителе. Если файл короче, то остаток последнего блока, его хвост или «slack space» будет содержать прежнюю информацию, то есть фрагмент старого файла.

Alternate data streams (ADS) — это дополнительные тела для файла в файловой системе NTFS, которые могут содержать сопутствующую информацию. Они недоступны с помощью штатных средств ОС и поэтому представляют скрытую для пользователя информацию.

Свободные и специальные разделы. Неиспользуемые и неразмеченные части диска также содержат информацию, которая была там прежде.

Иногда можно наткнуться на целый бывший раздел. Есть также разделы специального назначения, например, для свопинга или для хранения содержимого криптодиска.

Кроме того, на некоторых типах носителей встречаются технологические, не предназначенные для пользователей области, например, Host Protected Area (HPA). При помощи соответствующих программ они все же могут быть использованы и порой используются для хранения скрытой информации.

Копирование носителей

Любые экспертные исследования носителей компьютерной информации надо проводить, не изменяя их содержимого, если только это возможно. А возможно это всегда.

Исключением можно считать те случаи, когда эксперт не обладает исследовательским оборудованием или носителем нужной емкости. Учитывая, что исследовательским оборудованием в данном случае является самый обычный компьютер, а хорошее экспертное ПО распространяется бесплатно, такие причины автор не склонен считать уважительными. Но на практике это встречается. Надо напомнить, что если при экспертизе содержимое исследуемого носителя изменяется, некоторая оригинальная информация с него уничтожается, то, согласно УПК, на это следует получить предварительное разрешение от следователя, назначившего экспертизу.

Все исследователи единодушно рекомендуют делать копию оригинального носителя и проводить исследования с ней, а оригинал сохранить в неизменности для контроля и возможной повторной/дополнительной экспертизы. Если на экспертизу поступила копия, то ее также следует оставить в неприкосновенности в качестве мастер-копии, а исследования проводить над снятой с нее рабочей копией.

Для обнаружения скрытой информации копировать носитель нужно не средствами ОС, то есть не на уровне файловой системы, а уровнем ниже. Копирование надо производить на уровне контроллера устройства (также используется термин «Bit stream copying/imaging»). При этом копируется как информация, содержащаяся в файловой системе, так и скрытая для нее — свободные блоки, хвосты файлов и т.д.

В принципе, возможны исследования носителей на еще более низком уровне — на физическом. Для НЖМД это означает, что считывание производится не встроенными в накопитель магнитными головками, под управлением встроенного контроллера, а некими внешними средствами. При этом возможно снять остаточную намагниченность или намагниченность на границах магнитных дорожек и таким образом восстановить даже те данные, которые были недоступны для штатных магнитных головок исследуемого НЖМД. Это позволяет восстановить перезаписанные

(в том числе перезаписанные неоднократно) данные. Но такая экспертиза требует специального очень дорогого оборудования. Ограничимся рассмотрением экспертных исследований на уровне файловой системы и на уровне контроллера устройства.

Итак, оригинальный носитель перед проведением экспертизы копируется. Можно скопировать его на другой (такого же размера или большего) аппаратный носитель, а можно создать образ носителя в специальном файле или разделе. Копирование «носитель на носитель» можно произвести как предназначенным для этого отдельным устройством (дубликатором дисков), так и с помощью компьютера, используя соответствующее программное обеспечение, например, программу «dd». Копирование «носитель в файл» производится только программно, специальным ПО, например, программой «dd».

Копирование же на уровне файловой системы (также используется термин «logical copying/imaging/backup») применимо лишь в ограниченном числе случаев, например, при изучении только лог-файлов.

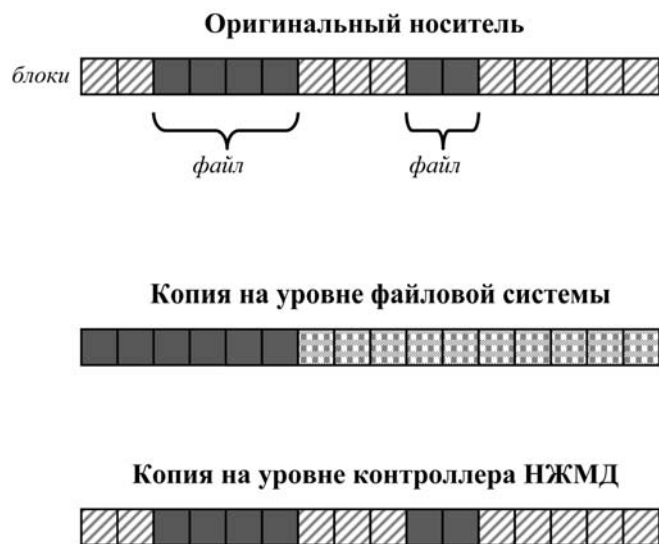


Схема копирования на уровне файловой системы (logical copying) и копирования на уровне контроллера диска (bit stream copying)

Копирование носителя может являться составной частью экспертизы. Копирование может быть проведено во время следственного действия вместо изъятия оригинального носителя. В последнем случае на экспертизу передается копия, но ее необходимо сохранить неизменной, так же как в случае с передачей на экспертизу оригинального носителя.

Есть опасение, что не все программные и аппаратные инструменты одинаково хорошо справляются с задачей копирования носителя.

Действительно, некоторые инструменты могут либо неточно/неполно копировать, так что содержимое копии отличается от оригинала, либо вносить какие-либо изменения в оригинал.

В Национальном институте юстиции США (National Institute of Justice, U.S. Department of Justice) были протестированы несколько таких программ [W12]. Согласно методике испытаний, корректность снятия копии содержимого (образа) диска определяется 4 параметрами:

- совпадение копии с оригиналом;
- возможность верификации копии;
- сохранение неизменности оригинала;
- детектирование внешних ошибок.

Проведенными исследованиями показана корректная работа следующих программ:

- dd из состава ОС FreeBSD 4.4 (без ошибок);
- Encase версии 3.20 (с тремя ошибками);
- Safeback версии 2.18 (с двумя ошибками);
- Safeback/DOS версии 2.0 (с четырьмя ошибками);
- dd из состава GNU fileutils 4.0.36, ОС Red Hat Linux 7.1 (без ошибок).

Разумеется, проводились и иные исследования в иных организациях, но автор приводит данный источник (National Institute of Justice) как наиболее авторитетный из известных. Использование упомянутых программ для снятия образа диска во время экспертизы или при проведении следственного действия не вызовет у специалистов сомнений по поводу корректности копирования.

Для сохранения неизменности оригинала или для дополнительной гарантии такой неизменности оригинальный носитель при копировании подключается в режиме «только чтение». Для этого во всех операционных системах, кроме Windows, используется режим «ro» команды монтирования файловой системы (mount). А для Windows, где такого режима не предусмотрено, используются специальные программные или аппаратные блокировщики записи, которых существует на рынке немало.

Для гарантии тождественности копии или образа диска после копирования следует произвести верификацию. В упомянутых выше программах и некоторых других предусмотрен режим верификации. Если его нет, то побитное сравнение содержимого оригинала и копии можно произвести иными программами.

Хэш-функции для удостоверения тождественности

В зарубежной практике для удостоверения целостности и неизменности данных на носителе используются однонаправленные хэш-функ-

ции*. Например, при снятии специалистом образа диска на месте происшествия подсчитывается хэш-функция, значение которой заносится в протокол. Эксперт, получив на исследование копию, подсчитывает с нее хэш-функцию. Если ее значение совпадает со значением, внесенным в протокол, эксперт и иные лица получают уверенность, что исследуемая копия совпадает с оригиналом с точностью до бита.

Аналогично хэш-функция используется для контроля целостности отдельных файлов. Например, при изъятии логов. Подсчитывается хэш-функция от лог-файла, она заносится в протокол. Если имеется уверенность в правильном подсчете хэш-функции, то сам лог-файл можно, в принципе, никак не оформлять, не печатывать, а переписать на переносной носитель без формальностей. Значение хэш-функции в протоколе обеспечивает неизменность файла при копировании и последующем хранении. Совпадение значений хэш-функции гарантирует полное совпадение файлов [18].

Отметим, что все эти выкладки — чистая теория. В отечественной уголовной практике контроль целостности на основе хэш-функций не применяется (хотя в гражданских делах были прецеденты).

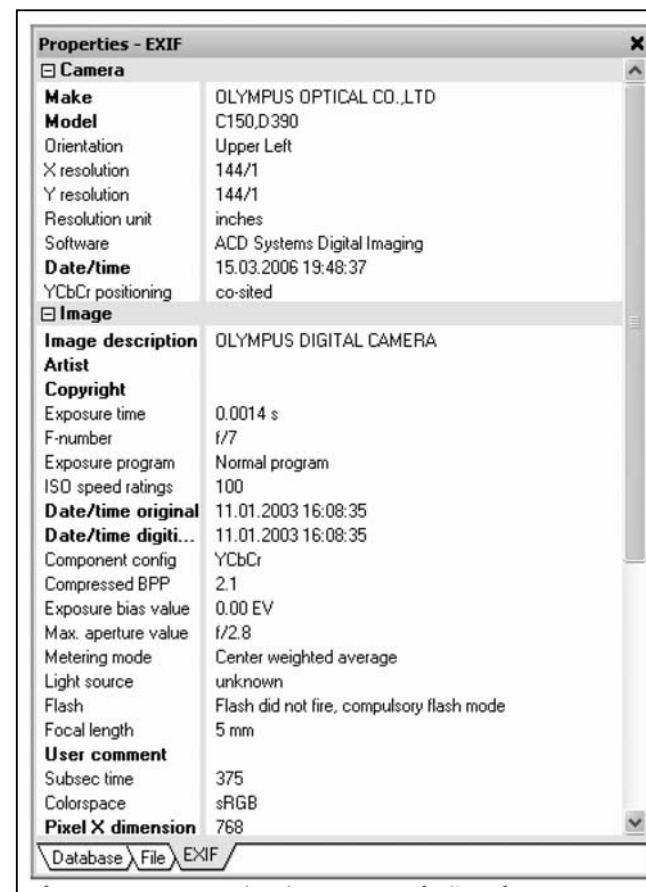
В качестве хэш-функций обычно используются широко известные алгоритмы MD5 [18, 33] и SHA-1 [34]. Они имеют достаточную стойкость. Хотя есть и гораздо более стойкие хэш-функции, например, SHA-256, SHA-512, WHIRLPOOL.

В России указанные алгоритмы имеют такую же стойкость, как и за рубежом, но они не являются стандартными. У нас имеется собственный стандарт для алгоритма хэш-функции — ГОСТ Р-34.11. Имеются даже его программные реализации, которые можно приспособить для вычисления хэш-функции от образа диска. Проблема в том, что хэш-функция считается криптографическим преобразованием, а его реализации — криптографической (шифровальной) техникой. Применение такой техники регламентируется соответствующими нормативными актами, она подлежит обязательной сертификации, использующие ее информационные системы — аттестации, а деятельность по обслуживанию шифровальной техники — лицензированию. Понятно, что при снятии копии диска специалистом в полевых условиях никак невозможно провести аттестацию системы и обеспечить соблюдение условий сертификата на шифровальную технику, даже если бы такой сертификат у специалиста имелся.

Поэтому автор не может рекомендовать официальное использование однонаправленных хэш-функций для удостоверения целостности информационного содержимого носителей. Их, конечно, полезно использовать. Можно даже заносить значение MD5 в протокол. Но нельзя ссылаться на совпадение значений хэшей в качестве доказательства неизменности данных.

Исследование файлов

Файлы, содержащие документы (текстовые, графические, табличные, комбинированные), очень часто несут кроме самого документа много служебной и сопровождающей информации, которая не видна для пользователя. Часто пользователь даже не подозревает о ее существовании. Однако эксперт о ней знает, а следовательно, может без труда извлечь такую дополнительную информацию из файла.



Служебная информация из необработанного файла формата JPEG позволяет получить дополнительные данные: модель фотоаппарата, время съемки, использование вспышки и многое другое

Например, в файлах с изображениями формата JPEG (jpg) хранятся сведения о прикладной программе или оборудовании, при помощи которой файл создавался или редактировался. В документах формата MS-Word хранится идентификатор (логин) создавшего пользователя, исходное размещение файла, прежние версии текста и много чего другого.

Шутка, обошедшая весь русский сегмент Интернета, — всего лишь полное имя файла, извлеченное из скрытых атрибутов документа MS-Word:

"C:\Хрень по работе\Гемор\Тупые клиенты\Неплательщики\оку-евшие\Уважаемый Сергей Анатольевич.doc"

Как при исследовании отдельных файлов (кроме простейших текстовых или ASCII-файлов), так и при исследовании дисков, иных носителей, компьютеров имеет смысл поставить перед экспертом вопрос касательно обнаружения скрытой, служебной информации, предусмотренной соответствующим форматом файла.

Другие типы носителей

Флэш-накопители

Весьма распространенные носители компьютерной информации на основе флэш-памяти не только надежнее, но и значительно удобнее исследовать, сняв предварительно их копию. Разумеется, речь идет о копировании не на уровне файловой системы, а на уровне контроллера устройства, то есть bitstream-копировании. Также копию можно снимать не в ходе КТЭ, а при изъятии таких накопителей.

Проще всего сделать копию, подключив такое устройство к лабораторному компьютеру с ОС типа UNIX или Linux. В этих системах есть все необходимое для безопасного (без возможности записи) подключения и побитового копирования. При вставлении такого накопителя в USB-разъем или иное устройство чтения оно опознается операционной системой. Если опознания не произошло, значит, не хватает соответствующего драйвера (модуля ядра), который нужно доустановить.

Пример опознавания флэш-накопителя с интерфейсом USB:

```
# dmesg
umass1: PNY USB DISK 2.0, rev 1.10/0.50, addr 2
da4 at umass-sim1 bus 1 target 0 lun 0
da4: < USB DISK 2.0 1.09> Removable Direct Access SCSI-0 device
da4: 1.000MB/s transfers
da4: 124MB (253952 512 byte sectors: 64H 32S/T 124C)
```

Подключаем опознанный накопитель с опцией «ro» (только чтение):

```
# mount_msdosfs -o ro /dev/da4s1 /mnt/usbdrv/

# mount
/dev/ad6s1a on / (ufs, local)
devfs on /dev (devfs, local)
/dev/ad6s1e on /tmp (ufs, local, soft-updates)
```

```
/dev/ad6s1f on /usr (ufs, local, soft-updates)
/dev/ad6s1d on /var (ufs, local, soft-updates)
/dev/da4s1 on /mnt/usbdrv (msdosfs, local, read-only)
```

Чтобы исключить возможность изменения информации на устройстве, его подключение (монтирование) осуществляется с опцией «-r» (или «-o ro»), то есть в режиме read-only. Далее при помощи программы «dd» все содержимое устройства побитово копируется в файл, который и будет подвергнут дальнейшему исследованию.

```
# dd if=/dev/da4 of=/home/fnn/usbimage.bin conv=notrunc,noerror,sync
253952+0 records in
253952+0 records out
130023424 bytes transferred in 1271.039536 secs (102297 bytes/sec)
```

Получившийся у нас файл с образом накопителя **usbimage.bin** может быть подключен к экспертной программе — «EnCase» «FTK» или какой-либо другой.

Если копирование накопителя производится на месте, то будет полезно подсчитать контрольную сумму, а лучше — хэш-функцию полученного файла и занести ее в протокол. Значение хэш-функции, которая вычислена несертифицированным и неаттестованным криптографическим средством, официально не может служить доказательством неизменности файла. Однако ее совпадение со значением хэш-функции, которое вычислит эксперт, будет дополнительным способом убедиться в целостности данных.

```
# md5 usbimage.bin
MD5 (usbimage.bin) = 4d3de473b8c7f01ec6ed6888f61f8c43
```

После этого отмонтируем накопитель и извлекаем его из разъема.

```
# umount /mnt/usbdrv/

# dmesg
umass1: at uhub3 port 2 (addr 2) disconnected
(da4:umass-sim1:1:0:0): lost device
(da4:umass-sim1:1:0:0): removing device entry
umass1: detached
```

Подключение и копирование USB-устройства под ОС класса Windows представляется более проблематичным, поскольку отсутствует возможность подключения (монтирования) накопителей в режиме «только чтение». Все USB-устройства в этой ОС подключаются с возможностью чтения и записи, и ОС может производить запись на устройство без санкции со стороны пользователя и без его уведомления. Для накопителей с интерфейсами SCSI и IDE (ATA) выпускаются аппаратные блокираторы за-

писи, а для USB-устройств такого приспособления автору найти не удалось. Впрочем, некоторые модели флэш-накопителей имеют собственный аппаратный блокиратор записи в виде переключателя на корпусе.

Зашифрованные данные

Шифрование отдельных записей, файлов, разделов, дисков и трафика применяется злоумышленниками достаточно широко. Кроме того, функции шифрования встроены во многие виды программного обеспечения, где они задействуются автоматически. Эксперт должен быть готов ко встрече с зашифрованными данными, не должен считать такой случай безнадежным. Хотя современная сильная криптография считается практически непреодолимой, на практике оказывается, что во многих случаях добраться до зашифрованных данных можно [56].

Перечислим вкратце основные случаи, когда эксперт в состоянии расшифровать зашифрованные данные.

Использование слабой криптографии

То ли из-за недостатка знаний, то ли времени, но многие злоумышленники по сию пору продолжают использовать довольно примитивные шифры. Например, операция XOR (исключающее «или») с определенным байтом или короткой последовательностью байтов. Эта операция проще всего реализуется программно, и «на вид» такие данные выглядят зашифрованными. Но преодолеть XOR-шифрование очень просто. Иные виды слабой криптографии применяются редко, поскольку они не так просты, как операция XOR, а более стойкие алгоритмы шифрования доступны в виде исходного кода и библиотек.

Например, троянская программа «Back Orifice» использует XOR для шифрования своего трафика. Известные производители также были замечены в подобной халтуре: например, XOR с фиксированной последовательностью для шифрования паролей использовался в «Microsoft Office» до 2000 года, в «PalmOS» до версии 4 и в некоторых других программах.

Использование коротких ключей и паролей

Даже в случае применения сильной криптографии зашифрованные данные будут плохо защищены, если использован короткий пароль. Часто пароль служит ключом шифрования. В других случаях длина ключа или множество его значений искусственно ограничиваются. В подобных случаях эксперт может применить метод перебора, также называемый «brute force». Этот метод реализован во множестве программ для многих разных алгоритмов шифрования. На взгляд автора, всегда полезно по-

нять метод перебора в течение нескольких часов над зашифрованными данными; затраты рабочего времени незначительны, свободный ресурс процессора всегда имеется, а вдруг получится?

Не слабые, но намеренно ослабленные алгоритмы, такие как, например, 40-битный DES в экспортной версии «Windows-NT», также поддаются вскрытию методом перебора. Но для этого потребуется значительная вычислительная мощность — несколько компьютеров, объединенных в кластер. Для такой задачи имеется доступное программное обеспечение.

Использование словарных паролей

Вместо прямого перебора пароля или ключа («brute force») можно попробовать подобрать пароль по словарю. Большинство пользователей выбирают в качестве пароля осмысленное слово или фразу. Это позволяет резко сократить количество вариантов при переборе. Словарь всех распространенных языков содержит меньше миллиона слов. Вместе со всеми возможными комбинациями это всяко меньше, чем пространство неосмысленных паролей, то есть всех возможных сочетаний символов такой же длины. Несловарный пароль в 8 символов можно безуспешно подбирать месяцами. А такой же длины словарный пароль находится перебором за секунды.

В распоряжении эксперта есть как свободно распространяемые, так и проприетарные программы для подбора паролей по словарю, а также различные словари к ним.

В качестве дополнительного словаря автор рекомендует использовать все символьные строки, найденные на диске подозреваемого. Велика вероятность, что в качестве пароля он выбрал какое-либо слово, выражение, номер или иную строку символов, которую где-то видел или сам употреблял. В том и в другом случае эта строка может осесть на жестком диске в каком-либо виде.

Неаккуратное обращение с открытым текстом

При шифровании файлов и в некоторых иных случаях открытый текст зашифровывается, результат шифрования записывается на диск, а файл, содержащий исходный текст, удаляется. Если такое удаление произведено штатными средствами ОС, без использования специальной процедуры «затирания» содержимого файла, то открытый текст останется на диске и может быть восстановлен. То же относится к сообщениям электронной почты: при шифровании исходный текст удаляется из базы сообщений, но не затирается и может быть обнаружен, если поверх не запишутся иные данные. Во время редактирования файла, хранящегося на криптидиске, редактор может сохранять временные копии вне этого крипто-

диска, а операционная система может временно сбрасывать редактируемый текст или его части из ОЗУ в область подкачки*. Перед распечаткой на принтере незашифрованная копия данных записывается в очередь печати, то есть опять же на диск. Словом, пользователю трудно проконтролировать все файловые операции. При их проведении открытый текст часто остается на диске, где его можно потом найти.

Также копии открытого текста бывают разбросаны по оперативной памяти. Не все программы аккуратно обращаются с ОЗУ и затирают за собой содержимое памяти. Сняв дампы* ОЗУ в период активности шифрующей программы или после, можно найти в нем открытый текст.

Неаккуратное обращение с паролем

Как уже указывалось, словарный пароль легко подобрать. Зато неподбираемый пароль трудно запомнить. Тем более, трудно запомнить несколько длинных и неосмысленных паролей. Поэтому злоумышленник может записать пароли где-то — в файле, в записной книжке, в мобильном телефоне, на столе. Или использовать в качестве пароля уже имеющуюся вблизи рабочего места надпись, например, с наклейки на системном блоке.

Также подозреваемый может использовать один пароль для нескольких ресурсов разной степени защищенности. Это достаточно распространенная практика. Например, он сумел запомнить один длинный и неосмысленный пароль и использовал его для шифрования ключа к криптодиску и для доступа на веб-сайт. Из конфигурационного файла браузера эксперт извлекает все запомненные пароли и пробует применить их к криптодиску — вот и не сработала сильная криптография.

Нешифрованные имена файлов

Имена файлов при обработке записываются трудноконтролируемым образом в еще большее количество мест, чем содержимое (тело) файлов. В зашифрованных архивах имена файлов часто не шифруются. Имена файлов часто запоминаются редакторами, файловыми оболочками. Даже если эксперту не удалось добраться до содержимого криптодиска, он наверняка найдет в нескольких местах на исследуемом компьютере оглавление этого криптодиска. По именам файлов многое можно сказать об их содержании. А если кроме имени известен еще и размер файла, то в отдельных случаях можно даже найти где-нибудь оригинал.

Известны случаи, когда расшифровать данные эксперту не удалось, но удалось получить оглавление зашифрованного диска. Соответствие имен файлов и их размеров известным файлам послужило доказательством. На таких доказательствах вполне может быть основано обвинение в нарушении авторских прав или в распространении порнографии.

Ректотермальный криптоанализ

Говорят, что человек — это слабое звено в системе информационной безопасности. Хотя автор и не согласен с рассмотрением человека в качестве «звена» или «элемента» информационной системы, следует признать, что большинство инцидентов происходят не из-за уязвимостей ПО или сбоев оборудования, а по вине персонала. Аналогичная ситуация наблюдается и в области исследования доказательств. Большинство известных автору случаев, когда эксперт смог расшифровать данные на исследуемом компьютере, — это сообщение пароля самим владельцем компьютера или оператором информационной системы.

Для того чтобы склонить подозреваемого или свидетеля к сотрудничеству со следствием, применяются различные методы, не входящие в сферу изучения криминалистики. Наука лишь отмечает, что человек является самым распространенным источником сведений для расшифровки зашифрованных данных.

Доступ к содержимому ОЗУ

В оперативной памяти могут храниться не только незашифрованные данные, но и ключи с паролями. Эксперт вряд ли получит доступ к работающему компьютеру с активированным криптодиском или иной системой шифрования, чтобы снять с него дамп оперативной памяти. Однако содержимое ОЗУ можно обнаружить в области подкачки, а также в дампах памяти, которые автоматически снимаются при сбоях в работе. Например, утилита «Dr.Watson» в Windows-2000 автоматически записывает дамп памяти сбойного процесса.

Содержимое ОЗУ с паролями, содержимое временных файлов и удаленных пользовательских файлов с паролями может быть найдено по всему диску в самых неожиданных местах. Систематический подход к задаче состоит в следующем. По исследуемому диску собираются все строковые величины, ключевые слова и фразы, они агрегируются и записываются в виде файла-словаря, который затем подключается к программе подбора паролей. Достаточно велика вероятность, что пароль хотя бы раз «осел» на диске или что пользователь использовал в качестве пароля слово или выражение, которое встречалось в прочитанных или написанных им текстах.

Использование кейлогера

В некоторых, достаточно редких случаях представляется возможность незаметно отследить действия подозреваемого, в том числе снять техническими средствами вводимый им пароль. Средства такие именуются кейлогерами (keylogger) и бывают программными и аппаратными.

Впрочем, этот метод относится, скорее, к ОРД, а не к экспертизе. Он более подробно описан в разделе 2.

Шифрование разделов и носителей

В некоторых носителях, таких как флэш-накопители, шифрование содержимого предусмотрено конструктивно.

По каким-то не вполне ясным для автора причинам некоторые проприетарные реализации такого шифрования на проверку оказываются нестойкими, уязвимыми, а то и вовсе притворными.

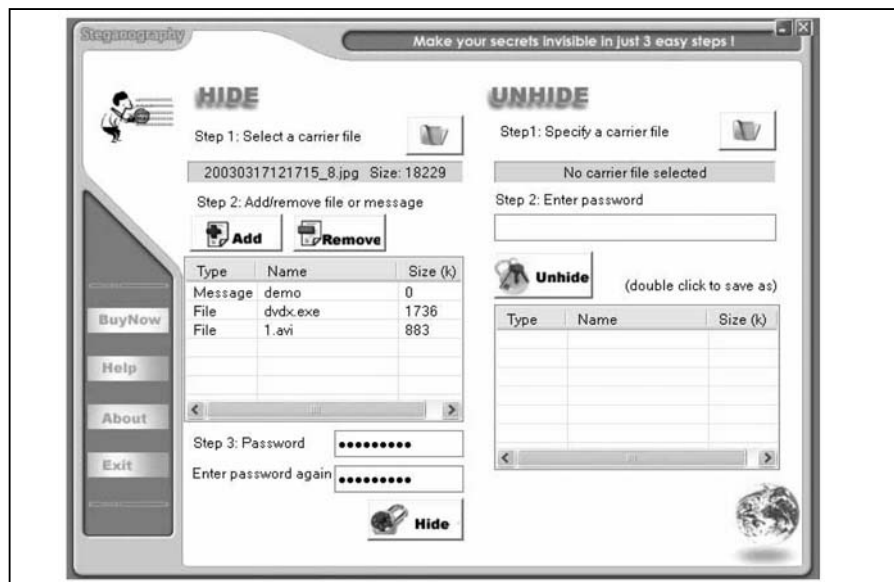
Поэтому, наткнувшись на проприетарную реализацию шифрования данных на носителе, эксперт должен первым делом предположить, что имеется намеренно или случайно оставленный производителем «черный ход». В ряде случаев такой ход обнаруживается простым поиском информации в Интернете. В других случаях производитель носителя сам берется расшифровать «надежно зашифрованные» данные (разумеется, по запросу правоохранительных органов, после исполнения ряда формальностей).

В отличие от проприетарных, открытые реализации шифрования все устойчивы. Во всяком случае, автору не известны случаи обнаружения в них «черного хода».

Стеганография

Этот метод, в отличие от шифрования, предусматривает сокрытие самого факта наличия информации на компьютере или в сообщении [66, 67].

Многие применяемые форматы данных (файлов и сообщений) содержат «нечувствительные» биты, которые могут быть изменены без ущерба



Одна из многочисленных программ для непрофессионалов, позволяющая скрывать произвольную информацию внутри файлов-контейнеров формата JPEG

для восприятия информации. Иные форматы предусматривают наличие обязательных, но неиспользуемых полей. И там и там может быть записана скрываемая информация.

Чаще всего в качестве стеганографических контейнеров используются изображения в формате BMP и JPEG, звуковые файлы в формате MP3 (MPEG-3), видеофайлы в формате AVI. Существует несколько программ (в том числе, свободных) для хранения информации в таких контейнерах и извлечения ее.

Стеганография чаще используется при пересылке сообщений. Для хранения же информации на компьютере применять стеганографические технологии неразумно, поскольку трудно скрыть наличие стеганографических программ. А если эксперт обнаружит такие программы, он непременно начнет искать скрытую информацию, то есть стеганография теряет свое значение.

Ниже показан пример работы одного из инструментов для обнаружения стеганографических контейнеров — программы «stegdetect/stegbreak»:

```
$ stegdetect *.jpg
cold_dvd.jpg : outguess(old)(**) jphide(*)
dscf0001.jpg : negative
dscf0002.jpg : jsteg(**)
dscf0003.jpg : jphide(**)
[...]
$ stegbreak -tj dscf0002.jpg
Loaded 1 files...
dscf0002.jpg : jsteg(wonderland)
Processed 1 files, found 1 embeddings.
Time: 36 seconds: Cracks: 324123, 8915 c/s
```

Средства и инструменты

Экспертные инструменты и авторское право

Часто автору приходится слышать мнение, что все применяемые экспертом (специалистом) программные инструменты должны быть лицензионными*. В противном случае, дескать, результаты экспертизы или следственного действия считаются полученными с нарушением закона и недопустимыми.

На самом деле соответствующая норма (ст. 75 УПК) сформулирована так: «Доказательства, полученные с нарушением требований настоящего Кодекса, являются недопустимыми». То есть не имеют юридической силы лишь те доказательства, при получении которых нарушались требования УПК, а не какого-либо иного закона.

Нарушает ли эксперт требования УПК, используя нелицензированную копию программы? Не нарушает, ибо УПК (глава 27) не содержит каких-либо требований к инструментам эксперта.

Эксперт в своем заключении даже не обязан указывать, какие инструменты он использовал. Обязан указать лишь «примененные методики» (ст. 204 УПК). Методика — совсем не то же самое, что инструмент или программа. Почти все экспертные программы используют одни и те же методики исследования, а именно: доступ к носителю через функции файловой системы, доступ к носителю помимо файловой системы (через функции BIOS), контекстный поиск на носителе, детектирование форматов данных на основе сигнатур и так далее.

Нарушает ли эксперт законодательство об интеллектуальной собственности, используя нелицензированную копию программы? Оказывается, тоже нет. Статья 23 закона «Об авторском праве...» гласит: «Допускается без согласия автора и без выплаты авторского вознаграждения воспроизведение произведений для судебного производства в объеме, оправданном этой целью». В четвертой части ГК, которая с 2008 года приходит на смену закону «Об авторском праве...», эта норма сформулирована схожим образом: «Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение произведения для осуществления производства по делу об административном правонарушении, для производства дознания, предварительного следствия или осуществления судопроизводства в объеме, оправданном этой целью» (ст. 1278).

Программа для ЭВМ — это произведение. Установка программы есть ее воспроизведение. Судебная компьютерно-техническая экспертиза — это как раз «для судебного производства» или «для производства предварительного следствия». Поэтому эксперт и специалист могут почти свободно использовать любой проприетарный софт, не опасаясь нареканий.

Многие компании-правообладатели и сами не возражают против бесплатного использования их программ экспертами или правоохранительными органами. Многие безвозмездно передавали образцы своего ПО для проведения экспертных исследований.

Таким образом, можно утверждать, что какие бы программы ни использовал эксперт в своих исследованиях, это само по себе не может служить основанием для непризнания результатов экспертизы.

Поиск информации на диске

Информация о файлах

Помимо самого файла, на диске сохраняется информация об этом файле в различных местах. Когда файл затерт, уничтожен без возможности восстановления, можно тем не менее установить и доказать факт его присутствия в прошлом по этим косвенным данным. Эти данные суть следующие:

- копии тела файла и их фрагменты в секторах диска, которые считаются свободными;
- заголовок файла в каталоге, а также во всех копиях этого каталога в свободных секторах диска;
- упоминания имени и, возможно, некоторых других атрибутов файла в «истории» и логах тех прикладных программ, которые его обрабатывали — редакторов, файл-менеджеров, клиентов электронной почты, архиваторов и т.п.;
- временные копии файла, которые создаются программами, которые этот файл редактируют или просматривают;
- промежуточные копии файла и его атрибутов, образующиеся при пересылке файла при помощи электронной почты, ICQ, FTP, веб-интерфейса;
- архивные копии диска, его отдельных каталогов, реестра, электронной почты и других объектов;
- миниатюры (thumbnails), которые создает ОС и некоторые вьюверы (программы просмотра) для ускорения просмотра списка файлов.

В некоторых случаях нет необходимости восстанавливать уничтоженную или зашифрованную информацию, достаточно лишь доказать ее наличие на исследуемом диске.

Например, по одному делу о нарушении авторских прав на программные продукты было установлено, что подозреваемый держал контрафактные копии программ на криптодиске*. Эксперт не смог подобрать ключ для расшифровки. Однако в этом и необходимости не было. Для подтверждения вины требовалось доказать не наличие программ на диске, а их использование подозреваемым. Эксперт обнаружил на диске многочисленные копии каталога криптодиска, записи в реестре, ярлыки (shortcuts) соответствующих программ, данные, обработанные этими программами, — и на этом основании сделал вывод, что программный продукт был установлен на исследуемом компьютере и использовался неоднократно.

В другом случае эксперт искал на диске подозреваемого электронные изображения денежных купюр, в подделке которых тот подозревался. Файлы с изображениями купюр оказались затерты без возможности восстановления. Однако сохранились миниатюры (thumbnails), которые автоматически создает ОС для показа списка файлов в каталоге. Для графических файлов миниатюра представляет собой уменьшенное изображение первой страницы. Несмотря на небольшой размер миниатюры, ее содержимое было видно достаточно четко. Эксперимент по созданию такой же миниатюры из большого изображения денежной купюры подтвердил гипотезу. Таким образом наличие файла с изображением на компьютере подозреваемого было доказано без обнаружения самого файла.

Подключение образа диска

Как указывалось выше, не обязательно изымать на экспертизу диск компьютера целиком. Вполне достаточно снять на месте bit stream-копию или образ этого диска. Исследуя этот образ, можно установить все, что и при исследовании самого диска (исключение составляет особый вид экспертизы, крайне редко применяющийся в России). Но даже когда экспертизу поступает сам магнитный диск, все исследования все равно проводятся над его образом, который снимается в самом начале экспертизы.

Образ диска может сниматься на такой же или большего объема диск по принципу «сектор в сектор». Другой, более удобный способ, когда образ диска создается в файле. В первом случае диск-образ физически подключается к лабораторному компьютеру и монтируется в режиме «read-only». Для этого используется команда «mount» с ключом «-r» или «-o ro»; такая команда есть в любой ОС, кроме «Windows». Для «Windows» придется подключать диск через специальное аппаратное устройство для блокировки записи. Во втором случае (образ в едином файле) подключение диска эмулируется специальной программой. Такие функции есть в «EnCase» и другом экспертном ПО.

Изучение архивов электронной почты и ICQ

На персональном компьютере сохраняется вся отправляемая и принимаемая корреспонденция. В зависимости от настроек, она может храниться долго или не очень или стираться сразу по прочтении. Но в любом случае, при получении и отправке информация записывается на диск хотя бы раз. А это значит, что если не в явном, то в скрытом виде она может найтись при экспертизе.

Средний пользователь хранит в архиве одну-две сотни сообщений электронной почты. Более активные пользователи могут хранить несколько тысяч. Вместе с копиями этих сообщений, вместе с удаленными сообщениями может получиться очень много информации. Не хватит никакой бумаги, чтобы всю ее распечатать. Поэтому никогда не следует давать задание эксперту найти и отпечатать всю найденную электронную переписку.

С другой стороны, сводить работу эксперта к обнаружению одного-двух заданных писем тоже неверно. Лучше всего поставить перед экспертом вопрос об обнаружении всей переписки как в явном, так и в скрытом (удаленном) виде.

Те сообщения, которые относятся к делу, следует распечатать на бумаге и приложить к заключению. Весь прочий архив переписки имеет смысл записать на компакт-диск. Если окажется, что распечатанного недостаточно, не надо будет проводить повторную экспертизу, достаточно

всего лишь провести осмотр содержимого компакт-диска, записанного экспертом. Для осмотра архива электронной почты или ICQ, записанного в каком-либо распространенном формате (например, текстовом), не требуется специальных знаний. Такой осмотр может провести следователь с понятиями. Кроме того, исследованный компьютер после хранения может оказаться и непригоден для повторного исследования — условия хранения вещественных доказательств у нас не самые оптимальные. А информация на компакт-диске, который приложен к заключению эксперта и хранится прямо в уголовном деле, — это надежнее и проще.

Решать, какая именно часть переписки относится к делу, целесообразно поручить эксперту. Для этого его необходимо ознакомить с материалами дела. В простейших случаях бывает достаточно изложить фабулу дела в постановлении о назначении экспертизы.

Кроме обнаружения архива переписки нужно поставить вопрос о том, принимались ли (отправлялись ли) найденные сообщения. Электронное письмо попадает в архив не только в том случае, когда оно отправлено с данного компьютера или принято на данный компьютер. Оно может быть записано (импортировано) в архив по особой команде пользователя. Оно может быть приложено к другому письму, которое поступило пользователю. Многие люди, когда меняют компьютер, переписывают со старого на новый весь архив электронной почты. Различные следы скажут эксперту, было ли найденное сообщение принято или отправлено при помощи исследуемого компьютера, или оно принималось/отправлялось из другого места, а на исследуемый диск попало каким-то иным путем.

Факт отправки или приема электронного сообщения нельзя строго доказать одним только обнаружением его на компьютере отправителя или получателя в ходе экспертизы. Необходимо подтвердить факт передачи письма «на другом конце» или на промежуточном узле. Иногда второй корреспондент известен. Но часто местоположение второй копии письма выясняется лишь в ходе проведения экспертизы. В таких случаях бывает полезно поставить перед экспертом вопрос, где еще можно обнаружить копию сообщения или следы его передачи.

Реконструкция просмотра веб-страниц

Из тех следов просмотра пользователем веб-сайтов (веб-сёрфинга), которые могут быть обнаружены на пользовательском компьютере, следует отметить cookie-файлы, историю просмотра и кэш браузера (временные файлы). Также при анализе следует учитывать хранимые браузером пароли к сайтам и закладки.

История просмотра веб-страниц — это, упрощенно говоря, перечень адресов (URL) веб-сайтов, к которым пользователь осуществлял доступ.

Одни браузеры хранят историю в своих настройках, другие — вместе с временными файлами.

Кэш браузера (временные файлы) — это копии HTML-файлов, изображений и иных файлов, загружаемых в ходе просмотра веб-страниц. Они сохраняются на локальном диске на случай повторного просмотра тех же страниц. Вместе с каждым файлом принимается и записывается срок его актуальности.

В cookie-файлах содержится адрес веб-сайта, который создал этот файл, значения переменных, время создания и срок актуальности этого cookie. Эти файлы сохраняются на компьютере пользователя по инициативе веб-сервера и предназначены, для того чтобы сервер мог сохранить индивидуальные настройки пользователя [71, 72].

Все описанные данные, если они сохранились, позволяют в подробностях восстановить последовательность просмотра пользователем веб-сайтов. Эта процедура может быть автоматизирована. Реконструкцию веб-сёрфинга по сохраненным данным браузера выполняют экспертные программы «EnCase», «FTK», «Pascos» и некоторые другие. Реконструкцию можно провести и вручную.

В свете изложенного вполне уместно выглядит такой вопрос эксперту: «Восстановить последовательность просмотра пользователем веб-сайтов в такой-то период времени» или «Установить, когда пользователь просматривал веб-сайт такой-то, в какой последовательности и какую информацию при этом получал».

Учитывая, что достаточно распространены веб-интерфейсы к электронной почте, при помощи восстановления просмотренных пользователем веб-страниц можно установить получение и отправку им сообщений электронной почты через такой веб-интерфейс.

Оценка найденного

Распространенной ошибкой следствия является поставить перед экспертом вопрос о наличии на НЖМД того или иного содержимого, но не поинтересоваться, каким образом найденная информация там оказалась. Добросовестный эксперт, конечно, сам, без дополнительного вопроса, укажет в заключении, каким путем найденная информация образовалась на диске.

Многие следователи и судьи молчаливо предполагают, что если информация найдена в компьютере, то именно пользователь компьютера поместил ее туда. Это не всегда так. Существует ряд путей, когда интересующая следствие информация попадает в компьютер помимо воли и без ведома его пользователя. Перечислим эти пути:

- НЖМД*, прежде чем попасть в исследуемый компьютер, мог использоваться в другом, у другого пользователя. Продаются подержанные

жесткие диски. Даже если диск (компьютер) куплен в магазине и считается «новым», не исключено, что он был возвращен в торговую сеть предыдущим покупателем. Некоторые предприятия-сборщики компьютеров для экономии используют подержанные комплектующие, не уведомляя об этом потребителей. Подержанная электроника с виду ничем не отличается от новой. Конечно, продавец, как правило, переразмечает и/или переформатирует НЖМД. Но прежняя информация при этом на диске остается и будет обнаружена в ходе экспертизы.

- Вредоносные программы, от которых никто не застрахован¹, скрытно внедряясь на компьютеры, часто открывают «черный ход», позволяющий как снимать информацию по сети с этого компьютера, так и записывать на него. Указанным «черным ходом» может воспользоваться как «хозяин» вредоносной программы, так и иное лицо. Поскольку особенности устройства и поведения всех выявленных вредоносных программ известны, находится немало желающих воспользоваться ресурсами скомпрометированных компьютеров для собственных целей. Злоумышленники постоянно сканируют Интернет в поисках известных «черных ходов», а найдя, пытаются получить контроль над компьютером, присоединив его к своей зомби-сети*. Плотность сканирования достаточно высока. Компьютер с известной уязвимостью, будучи «выставлен» в Интернет без защиты, заражается вредоносной программой в течение считанных минут. Описанным способом на диске скомпрометированного компьютера может образоваться информация без желания и ведома его пользователя.
- При просмотре веб-сайтов вся полученная браузером информация в том или ином виде откладывается на жестком диске. Попасть на веб-сайт пользователь может и без своего желания, будучи автоматически перенаправлен или завлечен обманом. На сайте могут размещаться рекламные баннеры*, содержание которых владелец сайта не контролирует. Кроме того, на диск (в кэш браузера) записывается не только просмотренная пользователем информация, но и такая, которую он даже не видел — не пролистал веб-страницу до конца, не дождался ее окончательной загрузки, не активировал скрипт, быстро закрыл всплывающее (pop-up) окно и так далее. То есть пользователь не видел информации и не желал ее получать, а эксперт нашел такую информацию на диске.
- Примерно то же относится к спаму*. Полученный пользователем без его желания спам, хотя и стирается, зачастую даже без беглого прос-

¹ Доказано, что своевременное обновление всего ПО и постоянное использование антивирусной программы, хотя и снижает риск заражения, но отсутствия вирусов не гарантирует. Обновления (патчи) к ПО и новые базы к антивирусам выходят несколько позже, чем соответствующие вирусы.

мотра, сохраняется на диске. Его содержимое наверняка будет найдено при проведении экспертизы и при неверном истолковании может привести к судебной ошибке. Известно, что в спаме часто рекламируются незаконные товары и услуги.

- Персональный компьютер редко используется человеком строго персонально. Члены семьи, друзья и коллеги вполне могут время от времени воспользоваться чужим персональным компьютером, чтобы нечто скачать с Интернета или переписать информацию с одного носителя на другой. Часто это делается без ведома владельца. Поэтому всегда остается вероятность найти на диске информацию, к которой пользователь не имеет отношения.
- Компьютеры иногда отдают в ремонт. В ходе диагностики и ремонта на диск может устанавливаться специализированное ПО (в том числе двойного назначения) и записываться всякая информация в тестовых целях. Конечно, тестовую информацию удалят, но впоследствии, в ходе экспертизы, она будет обнаружена и может быть неверно интерпретирована.

Автор вовсе не хочет сказать, что все, обнаруженное на компьютере подозреваемого, следует списывать на вирусы, спам и прежних владельцев. Как правило, эксперт в состоянии определить, когда, каким способом и в каком контексте найденная информация была записана на диск — и тем самым развеять сомнения относительно ее происхождения. Перед экспертом наряду с вопросом о присутствии на диске той или иной информации всегда надо ставить вопрос о том, каким способом и при каких обстоятельствах эта информация там оказалась.

Исследование программ

Когда заходит речь об исследовании создания программ для ЭВМ, сравнении двух программ, установлении соответствия исходного кода и исполняемого кода — словом, когда исследование не может ограничиться «внешней» функциональностью программ, то требуются специальные знания в области программирования. Специалист в сфере информационных технологий, компьютерных сетей, защиты информации и специалист в области программирования редко сочетаются в одном лице. Как правило, программист имеет лишь общие представления об ИТ и наоборот.

Поэтому, если требуются глубокие знания по программированию, стоит назначить по этому вопросу отдельную экспертизу.

Например, лицо подозревается в создании (именно создании, не модификации) вредоносной программы и получении с ее помощью конфиденциальных данных с компьютера потерпевшего. Доказательства, очевидно, могут быть найдены на компьютере подозреваемого в ходе проведения КТЭ. Имеет смысл назначить две отдельные экспертизы либо одну

комплексную экспертизу. Первый эксперт (специалист по ИТ) должен разыскать на изъятом компьютере тексты программ и исполняемый код, а также ответить на вопросы о наличии конфиденциальной информации из компьютера потерпевшего. А второй эксперт (программист) должен исследовать найденный исходный код и исполняемый код вредоносной программы и ответить на вопросы, касающиеся ее устройства, функциональности, изготовления и авторства.

Изучение печатных документов

С какой-то точки зрения лист бумаги, вышедший из принтера, тоже является носителем компьютерной информации. Хотя такая информация предназначена для восприятия человеком, но записана она была при помощи компьютера. То, что напечатано на принтере, неизбежно было представлено в цифровом виде. Поэтому все распечатки следует рассматривать наравне с электронными носителями.

На распечатках содержится не только информация, ориентированная на человека. Машинная информация там тоже есть.

Изготовители принтеров из США закладывают в них печать на каждой странице скрытых данных о дате, времени и заводском номере принтера. Сделано это было по настоянию властей, но информация почти сразу стала широко известна [W14]. В том числе опубликованы места печати скрытой информации и ее кодировка [W15, W16, W17]. Информация эта, разумеется, неофициальная. Но ее несложно будет проверить в ходе экспертизы. Достаточно на том же принтере или на принтере такой же модели распечатать контрольную страницу (чистый документ) и сравнить обнаруженные на ней скрытые коды с кодами на исследуемом документе.

Сведений о распечатке подобной скрытой сигнатуры принтерами, произведенными в других странах, нет.

Кроме нарочно созданных сигнатур у принтеров имеются индивидуальные особенности и особенности, присущие модели [47]. Поэтому экспертиза может не только привязать печатный документ к конкретному принтеру, но и по документу установить, на принтере какой модели он был напечатан.

Стоимость ПО

Несколько слов про иной вид экспертизы, необходимый при расследовании компьютерных преступлений.

На квалификацию преступления по ст. 146 (ч.ч. 2 и 3) УК влияет стоимость экземпляров или прав на использование произведения. Автор хотел бышний раз подчеркнуть, что в статье фигурирует именно **стоимость**. Не ущерб и не цена. Довольно часто на следствии происходит путаница (а то и

умышленная подмена понятий): эксперту ставят вопрос об ущербе правообладателю, в качестве доказательства приводят справку о цене программного продукта. В то время как оценить следует именно его стоимость.

Как известно, стоимость товара или услуги является объективной категорией. То есть она не определяется желаниями участников конкретной сделки, не зависит от мнения автора или правообладателя. Упомянутые субъекты могут устанавливать только цену конкретной сделки. А стоимость зависит от состояния рынка в целом, от полезности товара и других объективных категорий.

Поскольку стоимость объективна, ее можно оценить. Оценку стоимости в идеале должен проводить эксперт-экономист или эксперт-оценщик [L04]. Разумеется, эксперт должен быть независим от автора или правообладателя. **Оценку стоимости не может проводить потерпевший.** Хотя, к большому сожалению, в российской практике часто именно так и поступают — принимают в качестве стоимости прав на ПО сумму, декларированную потерпевшим.

Оценка стоимости программного обеспечения (точнее, прав на его использование) имеет свои особенности. Производство ПО с экономической точки зрения довольно сильно отличается от производства материальных товаров. Общие издержки на производство серии товара составляют почти 100%, а индивидуальные издержки на производство каждого экземпляра составляют ничтожную часть всех издержек. Отсюда и особенности в определении стоимости одного экземпляра ПО.

Другие экономические особенности программных продуктов таковы:

- Цена на ПО очень вариабельна. В зависимости от региона, потребителя, условий эксплуатации цена на одну и ту же программу может запросто отличаться в 10 и более раз. Нередки случаи, когда при определенных условиях или для определенных категорий пользователей лицензия на ПО вообще передается бесплатно, в то время как для прочих она стоит существенных денег.
- При выходе новой версии программы прежняя версия либо вовсе снимается с продажи, либо очень сильно дешевеет. В то время как цена новой версии обычно близка к прежней цене старой. Потребительские свойства более старой версии при этом не меняются.
- Часто новая версия программы (обновление до более новой версии) входит в цену старой, то есть легальным пользователям прежней версии ПО права на новую версию предоставляются бесплатно или с очень большой скидкой.
- Цена, как правило, нелинейно зависит от числа копий (инсталляций, пользователей). Например, лицензия на 1 копию стоит 1 условную единицу, на 20 копий стоит 10, на 50 копий — 20. В случае, когда использована 21 копия, их стоимость можно оценить в 10,5 условных единиц, в 11, в 20 или даже в 21.

- Некоторые программы могут вообще не продаваться в какой-то стране, хотя и пользоваться там некоторым спросом.
- Правообладатели порой бесплатно распространяют версию ПО с урезанными функциями или ограниченным сроком действия (так называемые пробные, ознакомительные, тестовые или триальные версии), но при этом такая ограниченная версия вполне удовлетворяет все потребности пользователя. Бывает, что пробная версия и полноценная версия программы устанавливаются с одного и того же дистрибутива и начинают отличаться друг от друга только с момента регистрации.
- Программы могут не продаваться без соответствующего оборудования или вне определенного комплекта программ. Но при этом сохраняется техническая возможность использовать их отдельно. В таком случае официальная цена на отдельную программу либо вообще не объявляется, либо выставляется в 0. Стоимость при этом далеко не нулевая.

Исходя из упомянутых сложностей, автор рекомендует для оценки стоимости прав на использование программы для ЭВМ назначать не экономическую, а комплексную экспертизу, с участием двух экспертов — экономиста и ИТ-специалиста. Особенно, когда оценка осложнена такими обстоятельствами, как использование устаревшей, изъятой из продажи версии ПО, использование версии, лицензируемой бесплатно для некоторых категорий, превышение количества инсталляций и т.д.

Конечно, не по каждому делу о нарушении авторских прав обязательно проводить экспертную оценку стоимости ПО. Иногда стоимость можно оценить без эксперта, исходя из цены. Если определенная программа продается (лицензируется) по одинаковой цене для всех или подавляющего большинства потребителей, то такую цену можно считать ее стоимостью. При наличии нескольких цен для различных условий следователь или суд может принять в качестве оценки наименьшую из этих цен.

Распространенные ошибки при оценке стоимости контрафактных программ или иных произведений, из опыта автора, таковы:

- из нескольких действующих цен на продукт в качестве оценки стоимости берется одна, причем выбор никак не обосновывается;
- в качестве оценки стоимости продукта берется цена на другую версию продукта — более новую, более старую, на другом языке и т.д.;
- оценка стоимости произведения (прав на его использование) поручается компьютерно-технической экспертизе;
- вместо стоимости оценивается цена продукта или ущерб правообладателю;
- оценка стоимости поручается правообладателю или производится следователем из данных, предоставленных правообладателем (например, фирменного каталога цен);
- при оценке стоимости через цену не учитываются условия, в которых

обвиняемый использовал программу, например, не учитывается наличие в лицензионном договоре скидок, льгот, периода бесплатного использования.

Но главной и самой распространенной ошибкой, разумеется, является оценка стоимости без проведения экспертизы.

Разбор образцов

В этой главе мы рассмотрим образцы заключений эксперта, подробно разберем их и укажем на ошибки.

Автор предлагает три экспертных заключения. Все они взяты из реальных уголовных дел, рассмотренных в суде. Первый пример изобилует ошибками, второй имеет всего несколько недостатков, а третий пример почти идеален и может быть рекомендован в качестве образца.

Отрицательный пример

Первое заключение взято из уголовного дела по статьям 146 и 273 УК. Исследование проводил эксперт Центра независимой комплексной экспертизы и сертификации (ЦНКЭС). Полный текст заключения приводится на последующих иллюстрациях.

Для начала рассмотрим поставленные перед экспертом вопросы.

Первый вопрос поставлен правильно. Речь можно вести не о контрафактности, а именно о признаках контрафактности. Сам факт контрафактности (то есть нарушения авторских прав) эксперт установить не может. Так что вопрос сформулирован верно, разве что формулировка немного корявая. Контрафактными (согласно определению из ст. 48 закона «Об авторском праве...») бывают не диски или иные носители, а записанные на них экземпляры произведений. Ну и термин «CD-диск», хотя и понятен, но звучит не вполне по-русски: говорят либо «CD», либо «компакт-диск».

Второй и пятый вопросы (они фактически идентичны) автор переформулировал бы иначе. Дело в том, что правообладатель — это владелец имущественных авторских прав, каковые права являются отчуждаемыми. То есть правообладатель может измениться, если будет заключен соответствующий договор, но произведение при этом не изменится ни на бит. Иными словами, «лицо является правообладателем» — это факт не технический, а юридический. Эксперт, как и в предыдущем случае, может лишь обнаружить признаки или какие-либо указания, что лицо является обладателем исключительных прав на произведение, но не может установить факт обладания такими правами.

Третий и шестой вопросы откровенно юридически безграмотны и неприемлемы для КТЭ. Во-первых, эксперт не может установить контрафактность произведений. Во-вторых, при нарушении авторских прав

нельзя вести речь об ущербе. При незаконном воспроизведении или ином использовании произведений у правообладателя ничего не пропадает, поэтому ущерба как такового нет. Можно вести речь о недополученной прибыли или иных убытках, но оценить их достаточно сложно. Именно поэтому законодатель оперирует в ст. 146 УК понятием «стоимость». Именно стоимость экземпляров или прав на их использование является квалифицирующим признаком этого преступления. Если экс-

НА РАЗРЕШЕНИЕ ЭКСПЕРТА ПОСТАВЛЕНЫ СЛЕДУЮЩИЕ ВОПРОСЫ:

1. Имеют ли представленные на исследование экземпляры CD-дисков признаки контрафактности, если да, то какие?
2. Кто является правообладателем данной продукции?
3. Если представленные на исследование экземпляры нелегитимные (контрафактные), то какой ущерб причинен правообладателям?
4. Является ли программное обеспечение, установленное на представленных жестких дисках, лицензионным?
5. Кто является правообладателем продукции программного обеспечения, установленного на данных жестких дисках?
6. Если программное обеспечение, установленное на представленных жестких дисках нелегитимное (контрафактное), то какой ущерб причинен правообладателям?
7. Находятся ли на представленных на исследование экземплярах CD-дисках и жестком диске (HDD) вредоносные программы? Если находятся, то могли ли они быть применены для модификации программных продуктов, установленных на жестком диске и произошла ли указанная модификация?

НА ЭКСПЕРТИЗУ ПРЕДСТАВЛЕНЫ:

- Внутренний жесткий диск Seagate Barracuda, опечатанный полоской белой бумаги с подписями.
- Переносной жесткий диск CUTIE FHD-254, опечатанный полоской белой бумаги с подписями.
- Два CD диска, упакованные в пластиковый бокс, опечатанные полосками белой бумаги с подписями.

ЭКСПЕРТИЗА:

Экспертиза проводилась в помещении ЦНКЭС.

Перед началом экспертизы было произведено вскрытие печатей на упаковке с носителями для возможности съема информации на магнитные носители.

Экспертиза проводилась в два этапа: первый - экспертиза компакт-дисков и переносного жесткого диска, второй - экспертиза внутреннего жесткого диска.

Этап № 1. Экспертиза CD – дисков и переносного жесткого диска:

перт возьмется оценивать ущерб, он вынужден будет признать, что ущерб нулевой, а стоимость при этом не будет оценена, что затруднит или делает невозможной квалификацию деяния.

Четвертый вопрос также относится к контрафактности экземпляров. Термин «лицензионный» употребляется в обиходе как антоним к термину «контрафактный». А контрафактность экземпляров, как уже неоднократно подчеркивалось, эксперт установить не может. Поэтому данный вопрос сформулирован некорректно.

Седьмой вопрос в первой своей части поставлен правильно и относится к области КТЭ. Во второй своей части вопрос содержит скрытое утверждение, что вредоносные программы используются для модификации программных продуктов, то есть программ для ЭВМ. На самом деле вредоносные программы используются для модификации не произведений, а компьютерной информации, и указанные отношения регулируются законодательством об информации [70, 81]. А использование программ для ЭВМ регулируется законодательством об авторском праве, в сферу которого вредоносные программы (ст. 273 УК) не входят. Речь можно вести лишь о программном обеспечении для преодоления технических средств защиты авторских прав (ст. 48.1 закона «Об авторском праве...»). Поэтому вторая часть вопроса 7 некорректна.

Перейдем к разбору самого заключения.

Ввиду отсутствия необходимого оборудования, необходимого для подключения переносного жесткого диска к системному блоку Центра, экспертиза переносного жесткого диска CUTIE FHD-254 не проводилась.

На исследование представлены следующие компакт – диски:

Таблица 1.

| № п/п | Наименование (внешний вид) компакт - диска |
|-------|--|
| 1. | Весь Autocad 2006 |
| 2. | № A4408G5061902 |

В результате проведения экспертизы установлено, что представленные компакт – диски №№ 1,2 таблицы № 1 имеют существенные отличия от лицензионных (изготовленных и реализуемых с соблюдением всех требований законодательства РФ в части авторского права) компакт-дисков. Соответствующий вывод сделан по результатам осмотра внешнего вида, а также файловой структуры данных компакт-дисков при помощи загрузки в память ЭВМ записанных на них программ. Данные компакт-диски и программные продукты, содержащиеся на них, имеют явные признаки контрафактности.

Список компьютерных программ, имеющих явные признаки контрафактности и расчет их стоимости, приведены в Таблице 2.

АНО «НЦКЭС»
Экспертиза
Подпись Эксперта

Таблица 2.

| № п/п | Наименование (внешний вид) компакт - диска | Наименование программного продукта | Право обладатель | Стоимость, |
|-------|--|------------------------------------|------------------|------------|
| 1. | Весь Autocad 2006 | AutoCAD 2004 | AutoDesk | Нет данных |
| | | AutoCAD 2005 | AutoDesk | 2 160 Евро |
| | | AutoCAD 2006 | AutoDesk | 4 320 Евро |
| 2. | № A4408G5061902 | Windows XP Professional Russian | Microsoft | 251 у.е.* |

*1 у.е = 1 доллару США по курсу ЦБ РФ на день изъятия дисков.

Цены взяты из «Справочника цен на лицензионное программное обеспечение», разработанного Некоммерческим Партнерством Поставщиков Программных Продуктов (НПППП).

Признаки контрафактности компакт – дисков, представленных на исследование, следующие:

1. Оформление лицевой (нерабочей) поверхности лицензионных компакт-дисков.

На лицевую (нерабочую) поверхность лицензионного компакт-диска наносится изображение высокого полиграфического качества. По окружности внешней границы компакт-диска должны быть нанесены: надпись, содержащая информацию о регистрации торговых марок, об авторском и смежных правах на данную программу для ЭВМ (базу данных) и предупреждение о последствиях их нарушения. Экспертиза показала, что представленные компакт-диски не имеют каких – либо изображений и текстовой информации о торговых марках, авторском и смежном праве.

2. Оформление реверса (рабочей поверхности) лицензионных компакт-дисков.

Оформление реверса (рабочей поверхности) компакт-диска. Вдоль концентрических окружностей в центре лицензионного компакт-диска наносится методом гравировки код IFPI (код Международной федерации производителей фонограмм), позволяющий однозначно идентифицировать оборудование, на котором изготовлен данный компакт-диск, а также информация о заводе-изготовителе.

У представленных на экспертизу компакт-дисков код IFPI отсутствует. Производитель на компакт-дисках не указан.

Данные признаки являются существенными признаками контрафактности.

3. Упаковка лицензионных компакт-дисков.

АНО «НЦКЭС»
Экспертиза
Подпись Эксперта

Лицензионные программы для ЭВМ, как правило, упаковываются в картонную коробку, оформляемую согласно стандартам фирмы-изготовителя, имеющую несколько степеней защиты (микро печать, голограммы и т.п.). На коробке должна присутствовать информация о фирме-разработчике, авторских и смежных правах. Кроме того, в упаковочную коробку вкладывается многостраничная документация (инструкция пользователя) и лицензия на программный продукт.

Лицензионные программы для ЭВМ компании Microsoft упаковываются в картонные коробки, типоразмеры и оформление которых соответствуют корпоративным стандартам производителя и имеют несколько степеней защиты. Неотъемлемой частью каждого продукта является Лицензионное соглашение между покупателем и фирмой-производителем. Каждая Лицензия или Регистрационная карта пользователя имеет серийный номер программного продукта, без которого установка программного продукта невозможна. Представленные на экспертизу компакт-диски с программами данной фирмы таких компонентов не содержат.

На боковой стороне картонной коробки с программами Майкрософт имеется специальный сертификат, имеющий следующие свойства:

- теплочувствительная краска при трении изменяет цвет с голубого на белый;
- попытка отклеить сертификат вызывает его разрыв;
- поворот сертификата в лучах света обнаруживает символ "OK" на логотипе Майкрософт.

Представленные на экспертизу компакт-диски с программными продуктами фирмы Майкрософт в момент осмотра не были упакованы, не имели картонных упаковочных компонентов, документации, лицензий и регистрационных карточек.

Описание комплекта AutoCAD:

Коробка

- Размеры коробки продукта—примерно 17.8 x 22.8 см. Толщина коробки может составлять 5, 7, 7.6, 12.7 или 15.2 см.
- Версии с Release 14 по 2000 поставлялись в картонных коробках, одна половина которых вставлялась в другую сбоку. Начиная с семейства 2002, коробка открывается сверху и имеет сплетение клапанов на дне.
- Серийный номер и сведения о продукте находятся, как правило, на верхнем клапане.
- Шифр продукта и текст с правовой информацией находятся на дне коробки.

АНО
Эксперт
подпись

При анализе внешних признаков контрафактности компакт-дисков (с. 3-6) они были сопоставлены и сравнены с некими «лицензионными» дисками. Но образцы таких дисков для сравнения эксперту следователем не предоставлялись. А согласно ст. 57 УПК, эксперт не вправе самостоятельно собирать материалы для экспертного исследования; такие образцы должны быть направлены эксперту следователем в числе прочих материалов, необходимых для производства экспертизы, либо по отдельному запросу эксперта.

Кроме того, программные продукты выпускаются на рынок в различных вариантах и различном исполнении. Наряду с «коробочными» версиями (они же «retail» или «розничные») возможны OEM-версии, версии, распространяемые через Интернет, и иные варианты, всего многообразия которых эксперт может не знать. Даже сам правообладатель может не знать, в каком оформлении выпускают его программный продукт издатель, с которыми он заключил договоры. Поэтому непохожесть исследуемых дисков на диски «коробочной» версии продукта еще не есть признак контрафактности.

Чтобы внешний вид экземпляра стал признаком контрафактности, следует сравнить его с внешним видом всех имевших место официальных изданий всех издателей во всех странах. Сравнение лишь с одним-единственным образцом — некорректно.

Указание экспертом правообладателя является логическим продолжением ошибки следователя в постановке вопроса. Эксперт не может определить правообладателя произведения, поскольку это факт юридический, а не технический. Принадлежность имущественных авторских прав тому или иному лицу зависит от заключенных договоров и от факта создания произведения тем или иным лицом (лицами). Эксперт же исследует лишь экземпляр произведения. Поэтому он может найти на произведении сведения об авторах, уведомление о принадлежности авторских прав, текст лицензионного соглашения и иные признаки. Но лишь признаки. Из которых однозначный вывод о правообладателе сделать нельзя.

- Серийный номер продукта и текст с правовой информацией находятся на дне коробки

Содержимое коробки

Содержимое коробки зависит от конкретного продукта; ниже перечислены требования, общие для всех них:

- Большинство печатных руководств имеет формат 17.8 x 22.8 см и стандартный мягкий переплет. Обратите внимание, что для тонких книг такой переплет невозможен, и они обычно бывают скреплены по сгибу.
- На задней стороне обложки печатных руководств обязательно должен быть заводской шифр.
- Все содержимое коробки (начиная с семейства 2002) подчиняется единой цветовой схеме.

Компакт-диск

- CD упакован в картонный или гибкий пластиковый конверт; все надписи на конверте нанесены методом офсетной печати.

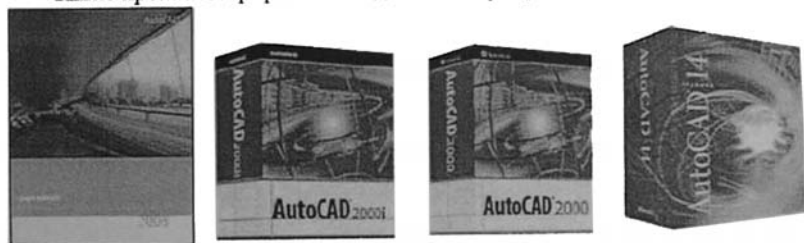
Примечание: AutoCAD 14 был последним продуктом, диск которого поставлялся в твердом пластмассовом футляре.

- Этикетка нанесена на диск методом шелкографии.

Примечание: Если этикетка отклеивается с диска, это свидетельствует о подделке.

- На внутреннем кольце CD нанесены номер партии и наименование завода-изготовителя тиража.

Ниже проиллюстрированы подлинные продукты компании Autodesk.



Представленный на экспертизу компакт-диск с программным продуктом фирмы Autodesk в момент осмотра был упакован в пластиковый бокс, не имел картонных упаковочных компонентов и документации.

Все эти признаки являются признаками контрафактности.

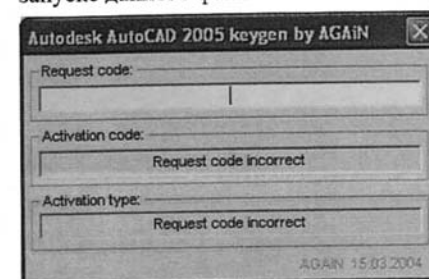
4. Наличие программ устраняющих защиту от несанкционированного копирования.

ПОДПИСЬ ЭКСПЕРТА

На компакт-диске не могут быть записаны программы для ЭВМ, позволяющие устранить либо обойти защиту от несанкционированного копирования.

На компакт-дисках находятся файлы вредоносных программ, позволяющие обойти встроенную в программные продукты средства защиты от несанкционированного копирования и получить тем самым незаконный доступ к программным продуктам компании Autodesk и компании Adobe, что является существенным признаком контрафактности представленных компакт-дисков с программными продуктами данных компаний.

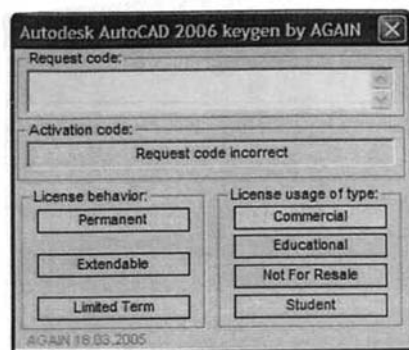
На компакт – диске «Весь Autocad 2006» в директории «..\Autocad 2005 Rus» обнаружен самораспаковывающийся файл-архив «AutoCAD2005Rus.exe», содержащий файл программы «keygen.exe». При запуске данного файла появляется следующий оконный интерфейс:



Установлено, что данная программа предназначена для генерации кода активации (не активированная копия программного продукта работать не будет) программного продукта «AutoCAD 2005» без ведома правообладателя – компании «AutoDesk» (т.е. с помощью программы можно осуществить доступ к компьютерной информации и копирование информации). На основании данного факта программа «keygen.exe» признана вредоносной.

На компакт-диске «Весь Autocad 2006» в директории «..\AutoCAD 2006 Rus\Crack» обнаружен файл программы «keygen.exe». При запуске данного файла появляется следующий оконный интерфейс:

ПОДПИСЬ ЭКСПЕРТА



Установлено, что данная программа предназначена для генерации кода активации (не активированная копия программного продукта работать не будет) программного продукта «AutoCAD 2006» без ведома правообладателя — компании «AutoDesk» (т.е. с помощью программы можно осуществить доступ к компьютерной информации и копирование информации). На основании данного факта программа «keygen.exe» признана **вредоносной**.

Этап № 2. Экспертиза жесткого диска.

Экспертиза представленного жесткого диска проводилась по следующей методике:

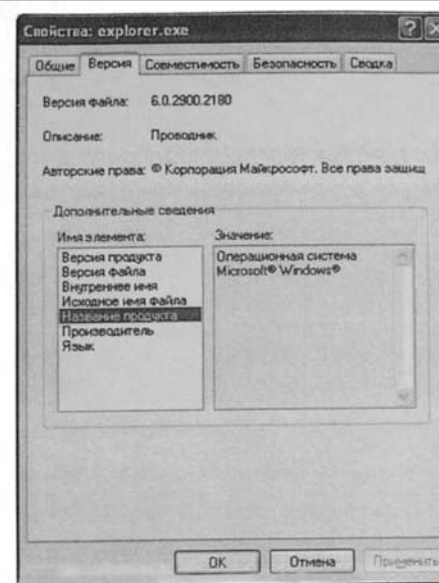
Жесткий диск был подключен к системному блоку Центра, после чего производился поиск информации, необходимой для ответа на поставленные вопросы.

В результате проведения экспертизы жесткого диска установлено:

На жестком диске в директории «C:\WINDOWS» обнаружен программный продукт Microsoft Windows XP Professional Russian, правообладатель компания Microsoft.

К признакам контрафактности обнаруженной операционной системы можно отнести факт возможной установки данной операционной системы с представленного на экспертизу компакт — диска № «A4408G5061902» (содержащего дистрибутив (установочные файлы) данной операционной системы, имеющего явные признаки контрафактности).

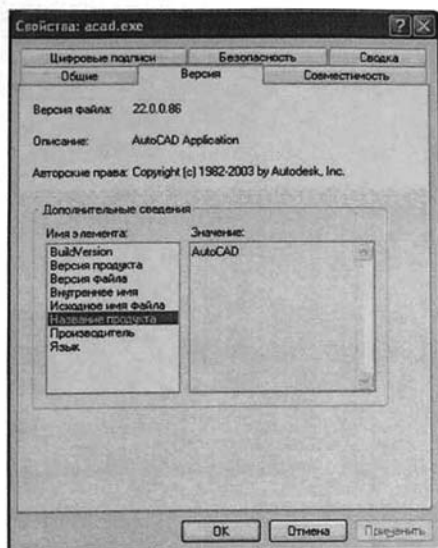
ЛЮ СЛЯКЗС
Экспертиза
Подпись Эксперта



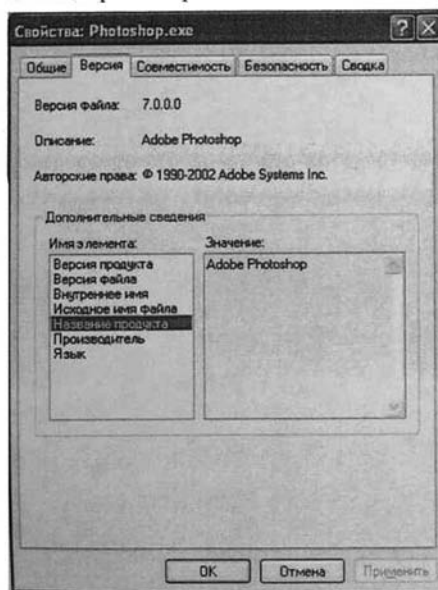
На представленном жестком диске в папке «C:\Program Files\AutoCAD 2005» обнаружен программный продукт «AutoCAD 2004» правообладатель компания «Autodesk». К признакам контрафактности данного программного продукта можно отнести возможный факт его установки с компакт — диска «Весь Autocad 2006», представленного на экспертизу, имеющего явные признаки контрафактности.

ЛЮ СЛЯКЗС
Экспертиза
Подпись Эксперта

Ряд иллюстраций, приведенных экспертом, не подписаны и не объяснены в тексте. У неспециалиста может создаться впечатление, что эти иллюстрации подтверждают правоту эксперта. На самом деле это не так.



На представленном жестком диске в папке «..\Program Files\Adobe\Photoshop 7.0» обнаружен программный продукт «Adobe Photoshop 7.0» правообладатель компания «Adobe».

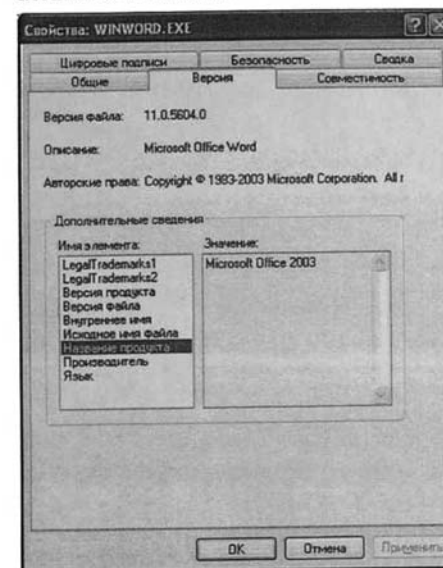


АНО «ПРИКЭС»
ЭКСПЕРТИЗА
ПОДПИСЬ ЭКСПЕРТА

Например, иллюстрация на странице 10 — это результат отображения некоторых атрибутов файла средствами операционной системы. Строчка «авторские права...» является лишь частью контента (ресурсов) файла «Photoshop.exe». Ее можно рассматривать как признак принадлежности авторских прав или как уведомление о таких правах. Но эксперт этого не объясняет. Он категорично утверждает «правообладатель — компания «Adobe», после чего приводит иллюстрацию, которую неспециалист может воспринять как подтверждение. Иными словами, отсутствие подписей к иллюстрациям вводит в заблуждение.

К признакам контрафактности данного программного продукта можно отнести возможный факт его установки с дистрибутива, имеющего признаки контрафактности, обнаруженного на представленном жестком диске (см. ниже).

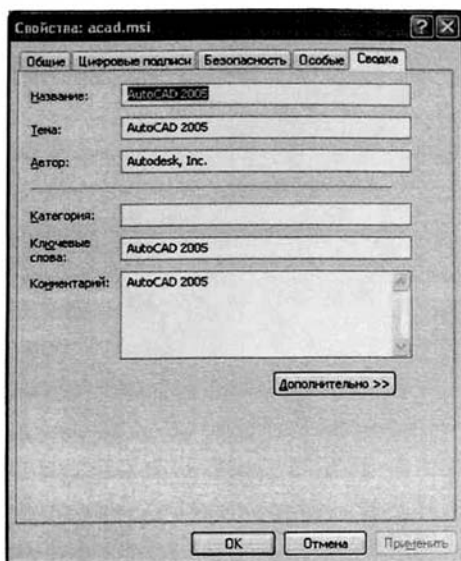
В папке «..\Program Files\Microsoft Office» обнаружен программный продукт «Microsoft Office 2003 Professional (Russian)», правообладатель компания Microsoft.



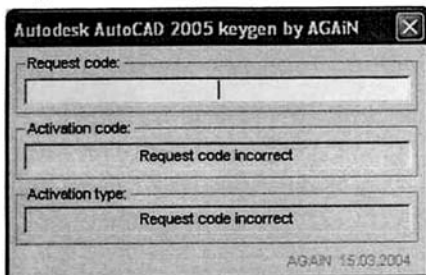
Признаков контрафактности данного программного продукта не обнаружено.

Так же на представленном внутреннем жестком диске в директории «..\Utils\Distrib\Autocad\Autocad 2005 RUS&ENG» обнаружен дистрибутив (установочные файлы) программного продукта «AutoCAD 2005» правообладатель компания «Autodesk».

АНО «ПРИКЭС»
ЭКСПЕРТИЗА
ПОДПИСЬ ЭКСПЕРТА



Явным признаком контрафактности данного программного продукта является наличие в директории, содержащий программный продукт поддиректории «crack» в которой содержится файл «keygen.exe». При запуске данного файла появляется следующий оконный интерфейс:



Установлено, что данная программа предназначена для генерации кода активации (не активированная копия программного продукта работать не будет) программного продукта «AutoCAD 2005» без ведома правообладателя — компании «AutoDesk» (т.е. с помощью программы можно осуществить доступ к компьютерной информации и копирование информации). На основании данного факта программа «keygen.exe» признана **вредоносной**.

Так же к признакам контрафактности обнаруженного дистрибутива программного продукта «AutoCAD 2005» можно отнести возможный факт его копирования с компакт — диска «Весь Autocad 2006», представленного на исследование, имеющего явные признаки контрафактности.

Экспертное заключение
С.А. Федотов

На жестком диске в директории «..\Utils\Distrib\Photoshop 7» обнаружен дистрибутив (установочные файлы) программного продукта «Adobe Photoshop 7.0» правообладатель компания «Adobe».

К признакам контрафактности данного программного продукта можно отнести возможный тот факт, что данный программный продукт (в виде дистрибутива) распространяется официально только на компакт — дисках. На других носителях дистрибутив программного продукта «Adobe Photoshop 7.0» официально не распространяется.

Сравнительный анализ программного обеспечения, установленного на представленном жестком диске и дистрибутивов программных продуктов, записанных на представленных на исследование компакт-дисках и жестком диске, содержащих программные продукты, имеющие признаки контрафактности, показал, что обнаруженные на жестком диске программные продукты могли быть установлены (либо скопированы) с представленных на исследование компакт-дисков и переносного жесткого диска (в соответствии с обнаруженными на данных носителях дистрибутивами программных продуктов).

Информация о стоимости обнаруженных на представленном жестком диске программных продуктов, имеющих признаки контрафактности, приведена в Таблице 3.

Таблица 3.

Расчет стоимости программ, имеющих признаки контрафактности, обнаруженных на жестком диске, представленном на экспертизу

| Программы, находящиеся на жестком диске | Правообладатель | Стоимость программного продукта |
|---|-----------------|---------------------------------|
| AutoCAD 2004 | Autodesk | Нет данных |
| AutoCAD 2005 (дистрибутив) | Autodesk | 2 160 Евро |
| Microsoft Windows XP Professional Russian | Microsoft | 251 у.е.* |
| Adobe Photoshop 7.0 | Adobe | Нет данных |
| Adobe Photoshop 7.0 (дистрибутив) | Adobe | Нет данных |

*1 у.е. = 1 доллару США по курсу ЦБ РФ на день изъятия жесткого диска.

Расчет стоимости программ

Для расчета стоимости программ принята следующая модель: для обнаруженного экземпляра программы с признаками контрафактности

Экспертное заключение
С.А. Федотов

Определение стоимости программ (прав на их использование) в соответствии с ценой является ошибкой. Тем более что из различных цен взята розничная, то есть максимальная.

Есть подозрение, что эксперт вообще не видит разницы между ценой и стоимостью. В тексте эти термины употребляются как синонимы.

определяется стоимость в соответствии с розничной ценой соответствующего лицензионного программного продукта на момент востребования носителей информации (компакт – дисков и жесткого диска).

В случае указания розничной цены программы в иностранной валюте, пересчет в рублевый эквивалент осуществляется по курсу ЦБ РФ на день изъятия информационных носителей.

Стоимость программ рассчитывалась по формуле $X * Y = Z$, где

X - Общее количество контрафактных экземпляров программ,

Y - Розничная цена экземпляра программы,

Z - Общая стоимость программ правообладателя.

Таким образом, стоимость программ на представленных компакт – дисках, составляет:

- компании «AutoDesk»:

6 480 (две тысячи сто шестьдесят) евро, что в пересчете согласно курсу ЦБ РФ на 07 июля 2006 г. (1 евро = 34 руб. 28,21 коп.) составляет 222 148 (двести двадцать две тысячи сто сорок восемь) рублей 01 коп.

- компании «Microsoft»:

251 (двести пятьдесят один) доллар 00 центов США, что в пересчете согласно курсу ЦБ РФ на 07 июля 2006 г. (1 доллар США = 26 руб. 91,11 коп.) составляет 6 754 (шесть тысяч семьсот пятьдесят четыре) рубля 69 коп.

Стоимость программ, установленных на представленном внутреннем жестком диске, составляет:

- компании «AutoDesk»:

2 160 (две тысячи сто шестьдесят) евро, что в пересчете согласно курсу ЦБ РФ на 07 июля 2006 г. (1 евро = 34 руб. 28,21 коп.) составляет 74 049 (семьдесят четыре тысячи сорок девять) рублей 34 коп.

- компании «Microsoft»:

251 (двести пятьдесят один) доллар 00 центов США, что в пересчете согласно курсу ЦБ РФ на 07 июля 2006 г. (1 доллар США = 26 руб. 91,11 коп.) составляет 6 754 (шесть тысяч семьсот пятьдесят четыре) рубля 69 коп.

И.Н. ФЕДOTOV
Эксперт
ПОДПИСЬ ЭКСПЕРТА

ВЫВОДЫ:

1. В результате проведенной экспертизы на представленных компакт – дисках (позиции №№ 1,2 таблицы № 1) обнаружены программные продукты, имеющие признаки контрафактности. Программы на компакт-дисках имеют следующие признаки контрафактности:

- отсутствие информации о торговых марках, а так же об авторском и смежных правах на лицевой поверхности;
- отсутствие полиграфического изображения на лицевой поверхности;
- отсутствие кода IFPI (код Международной федерации производителей фонограмм);
- отсутствие упаковочной коробки и документации;
- наличие на компакт-дисках вредоносных программ, позволяющих обойти защиту от несанкционированного копирования.

2. Правообладателями обнаруженных программных продуктов на компакт-дисках являются корпорация «Microsoft», компания «AutoDesk».

3. Стоимость программ, на представленных компакт – дисках, составляет:

- компании «AutoDesk»:

222 148 (двести двадцать две тысячи сто сорок восемь) рублей 01 коп.

- компании «Microsoft»:

6 754 (шесть тысяч семьсот пятьдесят четыре) рубля 69 коп.

4. Ввиду отсутствия необходимого оборудования, необходимого для подключения переносного жесткого диска к системному блоку Центра, экспертиза переносного жесткого диска CUTIE FHD-254 не проводилась.

Программные продукты, установленные на представленном на экспертизу жестком диске, имеют следующие признаки контрафактности:

- Установка программных продуктов с компакт – дисков, представленных на экспертизу, содержащих программные продукты, имеющие явные признаки контрафактности.
- Наличие вредоносной программы в директории, содержащий программный продукт.
- Несоответствие типа носителя, содержащего дистрибутив (установочные файлы) программного продукта, носителю,

И.Н. ФЕДOTOV
Эксперт
ПОДПИСЬ ЭКСПЕРТА

Разберем выводы эксперта.

Целый раздел заключения эксперта посвящен анализу программ для обхода технических средств защиты авторских прав. Эксперт ошибочно объявляет их вредоносными программами. Это утверждение не основано на законе, поскольку такие программы не приводят заведомо к несанкционированному копированию, модификации или уничтожению информации [21, 81]. А такая программа, как генератор ключей активации, вообще не приводит к копированию, модификации или уничтожению какой-либо информации.

При поиске признаков контрафактности копии ОС «Windows», которая установлена на исследуемом НЖМД, эксперт приводит единственный такой признак, дословно: «факт возможной установки данной операционной системы с представленного на экспертизу компакт-диска» (с. 8). Такой же, единственный признак контрафактности эксперт указывает для продукта «Photoshop» (с. 11). Других признаков контрафактности экземпляров этих программ эксперт не указывает. Однако в выводах (с. 15) при указании признаков контрафактности написано «установка программных продуктов с компакт-дисков», а слово «возможная» пропало. Итак, вывод относительно контрафактности «Windows» и «Photoshop» сформулирован экспертом категорично, хотя он основан на единственном признаке, который носит предположительный характер.

Оценка стоимости. Здесь эксперт исправил ошибку следователя, который ошибочно поставил вопрос об ущербе. Эксперт же отвечает на вопрос не об ущербе, а о стоимости прав на использование произведений.

Но оценка стоимости прав на использование соответствующих программ для ЭВМ может производиться в ходе экономической или товароведческой экспертизы. КТЭ не может дать такую оценку.

Кроме того, эксперт допустил ошибку, взяв цену на продукт «AutoCad» из справочника цен. Этот продукт имеет множество версий и несколько вариантов лицензий для разных условий его использования. Соответственно, нет и не может быть единой цены на этот продукт. Для данного уголовного дела ошибка эксперта усугубляется еще и тем, что лицензия на «AutoCad» предусматривает период бесплатного его использования, так называемое «trial use», или пробное использование. В этом режиме продукт устанавливается с того же самого дистрибутива. Следовательно, стоимость прав на такой вид использования составляет ноль. Понятно, что не имеет смысла говорить о стоимости экземпляров или прав на использование программы для ЭВМ, пока не выяснено, каким именно способом программу использовали или намеревались использовать. Нет смысла говорить о стоимости без изучения условий лицензионного договора. Особенно когда договор предусматривает бесплатные варианты использования. Очевидно, что такие вопросы, как анализ лицензионного договора, технический эксперт решать не имеет права.

Автор сомневается, может ли данное заключение служить отрицательным примером для разбора возможных ошибок эксперта. Скорее, стоит вести речь не об ошибках, а о тенденциозности и ангажированности эксперта.

Тем не менее на основе этого примера сформулируем перечень типичных ошибок при назначении и проведении КТЭ:

- недопустимые вопросы перед экспертом (см. главу «Неприемлемые вопросы»);
- содержащееся в формулировке вопроса неявное утверждение;
- проведение техническим экспертом оценочной деятельности (экономической экспертизы);
- проведение техническим экспертом экспертизы по установлению автора (автороведческой экспертизы) или правообладателя;
- использование экспертом сравнительных образцов, полученных из неуказанного источника, вопреки установленному УПК порядку;
- путаница вредоносных программ и программ для обхода технических средств защиты авторских прав [21, 70, 81].

Промежуточный пример

Приведенное ниже заключение автор мог бы охарактеризовать как добросовестное, но проведенное без должной тщательности и без использования специальных технических средств.

.....

**МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РФ
УПРАВЛЕНИЕ ВНУТРЕННИХ ДЕЛ КУРГАНСКОЙ ОБЛАСТИ
ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКОЕ УПРАВЛЕНИЕ**

г. Курган, ул. С.Васильева, 30а

тел. 41-60-75

ПОДПИСКА

Мне, Иванову Ивану Ивановичу, разъяснены в соответствии со ст. 199 УПК РФ права и обязанности эксперта, предусмотренные ст. 57 УПК РФ. Об ответственности за дачу заведомо ложного заключения по ст. 307 УК РФ предупрежден.

27 декабря 2002 г.

И.И.Иванов

ЗАКЛЮЧЕНИЕ ЭКСПЕРТА №12

г. Курган

9 января 2003 года

Производство экспертизы

Начато в 10 ч.00 мин. 27 декабря 2002 г.

Окончено в 15 ч.40 мин. 9 января 2003 г.

Старший эксперт МЭКО при ЭКУ УВД Курганской области старший лейтенант милиции Иванов И.И., имеющий высшее образование и стаж экспертной работы четыре года, на основании постановления о назначении экспертизы, вынесенного 26 декабря 2002 года старшим следователем СЧ СУ при УВД Курганской области старшим лейтенантом юстиции Пуховой А.М., по материалам уголовного дела №123456 произвел судебную компьютерно-техническую экспертизу.

ОБСТОЯТЕЛЬСТВА ДЕЛА

18.12.02 г. у Остановочного комплекса «Спорткомплекс «Зауралец» у Лоськова обнаружена и изъята денежная купюра достоинством 50 рублей серии «яч 8080000» образца 1997 г. с признаками подделки. Предварительным следствием установлено, что данная купюра изготовлена на компьютерном оборудовании, принадлежащем Прокопьеву А.Н. при помощи сканера, принадлежащего Дайданову И.Ю. По делу изъяты системные блоки, принадлежащие Прокопьеву А.Н., Дайданову И.Ю., цветные принтеры, дискеты.

НА ИССЛЕДОВАНИЕ ПРЕДСТАВЛЕНЫ:

1. Системный блок компьютера, изъятый у Прокопьева А.Н.

ПЕРЕД ЭКСПЕРТОМ ПОСТАВЛЕНЫ ВОПРОСЫ:

Имеются ли на жестком диске представленного системного блока файлы, которые содержат изображения денежных купюр?

ИССЛЕДОВАНИЕ:

1. ВНЕШНИЙ ОСМОТР

Объект на экспертизу доставлен нарочным.

Системный блок компьютера представлен без упаковки. Лицевая и боковые стороны системного блока заклеены фрагментами прозрачной липкой ленты типа «скотч». Этими же фрагментами ленты прикреплен лист бумаги, закрывающий лицевую сторону системного блока, и два фрагмента бумаги с оттисками круглой печати «№9*УВД Курганской области*МВД Российской Федерации». На одном фрагменте бумаги имеются росписи. К верхней стороне системного блока фрагментами прозрачной бесцветной липкой ленты типа «скотч» прикреплен лист бумаги. На листе бумаги имеется пояснительный рукописный текст: «Системный блок, изъятый у Прокопьева А.Н.».

Системный блок представляет собой IBM совместимый компьютер конфигурации ATX (см. Приложение, рис. 1).

Системный блок состоит из следующих комплектующих.

| Таблица 1. | | | | |
|--------------------|----------------------------|---------------|----------------|----------------------|
| Комплектующие | Марка (фирма-изготовитель) | Модель | Серийный номер | Примечание |
| Системный (корпус) | | Minitower ATX | | Серийный номер блока |

| | | | | |
|---------------------|--------------------------|----------------------------|--|-------------------|
| | | | | питания 456578 |
| Материнская плата | GIGABYTE P4 Titan533 | GA-8IEX | 0232002204 | |
| Процессор | INTEL | CELERON 1.8GHZ | 3226A475-1311 | 2 шт. |
| Модули памяти | | M10718 PC2100 128Mb | На каждом имеется наклейка оранжевого цвета с маркировкой «52765048» | |
| Дисковод | MITSUMI | D359M3D | P4DM9080874 | 3,5" |
| Видеокарта | PalitDaytona | GEFORCE4 MX440 64MB TV-OUT | 71ATO02029709 | |
| Жесткий диск (НЖМД) | Seagate Barracuda ATA IV | ST340016A | 3H58EB3M | 40 Гб |

При включении представленного системного блока (без жесткого диска) установлено, что системные дата и время соответствуют текущим.

Для производства исследования использовалась стендовая ПЭВМ с процессором Intel Pentium III-1000 с тактовой частотой 1000 Мгц, ОЗУ 256 Мб и жестким диском 60 Гб. На стендовой ПЭВМ были установлены: операционная система (ОС) Windows 98 русская версия, программная оболочка Windows Commander версия 3.52, пакет программ Norton Utilities, пакет программ Microsoft Office, программа Kaspersky Anti Virus (AVP) версия 3.5.133.0, программа ADCSee32 версия 2.4, программа AVSearch v3.12a, CorelDRAW v9.337.

Для просмотра информации с жесткого диска представленного компьютера она предварительно копировалась на дополнительный жесткий диск стендовой ПЭВМ емкостью 6,5 Гб. Для восстановления удаленных файлов использовалась программа UnErase Wizard из пакета Norton Utilities. Следует отметить, что не все файлы, восстанавливаемые данной программой, пригодны к использованию. Поэтому рассматривались только восстановленные неповрежденные файлы, которые могли быть безошибочно использованы каким-либо имеющимся программным обеспечением на стендовой ПЭВМ. Удаленные файлы во избежание повреждения информации восстанавливались на диск стендового компьютера.

Исследуемый жесткий диск подключали к стендовому компьютеру в качестве дополнительного съемного диска. Работа по исследованию представленного НЖМД включала в себя общий осмотр жесткого диска, просмотр выявленных файлов, восстановление и просмотр удаленных файлов. Для просмотра каталогов и файлов с НЖМД исследуемого системного блока они предварительно копировались на диск стендового компьютера. В результате общего осмотра НЖМД установлены следующие признаки, которые сведены в таблицу 2.

Таблица 2.

| Общие признаки исследуемого НЖМД | | | | | | | | |
|----------------------------------|---------------|---------------------|------------------------------|------------------------|------------------|---------------|-------------------|----------------|
| Объект | Емкость диска | Количество разделов | Имя раздела (диск в системе) | Емкость раздела (байт) | Файловая система | Занято (байт) | Каталогов (папок) | Файлов (всего) |
| НЖМД | 40Гб | 2 | HARDC (C:) | 10476945408 | FAT32 | 9545441280 | 2115 | 41268 |
| | | | HADR2 (D:) | 29514285056 | FAT32 | 25102516224 | 2109 | 33539 |

В результате осмотра НЖМД обнаружены файлы.

Таблица 3.

| Файлы, содержащие информацию по уголовному делу, находящиеся на представленном НЖМД | | | | |
|---|------------------------------------|-----------|-----------------------------------|--|
| № п/п | Путь | Имя файла | Размер (в байтах), дата создания | Описание файла |
| 1 | D:\Рефераты\editors\рефффф\рефффф\ | 4.cdr | 1105302 08.12.2002 15:35:12 | Содержит графическое изображение оборотной стороны купюры достоинством 50 рублей. Файл распечатан из графического редактора CorelDRAW v9.337 на принтере фирмы EPSON модели EPSON STYLUS C62 (см. Приложение с. 4) |
| 2 | D:\Рефераты\editors\рефффф\рефффф\ | 5.cdr | 1144538 08.12.2002 15:35:22 | Содержит графическое изображение лицевой стороны купюры достоинством 50 рублей. Файл распечатан из графического редактора CorelDRAW v9.337 на принтере фирмы EPSON модели EPSON STYLUS C62 (см. Приложение с. 5) |

При осмотре НЖМД, файлов, в удаленном виде содержащих графические изображения денежных купюр, не обнаружено.

ВЫВОД

На НЖМД системного блока, представленного на экспертизу, имеются файлы, содержащие графические изображения денежных купюр. Файлы описаны в таблице 3 заключения и распечатаны в Приложении к заключению эксперта (с. 4, 5).

Эксперт

И.И.Иванов

Постановка вопроса эксперту представляется чрезмерно лаконичной. По уголовному делу подлежат доказыванию различные обстоятельства. Эксперт в состоянии не только установить факт наличия изображения денежной купюры на компьютере, но также сказать кое-что про следующие обстоятельства:

- когда это изображение было туда помещено;
- при помощи каких средств это изображение было изготовлено и/или обработано;
- когда оно было изготовлено;
- есть ли следы обработки, распечатки, копирования этого изображения.

Возможно, не на все перечисленные вопросы эксперт мог дать категоричный ответ. Возможно, на некоторые из них он ответил бы предположительно. Все равно такие ответы послужили бы к изобличению фальшивомонетчиков. Простое присутствие изображений денежных купюр на компьютере еще ни о чем не говорит. К примеру, на компьютере автора эти изображения также присутствовали, поскольку они были приложены к заключению эксперта, которое автор получил от своего корреспондента в электронном виде.

Судя по описанию компьютера, он был опечатан неправильно, то есть не опечатаны разъемы питания и подключения периферии. Если автор правильно понял написанное экспертом, то следует признать, что неизменность доказательств не была обеспечена. И этот факт добросовестный эксперт обязан был указать в своем заключении открытым текстом. Если же автор понял неправильно и разъемы компьютера все-таки были опечатаны, то следует отметить неясность в формулировках.

Эксперт вовсе не обязан подробно описывать внешний вид и состояние объекта исследования. Такое описание, конечно, не повредит. Однако оно не требуется. А вот что точно требуется для правильной оценки доказательств — это неизменность. Эксперт, по мнению автора, обязан отразить свое мнение по поводу сохранности и неизменности компьютерной информации на исследуемом объекте. Например, так: «состояние печатей свидетельствует, что доступ к содержащейся в компьютере информации был невозможен с момента изъятия до момента начала экспертизы».

Положительный пример

Далее приводится заключение, которое если и не идеально, то может служить образцом почти для всех российских экспертов.

Перед экспертом поставлены вопросы:

1) Имеются ли в памяти системного блока персонального компьютера, изъятого в НГКИ, файл, содержащий текстовый фрагмент согласно Приложению? Если данный файл имеется, то каково его месторасположение в памяти системного блока компьютера?

2) Какова дата создания данного файла?

3) Удалялся ли данный файл, если да, то какова дата его удаления?

4) Подлежит ли данный файл восстановлению, если да, то имеется ли возможность изготовить его копию на бумажном носителе?

Внешний осмотр поступивших объектов

Картонная коробка, заклеенная фрагментами бумаги, на поверхности которых имеются отпечатки круглой печати: «УБОП при УВД ЯНАО*МВД РФ УПРАВЛЕНИЕ ПО БОРЬБЕ С ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ*ИНН 8901003107*ПРИ УПРАВЛЕНИИ ВНТРЕННИХ ДЕЛ ЯМАЛО-НЕНЕЦКОГО АО ЗОНАЛЬНЫЙ ОТДЕЛ г. НОЯБРЬСКА» и рукописный текст «ПОНЯТЫЕ 1 (подпись), 2 (подпись)». Целостность упаковки и отпечатков печати видимых повреждений не имеет. При вскрытии упаковки извлечен системный блок в корпусе светло-серого цвета (металлик) типоразмера «MiddleTower» максимальными размерами 42,0X18,0X43,4 см (высота X ширина X длина). Лицевая декоративная наклейка выполнена из пластмассы черного цвета.

Копия письма (представлена в Приложении к заключению эксперта).

ИССЛЕДОВАНИЕ

1. План исследования

1.1 Исследование системного блока производили в следующей последовательности:

- исследование состояния системного блока и определения его технических характеристик;
- исследование состояния накопителя (НЖМД) и определение его технических характеристик;
- исследование файловой системы и информации на НЖМД;
- исследование программного обеспечения на НЖМД;
- исследование компьютерной информации с целью поиска текстовых файлов;
- исследование компьютерной информации с целью поиска удаленных файлов и их последующего восстановления;
- исследование компьютерной информации с целью поиска программного обеспечения для защиты информации и поиск файлов, защищенных при помощи данного программного обеспечения.

2. Методика исследования

2.1. Исследование системного блока производили по следующей методике:

Исследование состояния системного блока проводилось по следующей методике:

- производилось вскрытие корпуса системного блока;
- визуальным осмотром устанавливался состав внутренних аппаратных компонентов (комплектующих устройств) представленного на исследование системного блока;

– из системного блока извлекался НЖМД; процедура изъятия носителя данных обусловлена требованием полной сохранности исследуемой информации путем обеспечения условий, исключающих какую-либо запись на них новых данных;

– к системному блоку в соответствии с эксплуатационными правилами подключались электропитание, монитор и клавиатура;

– системный блок включался, производилась загрузка операционной системы с системной дискеты эксперта, определение установленной системной даты и времени, диагностирование входящих в системный блок устройств.

Исследование состояния НЖМД (установленного в системном блоке) проводилось последовательно по следующей методике:

– визуальным осмотром устанавливался интерфейс, состояние перемычек и переключателей НЖМД;

– исследуемый НЖМД помещался в стендовую ПЭВМ; производилась загрузка операционной системы с загрузочного компакт-диска эксперта (сохранность данных на исследуемом НЖМД обеспечивалась утилитой PDBlock Lite фирмы Digital Intelligence Inc.) и программой partinfo.exe (из комплекта PowerQuest Partition Magic 8.0), определялись технические параметры НЖМД (количество цилиндров, сторон (головок), секторов на треке, количество секторов, размеров секторов и емкости);

– выявлялись таблицы разделов НЖМД с определением их основных параметров (начало и конец раздела, тип файловой системы, идентификаторы и метки разделов);

– определялась логическая адресация системных областей разделов НЖМД (загрузочной записи, главной файловой таблицы MFT, корневого каталога);

– производился поиск признаков повреждения целостности структуры данных (несоответствие заявленных параметров раздела фактическим, наличие сбойных, потерянных кластеров) и устанавливалась возможность доступа к данным на исследуемом НЖМД;

– исследуемый НЖМД помещался во внешний корпус для быстрой смены НЖМД, подключался к лабораторному компьютеру по USB-порту (сохранность данных на исследуемом НЖМД обеспечивалась программой NCSF Software Write-block XP организации National Center For Forensic Science);

– производилось создание файла-образа, содержащего точную копию исследуемого НЖМД на вспомогательном НЖМД лабораторного компьютера путем посекторного копирования с фиксацией технических параметров формата носителя с использованием специального программного обеспечения для экспертного исследования компьютерных носителей информации;

– осуществлялся вывод в файл на НЖМД лабораторного компьютера списка всех папок (каталогов) и файлов логических дисков исследуемого НЖМД.

Исследование файловой системы и информации на НЖМД системного блока, поступившего на экспертизу, проводилось по следующей методике:

– производился поиск файлов с расширением имен, соответствующих программам-архиваторам; выявленные архивные файлы разархивировались в отдельную папку (каталог) на НЖМД лабораторного компьютера;

– производился поиск удаленных файлов; файлы, подлежащие восстановлению, восстанавливались в отдельную папку (каталог) НЖМД лабораторного компьютера;

– производился поиск скрытых (зашифрованных) данных (логических и виртуальных дисков, папок (каталогов) и файлов данных);

– определялись признаки поиска информации (ключевые слова, изображения, расширения имен файлов и т.д.), соответствующие задачам исследования;

– производился поиск файлов, содержащих искомые признаки, с помощью специальных программ поиска информации на исследуемом носителе данных (точной копии) и в каталогах с восстановленными и разархивированными файлами на лабораторном компьютере;

– осуществлялся просмотр (визуализация) выявленных файлов, содержащих искомые признаки с помощью соответствующего программного обеспечения;

– производилась распечатка информации из файлов, содержание которых соответствует задачам исследования.

3. Экспертное оборудование и методическая литература, использованные при проведении исследования

3.1. Аппаратно-программный комплекс для экспертного исследования компьютерных носителей информации в составе:

– персональная ЭВМ на базе процессора AMD Athlon XP-M 3000+ производства фирмы «MEDION» (Германия);

– лазерный принтер «HP LaserJet 1200» производства «Hewlett Packard» (США);

– внешний корпус для быстрой смены НЖМД модель USB2.0-HDD3-EUR-1;

– программное обеспечение для экспертного исследования компьютерных носителей информации «EnCase Forensic Edition v.4.20» производства «Guidance Software Inc.» (США);

– операционная система «Microsoft Windows XP Home Edition» производства «Microsoft» (США);

– прикладное программное обеспечение «Microsoft Word» производства «Microsoft» (США);

– антивирусное программное обеспечение «eTrust Antivirus v.7.1.192» фирмы «Computer Associates International Inc.»;

– сервисное программное обеспечение «PDBlock Lite» фирмы «Digital Intelligence Inc.»;

– сервисное программное обеспечение «NCSF Software Write-block XP» организации «National Center For Forensic Science»;

– сервисное программное обеспечение «Partition Magic 8.0» фирмы «PowerQuest».

3.2. Методическая и справочная литература:

Зубаха В.С., Саенко Г.В., Усов А.И. и др. Общие положения по назначению и производству компьютерно-технической экспертизы: Методические рекомендации. – М.: ГУ ЭКЦ МВД России, 2001;

Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. М., 2001;

Усов А.И. Методы и средства решения задач компьютерно-технической экспертизы: Учебное пособие. – М.: ГУ ЭКЦ МВД России, 2002;

Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения: Учебное пособие / А.И.Усов // Под ред. проф. Е.Р.Россинской. М., 2003;

EnCase Forensic Edition v.4. Руководство пользователя. Guidance Software, 2003;

Тушканова О.В. Терминологический справочник судебной компьютерной экспертизы: Справочное пособие. – М.: ГУ ЭКЦ МВД России, 2005.

4. Результаты исследования

4.1. Исследование системного блока:

Визуальным осмотром установлено, что корпус системного блока, представленного на экспертизу, внешних повреждений не имеет. Правая боковая сторона системного блока опечатана двумя бумажными пломбами с №№007574, 007573. Представленный системный блок состоит из следующих комплектующих:

| Таблица 1. Комплектующие, входящие в состав системного блока | | | | |
|---|--------------------------------|----------------------------|--|---|
| Комплек- тующие | Фирма изготовитель Марка | Модель | Серийный номер | Примечание |
| Блок питания Материнская плата Процессор | ASUS | 200X PSLD2-VM | 5AM0AB050239 | Не извлекался в связи с высо- кой вероятностью повреждения |
| | INTEL | | Серийный номер на вентиляторе 5622D | |
| Модуль памяти Дисковод (НГМД) | GEIL | 512MB PC2-4300 DDR2-533 | GX25124300X | Эксперт вводит 7200.7 |
| | NEC | FD1231H | JAPL58JC0026 | |
| НЖМД Barracuda | Seagate, | ST3160812AS | 5LS06CZY обозначение – | |
| | НЖМД NEC Corporation | ND-4550A | 5XC9R92S111 | |
| Привод компакт- дисков | | | | |

Для последующего исследования на стендовом экспертном оборудовании произведено изъятие из системного блока указанного НЖМД.

В результате исследования состояния системного блока, без НЖМД, установлено:

– значение системной даты, имеющееся в BIOS представленного на исследование системного блока, соответствует текущей;

– значение системного времени, имеющееся в BIOS представленного на исследование системного блока, соответствует текущему.

Исследование информации на НЖМД.

Исследование состояния накопителя на жестких магнитных дисках (НЖМД).

Исследуемый НЖМД помещался в стендовую ПЭВМ; производилась загрузка операционной системы с загрузочного компакт-диска эксперта (сохранность данных на исследуемом НЖМД обеспечивалась утилитой PDBlock Lite фирмы Digital Intelligence Inc.) и программой partinfo.exe (из комплекта PowerQuest Partition Magic 8.0), определялись технические параметры НЖМД (количество цилиндров, сторон (головок), секторов на треке, количество секторов, размеров секторов и емкости);

– выявлялись таблицы разделов НЖМД с определением их основных параметров (начало и конец раздела, тип файловой системы, идентификаторы и метки разделов, размер и количество кластеров);

– определялась логическая адресация системных областей разделов НЖМД (загрузочной записи, главной файловой таблицы MFT, корневого каталога).

В результате исследования установлены следующие параметры исследуемого НЖМД:

Таблица 2.

| № п/п | Значения параметров НЖМД | | | |
|-------|--|--|--|--|
| | Количество цилиндров в системе адресации CHS | Количество головок в системе адресации CHS | Количество секторов на дорожке в системе адресации CHS | Значение хэш-функции, рассчитанное для НЖМД по алгоритму MD5 |
| НЖМД | 19457 | 255 | 16 | C7124548E12795B9C15BCEEE1BDF10E9 |

Исследуемый НЖМД имеет параметры разделов, приведенные в таблицах №№3, 4.

Таблица 3.

| № п/п | Раздел | Тип раздела | Начало раздела | | | Конец раздела | | |
|-------|-----------------------|-------------|----------------|---------|--------|---------------|---------|--------|
| | | | Цилиндр | Сторона | Сектор | Цилиндр | Сторона | Сектор |
| НЖМД | №1 (C:) | NTFS | 0 | 1 | 1 | 5098 | 254 | 63 |
| | | Extended | 5099 | 0 | 1 | 16708 | 254 | 63 |
| | №2 (D:) | NTFS | 5099 | 1 | 1 | 16708 | 254 | 63 |
| | | | 16709 | 0 | 1 | 19456 | 254 | 63 |
| | | | | | | | | |
| | Неразмеченная область | | | | | | | |

Таблица 4.

| № п/п | Раздел | Формат раздела | Номер раздела | Метка раздела | Объем раздела (байт) | Занято (байт) |
|-------|---------|----------------|---------------|---------------|----------------------|---------------|
| НЖМД | №1 (C:) | NTFS | 183ED056 | | 41940669952 | 3829933568 |
| | №2 (D:) | NTFS | 942AB287 | | 95495468032 | 70546432 |

Исследуемый НЖМД не имеет повреждений целостности структуры данных, доступ к данным возможен.

Исследование файловой системы и информации на НЖМД.

Исследуемый НЖМД подключали к лабораторному компьютеру в качестве внешнего съемного диска по USB-шине. Исследуемый НЖМД защищали от записи с помощью программного средства блокирования записи NTFS Software Write-block XP (блокиратора записи, разработанного National Center For Forensic Science). Исследование файловой системы и информации, содержащейся на НЖМД, проводилось на точной копии (образе) исследуемого накопителя, созданного на лабораторном компьютере с помощью программного обеспечения для экспертного исследования компьютерных носителей информации EnCase Forensic Edition v.4.20, а также в каталогах с восстановленными и разархивированными файлами на лабораторном компьютере.

Исследованием установлено, что на НЖМД имеются удаленные и подлежащие восстановлению файлы. Восстановление удаленной информации произведено при помощи программного обеспечения для экспертного исследования компьютерных носителей информации EnCase Forensic Edition v.4.20 в отдельную папку (каталог) на лабораторном компьютере.

Исследованием установлено, что на НЖМД имеются файлы с расширением имен, соответствующих программам-архиваторам, которые содержат архивные файлы. Разархивация выявленной информации произведена в отдельную папку (каталог) на лабораторном компьютере.

На НЖМД с помощью программного обеспечения для экспертного исследования компьютерных носителей информации EnCase Forensic Edition v.4.20 произведен контекстный поиск информации, соответствующей задаче исследования. В результате проведенного поиска обнаружены файлы, содержащие данные, соответствующие задаче исследования. Обнаруженные файлы описаны в таблице.

Таблица 5.

| Файлы, обнаруженные на НЖМД | | | | | |
|-----------------------------|------------|---|------------|---------------|------------------------|
| № п/п | Накопитель | Путь | Имя файла | Размер (байт) | Примечание |
| 1 | НЖМД | C:\RECYCLER\S-1-5-21-1456376166-2215607188-3175822896-1614\ | Dc5835.doc | 21504 | Файл распечатан, с. 12 |
| 2 | НЖМД | C:\RECYCLER\S-1-5-21-1456376166-2215607188-3175822896-1614\ | Dc5780.tmp | 21504 | Файл распечатан, с. 13 |

Кроме того, в свободной области НЖМД (в области, не относящейся к конкретному файлу файловой системы) в секторах 30761049594-30761051724 и 30762325498-30762327628 обнаружена информация, аутентичная содержанию копии письма, которая распечатана на с. 10, 11.

Обнаруженные файлы являются удаленными файлами. Определить время удаления файлов не представляется возможным, так как файловая система в данном случае не сохранила подобную служебную информацию. На основе анализа данных, находящихся в \$MFT НЖМД, представленного на исследование, установлено, что удаленный файл Dc5835.doc имел имя файла в файловой системе «Письмо Петрову.doc»

Анализом метаданных обнаруженных файлов установлено:
 Файл **Dc5835.doc** содержит в метаданных следующие сведения:
 Создан: 02.09.2004 11:37:00
 Изменен (дата последнего сохранения): 13.09.2005 18:21:00
 Напечатан (последний раз): 01.10.2004 13:45:00

Автор: IVANOVA
 Организация: OFFICE
 Редакция: 3
 Общее время правки (в минутах): 63

Авторы последних 10 изменений:

Таблица 6.

| Автор | Путь |
|---------|--|
| IVANOVA | C:\Documents and Settings\IVANOVA\Application Data\Microsoft\Word\Автокопия Документ1.asd |
| IVANOVA | C:\Documents and Settings\IVANOVA\Мои документы\письма\Письмо Петрову.doc |
| IVANOVA | C:\Documents and Settings\IVANOVA\Application Data\Microsoft\Word\Автокопия Письмо Петрову.asd |
| IVANOVA | C:\Documents and Settings\IVANOVA\Мои документы\письма\Письмо Петрову.doc |
| IVANOVA | C:\Documents and Settings\IVANOVA\Мои документы\письма\Письмо Петрову.doc |

Файл Dc5780.tmp содержит в метаданных следующие сведения:
 Создан: 02.09.2004 11:37:00
 Изменен (дата последнего сохранения): 13.09.2005 18:21:00
 Напечатан (последний раз): 01.10.2004 13:45:00

Автор: IVANOVA
 Организация: OFFICE
 Редакция: 3
 Общее время правки (в минутах): 63
 Авторы последних 10 изменений:

Таблица 7.

| Автор | Путь |
|---------|--|
| IVANOVA | C:\Documents and Settings\IVANOVA\Application Data\Microsoft\Word\Автокопия Документ1.asd |
| IVANOVA | C:\Documents and Settings\IVANOVA\Мои документы\письма\Письмо Петрову.doc |
| IVANOVA | C:\Documents and Settings\IVANOVA\Application Data\Microsoft\Word\Автокопия Письмо Петрову.asd |
| IVANOVA | C:\Documents and Settings\IVANOVA\Мои документы\письма\Письмо Петрову.doc |
| IVANOVA | C:\Documents and Settings\IVANOVA\Мои документы\письма\Письмо Петрову.doc |

ВЫВОДЫ:

1-4. На НЖМД системного блока, представленного на экспертизу, обнаружен удаленный файл Dc5835.doc, содержание которого аутентично копии письма, представленного на экспертизу. Файл описан в таблице 5 заключения эксперта и распечатан на с. 12. На основе анализа метаданных данного файла установлено, что он был создан 02.09.2004 11:37:00 пользователем IVANOVA, организация OFFICE (по сведениям, содержащимся в файле Dc5835.doc); изменен (дата последнего сохранения): 13.09.2005 18:21:00; напечатан (последний раз): 01.10.2004 13:45:00. Пользователем системного блока, представленного на экспертизу, согласно данным, имеющимся в файловой системе исследованного НЖМД, является VETROVA.

Копии данного файла могут находиться на НЖМД системного блока

| Автор | Путь |
|------------------------------|--|
| Автокопия Документ1.asd | C:\Documents and Settings\IVANOVA\Application Data\Microsoft\Word\ |
| Письмо Петрову.doc | C:\Documents and Settings\IVANOVA\Мои документы\письма\ |
| Автокопия Письмо Петрову.asd | C:\Documents and Settings\IVANOVA\Application Data\Microsoft\Word\ |

пользователя IVANOVA по следующим координатам:

На основе анализа данных, находящихся в \$MFT НЖМД, представленного на экспертизу, установлено, что удаленный файл Dc5835.doc имел имя файла в файловой системе «Письмо Петрову.doc». Определить время удаления файла Dc5835.doc не представляется возможным по причинам, указанным в исследовательской части заключения.

На представленном НЖМД обнаружен удаленный файл Dc5780.tmp, который, вероятно, является временной копией файла Dc5835.doc. Файл описан в таблице 5 заключения эксперта и распечатан на с. 13.

В свободной области НЖМД (в области, не относящейся к конкретному файлу файловой системы) системного блока, представленного на экспертизу, в секторах 30761049594-30761051724 и 30762325498-30762327628 обнаружена информация, аутентичная содержанию копии представленного письма. Обнаруженная информация распечатана на с. 10, 11.

Постановка вопросов перед экспертом предельно корректна. Следователь избегает скрытых утверждений и не требует от эксперта установления нетехнических фактов, например, кем было написано письмо. В то же время следователь не ограничивается вопросом о наличии информации на диске. Он также интересуется обстоятельствами ее появления и расположения. Как уже отмечалось ранее, само по себе наличие информации на НЖМД еще ни о чем не свидетельствует — информация могла попасть на диск несколькими различными путями, в том числе без ведома и желания последнего владельца исследуемого компьютера.

Следует отметить грамотное применение экспертом специальных технических средств — стендовой ЭВМ со специальной экспертной ОС, блокиратора записи на исследуемый диск, экспертной программы «EnCase».

Из недостатков этого заключения автор может указать разве что некоторый избыток технических деталей и употребление непонятных для судьи терминов типа «таблица MFT» или «USB-шина», без которых можно было бы обойтись. Обилие технической терминологии может запутать неспециалиста и вызвать претензии защиты по поводу языка, на котором составлен документ, или по поводу разъяснения сути обвинений.