

**Николай Николаевич
ФЕДОТОВ**

**Форензика –
компьютерная
криминалистика**



**Издательство
«Юридический Мир»**

Москва
2007

Оглавление

Федотов Н.Н. **Форензика — компьютерная криминалистика** —
М.: Юридический Мир, 2007. — 432 с.

Форензика — прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании доказательств в виде компьютерной информации, методах поиска, получения и закрепления таких доказательств. Форензика является подразделом криминалистики.

Книга рассказывает о методах раскрытия и расследования компьютерных преступлений, правилах сбора, закрепления и представления доказательств по ним применительно к российскому законодательству. В книге имеются также сведения, относящиеся к гражданским делам, в которых затрагиваются информационные технологии, — таким как дела об авторских правах на программы для ЭВМ и иные произведения в электронной форме, дела о доменных именах, дела об использовании товарных знаков и других средств индивидуализации в Интернете.

Кто должен прочитать эту книгу:

- оперативные сотрудники правоохранительных органов;
- следователи;
- эксперты;
- судьи;
- государственные обвинители;
- адвокаты;
- студенты юридических специальностей;
- работники служб информационной безопасности;
- правозащитники.

Каждый из упомянутых категорий, прочитав книгу, сможет приобрести или усовершенствовать свои знания, касающиеся киберпреступлений.

В книге сделан упор на практику: описывается, как практически реализовать то или иное мероприятие, приведены примеры работы с цифровыми доказательствами из реальных уголовных и гражданских дел.

Введение	11
<i>Название</i>	<i>11</i>
<i>Другие разделы</i>	<i>11</i>
<i>Ценз</i>	<i>12</i>
Предмет	12
<i>Целостность</i>	<i>13</i>
<i>Форензика и прогресс</i>	<i>14</i>
Задачи	15
Общенаучные методы	16
Специальные методы	19
Формы	19
Привлечение специалистов	21
<i>Хакеры на службе?</i>	<i>22</i>
Вовлечение общественности	23
<i>Общественные связи (пиар)</i>	<i>23</i>
<i>Потерпевший</i>	<i>24</i>
Роль экспертно-криминалистических подразделений	25
Современное состояние	26
Специальные технические средства	28
<i>Аппаратные средства</i>	<i>30</i>
<i>Экспертные программы</i>	<i>30</i>
<i>Наборы хэшей</i>	<i>31</i>
<i>Архивирование</i>	<i>32</i>
<i>Значение спецсредств</i>	<i>32</i>
<i>Криминалистические информационные системы</i>	<i>33</i>
Этапы	34
Контрфорензика	35
Заключение	36
 1. Компьютерные преступления	37
<i>Что такое «компьютерное преступление»?</i>	<i>37</i>
<i>Избыточная криминализация</i>	<i>38</i>
Криминалистическая характеристика	39
<i>Статистика</i>	<i>40</i>
<i>Личность вероятного преступника</i>	<i>41</i>
<i>Оперативность</i>	<i>47</i>

<i>Приоритетность расследования</i>	49
Онлайн-мошенничество	50
<i>Способ</i>	50
<i>Обстановка</i>	52
<i>Преступник</i>	53
<i>Потерпевший</i>	53
<i>Следы</i>	53
Клевета, оскорбления и экстремистские действия в Сети	54
<i>Способ</i>	54
<i>Преступник</i>	57
<i>Обстановка</i>	58
<i>Следы</i>	59
DoS-атаки	59
<i>Способ</i>	59
<i>Преступник</i>	60
<i>Обстановка</i>	61
<i>Потерпевший</i>	62
<i>Следы</i>	64
Дефейс.....	65
<i>Способ</i>	65
<i>Преступник</i>	67
<i>Следы</i>	67
<i>Потерпевший</i>	68
Вредоносные программы	68
<i>Способ</i>	68
<i>Преступник</i>	69
<i>Звонилки (dialers)</i>	72
<i>Следы</i>	73
Кардерство	74
<i>Способы</i>	74
<i>Получение</i>	75
<i>Реализация</i>	76
<i>Скиминг</i>	77
<i>Использование интернет-казино</i>	80
<i>Фиктивные покупки</i>	80
<i>Реальный пластик</i>	83
<i>Белый пластик</i>	84
<i>Посреднические онлайн-сервисы</i>	85
<i>Почему мошенничество?</i>	86

Мошенничество с трафиком	87
Нарушение авторских прав в офлайне	88
<i>Способ</i>	88
<i>Преступник</i>	89
<i>Потерпевший</i>	89
<i>Следы</i>	90
<i>Политизированность</i>	91
Нарушение авторских прав в Сети	92
<i>Способ</i>	92
<i>Преступник</i>	92
<i>Потерпевший</i>	93
<i>Следы</i>	94
Фишинг.....	94
<i>Способ</i>	94
<i>Преступник</i>	101
<i>Потерпевший</i>	101
Киберсквоттинг	102
<i>Определение</i>	102
<i>Правовая оценка</i>	103
Другое	105
<i>Платежи через Интернет</i>	105
<i>Терроризм и кибервойна</i>	108
<i>Мошенничество в онлайн-играх</i>	109
<i>Использование RBL</i>	111
<i>Накрутка</i>	115
Заключение к разделу 1	118

2. Оперативно-розыскные мероприятия119

Взаимодействие	119
Перехват и исследование трафика.....	121
<i>Значение</i>	121
<i>Пример</i>	121
<i>Организация перехвата</i>	125
<i>Шифрованный трафик</i>	127
Исследование статистики трафика	131
<i>Netflow</i>	131
<i>Пример</i>	131
Другие данные о трафике	136
<i>Анализ заголовков пакетов</i>	137

Избирательный перехват	138
Исследование логов веб-сервера	139
Значение логов.....	139
Содержание	141
Можно ли доверять логам?.....	142
Исследование системных логов.....	142
Системные логи Windows	143
Системные логи UNIX и Linux	144
Системные логи IOS.....	144
Исследование логов мейл-сервера и заголовков электронной почты.....	145
Как устроено	145
Следы	146
Примеры	147
Можно ли доверять заголовкам?	154
Формат сообщений	155
Документирование прохождения сообщений	155
Деревенский вариант	155
Провинциальный вариант.....	156
Столичный вариант	156
Анонимные ремейлеры	156
Установление принадлежности и расположения IP-адреса	158
Уникальность	158
Регистраторы.....	159
Установление принадлежности IP-адреса через whois-клиент.....	160
Установление принадлежности IP-адреса через веб-форму.....	162
Корректность.....	162
Трассировка IP-адреса	162
Неуловимый IP	167
Пространство и время	168
Документирование	169
Физическое расположение	169
Пример	170
Прочее.....	171
Установление принадлежности доменного имени.....	172
Изучение ответа	175
Достоверность данных регистратора	177
Анонимизация владельцев	177
Документирование	178
Принадлежность адреса электронной почты	180

Почтовый ящик	180
Передача сообщений	180
Достоверность	186
Установление	186
Примеры	187
Кейлогеры	191
Аппаратные кейлогеры	191
Программные кейлогеры	192
Интернет-поиск как метод ОРД	192
Заключение к разделу 2	195

3. Следственные действия.....196

Осмотр компьютера	196
Особенности	196
Стандарты.....	197
Лог-файлы, доказательная сила логов.....	198
Определение	198
Примеры	198
Лог как доказательство	202
Цепочка доказательности	203
Корректность генерирующей программы	203
Примеры	204
Неизменность при передаче	205
Корректность логирующей программы.....	206
Неизменность при хранении логов	206
Корректность изъятия.....	206
Неизменность после изъятия	208
Корректность интерпретации.....	208
Процедура приобщения логов	209
Деревенский вариант	209
Провинциальный вариант.....	209
Столичный вариант	210
Снятие копии диска	211
Стерильность.....	212
Тактика обыска.....	212
Принципы	213
Общие правила изъятия компьютерной техники при обыске.....	213
Особенности	215
Ноутбук (лэптоп, переносной компьютер)	216

<i>Наладочный компьютер (КПК)</i>	216
<i>Принтеры</i>	217
<i>Сканеры</i>	218
<i>Флэш-накопители</i>	218
<i>Мобильные телефоны</i>	220
<i>Коммутаторы и маршрутизаторы</i>	220
<i>Автомобильные компьютеры</i>	221
<i>Модемы</i>	221
<i>Цифровые фотоаппараты</i>	222
<i>Сменные накопители</i>	222
Короткоживущие данные.....	223
<i>Перечень</i>	223
<i>Снятие</i>	225
<i>Как выключать?</i>	227
Работа с потерпевшими	229
Заключение к разделу 3	230

4. Заверение контента231

Размещение на веб-сайте	232
<i>Практика</i>	232
<i>Просмотр</i>	233
<i>Динамические веб-страницы</i>	233
<i>Особенности браузера</i>	234
<i>Адресация</i>	235
Размещение в телеконференции (newsgroup)	237
Размещение в файлообменных сетях	240
<i>Доказательство наличия контента</i>	243
<i>Выявление источника</i>	244
<i>Доказательство использования</i>	244
<i>Виды преступлений</i>	245
Контент и доменное имя	246
<i>Правовая защита домена</i>	246
<i>Путаница сайта и ДИ</i>	246
<i>Примеры</i>	247
Заключение к разделу 4	249

5. Компьютерно-техническая экспертиза250

Место и роль КТЭ	250
<i>Общее</i>	250

<i>Кто может быть экспертом?</i>	251
<i>Проблемы с пониманием</i>	253
Приемлемые вопросы	254
<i>Поиск информации</i>	255
<i>Следы</i>	256
<i>Программы</i>	256
<i>Время</i>	257
<i>Пользователь</i>	257
<i>Итоги</i>	258
Неприемлемые вопросы.....	258
<i>Контрафактность</i>	258
<i>Стоимость</i>	259
<i>Правомерность доступа</i>	260
<i>Оценка содержания</i>	261
<i>Резюме</i>	262
Объекты исследования.....	263
<i>Оригинал или копия?</i>	263
Методы КТЭ	264
<i>Исследование файловых систем</i>	264
<i>Копирование носителей</i>	267
<i>Хэш-функции для удостоверения тождественности</i>	269
<i>Исследование файлов</i>	271
Другие типы носителей	272
<i>Флэш-накопители</i>	272
Зашифрованные данные	274
<i>Использование слабой криптографии</i>	274
<i>Использование коротких ключей и паролей</i>	274
<i>Использование словарных паролей</i>	275
<i>Неаккуратное обращение с открытым текстом</i>	275
<i>Неаккуратное обращение с паролем</i>	276
<i>Нешифрованные имена файлов</i>	276
<i>Ректотермальный криптоанализ</i>	277
<i>Доступ к содержимому ОЗУ</i>	277
<i>Использование кейлогера</i>	277
<i>Шифрование разделов и носителей</i>	278
<i>Стеганография</i>	278
Средства и инструменты	279
<i>Экспертные инструменты и авторское право</i>	279
Поиск информации на диске.....	280

Информация о файлах.....	280
Подключение образа диска	282
Изучение архивов электронной почты и ICQ.....	282
Реконструкция просмотра веб-страниц	283
Оценка найденного	284
Исследование программ.....	286
Изучение печатных документов	287
Стоимость ПО.....	287
Разбор образцов	290
Отрицательный пример	290
Промежуточный пример.....	307
Положительный пример	311
6. Участие специалиста в судебном заседании	321
7. Тенденции и перспективы	323
Тенденции.....	323
Понимание и просвещение.....	324
Широкополосный доступ	325
Интеллектуальная собственность.....	326
Конвергенция.....	327
Перспективы.....	328
Законодательство	328
Криминалистическая техника	328
Служба	328
Новые отношения	329
Неолиберализм и неоконсерватизм	330
Возрастание роли Интернета	331
Литература.....	332
Офлайновые публикации.....	332
Интернет-публикации	336
Нормативные акты	339
Официоз или сленг? Словарь официальных и жаргонных технических терминов.....	340

Введение

Название

Термин «форэнзика» произошел от латинского «foren», что значит «речь перед форумом», то есть выступление перед судом, судебные дебаты — это был один из любимых жанров в Древнем Риме, известный, в частности, по работам Цицерона. В русский язык это слово пришло из английского. Термин «forensics» является сокращенной формой «forensic science», дословно «судебная наука», то есть наука об исследовании доказательств — именно то, что в русском именуется криминалистикой. Соответственно, раздел криминалистики, изучающий компьютерные доказательства, называется по-английски «computer forensics». При заимствовании слово сузило свое значение. Русское «форензика» означает не всякую криминалистику, а именно компьютерную.

Другие разделы

Традиционные разделы криминалистики — дактилоскопия, баллистика, токсикология — развиваются уже более ста лет. В них не только накоплен большой опыт и отточены методики исследования. Некоторые особенности криминалистических технологий отражены в законодательстве. Например, законодательством прямо предусматривается взятие отпечатков пальцев и отстрел оружия в определенных случаях. Компьютерная криминалистика только что родилась. Опыт и инструментарий ее пока невелик. А требования законодательства совсем не заточены под особенности применяемых технологий, и даже иногда препятствуют их использованию.

Форензика оказалась почти не связанной с другими разделами криминалистики. Разве что прослеживается некоторая связь с технико-криминалистическим исследованием документов — компьютеры и компьютерная периферия широко применяются для подделки традиционных, бумажных документов.

Внутри форензики уже наметился один обособленный раздел — исследование программ для ЭВМ. Изучение устройства программ по исполняемому коду, методы создания вредоносных программ и противодействия им — это требует своих методов, существенно отличающихся от прочих методов форензики, применяемых для поиска, сбора и исследования цифровых доказательств. Хорошие специалисты по вредоносным программам, как правило, имеют узкую специализацию и не занимаются ничем иным — ни восстановлением скрытой информации, ни фиксации короткоживущих данных, ни трассировкой источника DoS-атаки. И нап-

ротив, эксперт, специализирующийся на исследовании информационного содержимого компьютеров, вряд ли возьмется за исследование неизвестного компьютерного вируса.

Некоторые авторы разделяют компьютерную криминалистику (computer forensics) и сетевую криминалистику (network forensics). Применяемые методы в том и в другом случае действительно отличаются.

Ценз

Для полного понимания данной книги необходимо владеть компьютером на уровне продвинутого пользователя и иметь базисные представления о современных коммуникационных технологиях и Интернете.

Автор весьма опечален, что пришлось ограничить таким образом круг читателей, но, к большому сожалению, по-другому поступить невозможно. Понимание материала настоятельно требует специальных познаний.

Если вдаваться в подробные объяснения о том, что такое файловая система, как работает протокол TCP или почему мощность процессора не влияет на скорость интернет-соединения, то вместо работы по криминалистике получится пятисотстраничный самоучитель по работе на компьютере, в котором всего несколько страниц — по делу. Именно такая история происходит с большинством книг, изданных в Европе и США [1-6, 74], которым подошло бы название «Компьютерная криминалистика для чайников». Также практикуется чисто популяризаторский подход, при котором материал излагается поверхностно, хотя и занимательно; специальных знаний не требует, но и не дает [39].

Если в подробные объяснения не вдаваться, а просто привести определения всех используемых терминов, как это любят делать отечественные авторы, то подготовленный читатель будет на этих страницах скучать, а неподготовленный все равно ничего не поймет. Определения — не объяснения. Подобный метод изложения незнакомого материала напоминает книгу на иностранном языке, к которой приложен словарь этого языка; одним читателям он не нужен, другим не поможет.

Поэтому не остается ничего иного, как рассчитывать на определенный уровень компьютерной грамотности читателя.

А имеющийся в конце книги словарь компьютерных терминов преследует совсем иную цель — отделить устоявшиеся термины от жаргонных и указать, какие из многочисленных вариантов следует использовать в официальных документах.

Предмет

Форензика (компьютерная криминалистика) является прикладной наукой о раскрытии и расследовании преступлений, связанных с компь-

ютерной информацией, о методах получения и исследования доказательств, имеющих форму компьютерной информации (так называемых цифровых доказательств), о применяемых для этого технических средствах.

Предметами форензики являются:

- криминальная практика — способы, инструменты совершения соответствующих преступлений, их последствия, оставляемые следы, личность преступника;
- оперативная, следственная и судебная практика по компьютерным преступлениям;
- методы экспертного исследования компьютерной информации и, в частности, программ для ЭВМ;
- достижения отраслей связи и информационных технологий (ИТ), их влияние на общество, а также возможности их использования как для совершения преступлений, так и для их предотвращения и раскрытия.

Целостность

Несколько слов об особенностях изучаемых следов. Почти все следы, с которыми приходится работать специалисту по форензике, имеют вид компьютерной информации, регулярной или побочной. Их достаточно легко уничтожить — как умышленно, так и случайно. Часто их легко подделать, ибо «поддельный» байт ничем не отличается от «подлинного». Фальсификация электронных (цифровых) доказательств выявляется либо по смысловому содержанию информации, либо по оставленным в иных местах следам, тоже информационным. Цифровые доказательства нельзя воспринять непосредственно органами чувств человека, но только через посредство сложных аппаратно-программных средств. Поэтому эти следы сложно продемонстрировать другим лицам — понятым, прокурору, судье. Не всегда просто обеспечить неизменность следов при их хранении. И не только обеспечить, но и доказать суду эту неизменность.

Вообще, понятие «неизменность» лишь с натяжкой применима к компьютерной информации. На некоторых видах носителей она хранится действительно статически — в виде разной намагниченности участков носителя или вариаций его оптических свойств. Но в других случаях метод хранения информации таков, что предусматривает постоянную смену носителя. Или предусматривает случайные величины.

Оперативная память компьютера (типа DRAM) регенерируется раз в несколько миллисекунд. То есть записанные там сигналы фактически стираются и записываются вновь. При передаче по многим каналам связи используется помехоустойчивое кодирование в расчете на возникающие при передаче ошибки; эти ошибки неизбежно возникают, но исправляются на принимающей стороне линии за счет избыточности кода. В

центральном процессоре тоже постоянно происходят ошибки при совершении арифметическо-логических операций, но если их не слишком много, они исправляются благодаря внутренней диагностике. В сетевых протоколах, которые мы считаем «надежными», таких как ТСР, эта надежность достигнута именно за счет того, что пропавшие в пути датаграммы или иные блоки информации перепосылаются, пока не будет подтвержден их верный прием. Запись на компакт-диск ведется с использованием кода Рида-Соломона с коррекцией массовых ошибок. То есть технология заведомо рассчитана на возникновение ошибок на этапе считывания. И такие ошибки всегда возникают. Но исправляются благодаря избыточности кода. Одним словом, «неизменной» компьютерную информацию может вообразить лишь пользователь, который не знает подробностей внутреннего устройства компьютерной техники и программного обеспечения.

Специалисты говорят про «неизменность» только с такими пользователями. Между собой они используют понятие «целостность», подразумевая, что информация может в процессе хранения и передачи сколько угодно раз изменяться, перекодироваться или сменять носители. Требуется лишь, чтобы первоначальная информация совпадала с конечной с точностью до одного бита — это и есть целостность.

Форензика и прогресс

Теперь — о технических достижениях. Влияние передовых достижений техники и технологии на преступность возможно тремя путями.

Во-первых, неостановимый технический прогресс дает возможность совершать преступления новыми способами и при помощи новых орудий. Естественно, в той же мере прогресс способствует появлению новых способов раскрытия преступлений — как старых, так и новых. Например, то же старое мошенничество в наш век совершается при помощи сети Интернет. Но суть и предмет посягательства у мошенничества прежние. Новыми являются лишь орудия совершения — веб-сайт, электронная почта, платежная система.

Во-вторых, достижения информационных технологий порождают принципиально новые общественные отношения, каковы отношения и становятся предметом преступных посягательств. При этом способ посягательства и орудия могут быть как старыми, так и новыми, с учетом достижений ИТ. Самый яркий пример — доменные имена. Такого общественного отношения, как право распоряжаться доменным именем, до недавних пор просто не существовало. Не было и посягательств. Ныне доменные имена охраняются законом (они причислены к объектам интеллектуальной собственности). И существует целый класс правонарушений, связанных с доменами, — киберсквоттинг*.

В-третьих, развитие ИТ может привести к появлению не просто новых общественных отношений, но нового субъекта таких отношений. Появление полноценного искусственного интеллекта уже явно просматривается на научном горизонте. А пока можно говорить о первых шагах в этом направлении. Программа для ЭВМ еще не рассматривается в качестве субъекта права, но в качестве стихийной силы уже иногда рассматривается. Программам уже дано принимать решения, которые могут существенно влиять на благосостояние и даже жизнь людей. Программы уже могут порождать новые объекты авторского права. Словом, появление принципиально нового субъекта, нового члена общества со своими правами — искусственного интеллекта — не за горами. А его появление вызовет новые правоотношения и, соответственно, новые преступления.

Задачи и приложения

Форензика решает следующие задачи:

- разработка тактики оперативно-розыскных мероприятий (ОРМ) и следственных действий, связанных с компьютерной информацией;
- создание методов, аппаратных и программных инструментов для сбора и исследования доказательств компьютерных преступлений;
- установление криминалистических характеристик правонарушений, связанных с компьютерной информацией.

Сферы применения форензики суть следующие.

1. Раскрытие и расследование уголовных преступлений, в которых фигурируют компьютерная информация как объект посягательства, компьютер как орудие совершения преступления, а также какие-либо цифровые доказательства.
2. Сбор и исследование доказательств для гражданских дел, когда такие доказательства имеют вид компьютерной информации. Особенно это актуально по делам о нарушении прав интеллектуальной собственности, когда объект этих прав представлен в виде компьютерной информации — программа для ЭВМ, иное произведение в цифровой форме, товарный знак в сети Интернет, доменное имя и т.п.
3. Страховые расследования, проводимые страховыми компаниями касательно возможных нарушений условий договора, страхового мошенничества, особенно когда объект страхования представлен в виде компьютерной информации или таким объектом является информационная система.
4. Внутрикорпоративные расследования инцидентов безопасности, касающихся информационных систем, а также работы по предотвращению утечки информации, содержащей коммерческую тайну и иные конфиденциальные данные.

5. Военные и разведывательные задачи по поиску, уничтожению и восстановлению компьютерной информации в ходе оказания воздействия на информационные системы противника и защиты своих систем.
6. Задачи по защите гражданами своей личной информации в электронном виде, самозащиты своих прав, когда это связано с электронными документами и информационными системами [5, W16].

Во многих из этих приложений некоторые методы форензики очень тесно интегрированы с методами технической защиты информации. Эти методы даже кое-где пересекаются. Несмотря на это, форензика никак не может быть приравнена к защите информации, поскольку цели у этих дисциплин разные.

Общенаучные методы

Все научные методы (наблюдение, измерение, описание, сравнение, эксперимент, моделирование, объяснение, анализ, синтез, предсказание) применяются в компьютерной криминалистике без ограничений. Хотя имеют некоторые особенности.

Такой общенаучный метод, как наблюдение, применяется в форензике достаточно своеобразно. Дело в том, что основным объектом исследования является компьютерная информация, которая в принципе не может наблюдаться человеком непосредственно. И изменяться непосредственно также не может. Непосредственные органы чувств человека — зрение, слух, осязание — не в состоянии воспринимать компьютерную информацию. Но это еще не настоящее своеобразие. В мире много объектов, которые не могут восприниматься человеком непосредственно — глазами, ушами и пальцами. Это еще не повод объявлять соответствующую науку уникальной. Для наблюдения «ненаблюдаемых» величин есть большое количество инструментов и способов — микроскопы, вольтметры, интерферометры и так далее. При помощи таких инструментов-посредников человек может наблюдать и изучать то, что не наблюдается невооруженным глазом. Все дело в сложности, детерминированности и прозрачности принципов действия таких «технических посредников».

При изучении компьютерной информации количество и сложность таких посредников настолько велики, что количество это переходит в качество. Мы не всегда знаем всех посредников, стоящих между информацией на компьютерном носителе и нашими глазами. Мы с большим трудом можем представить, какие именно преобразования претерпела информация по пути от своей исходной формы до наших глаз.

Представим себе, что на месте преступления обнаружен след — отпечаток обуви. Он воспринимается органами чувств человека непосред-

ственно. Если для восприятия и требуются какие-то технические средства, то лишь самые простые (например, фонарик или очки), принцип действия которых ясен любому и легко представим. А чаще технических средств и вовсе не требуется. Следователь и понятые своими глазами видят отпечаток обуви, прекрасно понимают механизм его возникновения. Не испытывая сомнений, они фиксируют этот след в протоколе, а после готовы показать под присягой, что видели именно отпечаток обуви. И у судьи не появится сомнений, что они могли видеть не то, что было на самом деле.

Совсем по-другому с компьютерной информацией.

Представим, что на «месте происшествия», а именно на диске сервера, в лог-файле*¹ обнаружена запись. Органами чувств человека она не воспринимается. Чтобы увидеть эту запись, потребуется посредничество следующих технических средств:

- механизм жесткого диска (НЖМД*);
- контроллер НЖМД с внутренней микропрограммой (firmware);
- внешний АТА-контроллер;
- программное обеспечение BIOS;
- операционная система;
- файловая система (драйвер);
- программное обеспечение для просмотра содержимого файла (например, вьювер «less»);
- драйвер экрана;
- программный экранный шрифт;
- аппаратные средства ввода и вывода (клавиатура, монитор) со своими собственными микропрограммами.

Вот сколько посредников стоят между компьютерной информацией и глазами «очевидца»! Все они изготовлены разными производителями. Не для всех из них имеются единые технические стандарты. Не для всех доступны описания. И ни в одном из этих средств нельзя быть полностью уверенным — все знают об ошибках в программном обеспечении, о возможности вирусов, троянов* и программных закладок. Могут ли понятые уверенно утверждать, что именно они видели? Даже не рассматривая возможности намеренных закладок в программах... А если оператор, запуская вьювер, ошибся на одну букву в имени каталога или файла? А если «/var» — это не локальный диск, а подмонтированный сетевой? А если владелец аккаунта* сделал себе удобства ради такой, например, alias:

```
alias less='grep -v "Deny UDP"
```

¹ Звездочкой отмечены термины, которые имеются в прилагаемом словаре.

то что же мы увидим, думая, что просматриваем лог-файл командой «less /var/log/security.log»? Мы увидим вместо настоящего лог-файла картину, мягко выражаясь, сильно искаженную, а лучше сказать — вовсе неверную.

Итак, особенностью наблюдения в отношении компьютерной информации является то, что непосредственно наблюдаемое (то есть изображение на экране монитора) имеет отношение к объекту наблюдения (то есть компьютерной информации) не просто косвенное, а очень-очень-отдаленно-посредственно-седьмая-вода-на-киселе-косвенное отношение. По пути происходит не просто большое количество преобразований, но непредставимо большое, трудно контролируемое, зависящее от множества незнакомых людей и невоспроизводимых факторов количество преобразований.

Другие общенаучные методы — анализ и синтез — также имеют в обсуждаемой науке свои особенности.

Дело в том, что в других технических науках при изучении объектов мы имеем дело только с объективными физическими процессами. Здесь же мы сталкиваемся со свободной человеческой волей, которая «защита» в такой объект исследования, как программа для ЭВМ. Будучи объектом искусственного происхождения, программа несёт в себе волю программиста, отпечаток его личности, выполняет его замыслы, реализует его видение. То есть программа для ЭВМ — это уже не в полной мере объективная реальность. Хотя до полноценного субъекта — искусственного интеллекта — ей еще далеко.

Поясним утверждение на примере. Известно, что злоумышленник мог установить на свой компьютер программу типа «логическая бомба*» для уничтожения всей критичной информации при угрозе попадания компьютера в чужие руки. Она должна сработать при заданных условиях: при выполнении каких-то действий на компьютере или, наоборот, — при невыполнении каких-то действий. Оставим сейчас за скобками стандартный метод (отключение компьютера, изъятие из него носителя информации и изучение его копии, что делает невозможным активацию программы-бомбы) и зададимся вопросом: как можно определить условия срабатывания такой программы для ее нейтрализации? Подумав немного, приходим к выводу, что ключ к пониманию алгоритма действия и условий срабатывания сей неизвестной программы следует искать исключительно в голове ее автора. Только поняв его образ мыслей и шаблоны поведения, можно догадаться, как поведет себя его программа. Формально программа — детерминированный объект. Но фактически изучать ее надо через изучение субъекта, обладающего свободой воли. То есть программа как бы обладает свободой воли, во всяком случае, такое допущение откроет нам путь к ее познанию.

Но разве не возникает та же ситуация с иными техническими устройствами, включая механические? Разве на их работу не наложила отпечаток личность создателя? Автор берётся утверждать, что вышеописанная особенность характерна лишь для устройств, реализующих довольно сложный алгоритм. Алгоритм — это как раз тот объект, в котором и может содержаться частичка «воли». Кроме компьютерных программ, какие устройства реализуют алгоритмы? Причем алгоритмы не примитивные, а достаточно сложные, многовариантные. Теоретически такие устройства могут существовать, но в своей жизни автор их не встречал. Поэтому он берётся утверждать, что только компьютерные программы обладают описанным свойством, то есть могут рассматриваться как обладающие условной свободой воли.

Специальные методы

Наряду с общенаучными форензика применяет и специальные методы исследования, свойственные только ей. Назовем некоторые из этих методов.

- Создание и применение специализированных криминалистических информационных систем; перенастройка и использование в своих целях систем двойного назначения.
- Использование в целях обнаружения или исследования доказательств публичных поисковых систем (таких как «Google»), а также поисковых систем специального назначения (типа «Эшелон»).
- Создание виртуальной личности для целей проведения с ее помощью ОРМ и агентурной работы.
- Сбор хэш-функций известных файлов для отделения их от файлов, содержащих оригинальную пользовательскую или модифицированную информацию.
- Архивирование полного содержимого носителей для целей последующего расследования возможных инцидентов.
- Эмулирование сетевых сервисов для исследования поведения подозрительных программ в лабораторных условиях.

Формы

Общенаучные и специальные методы компьютерной криминалистики должны использоваться в борьбе с преступностью в следующих формах.

1. Производство компьютерно-технических экспертиз. Кроме этих, «родных» для себя экспертиз, ИТ-специалисты должны принимать участие в некоторых других видах экспертиз. Например, товароведческая

(экономическая) экспертиза по определению стоимости прав на использование экземпляра ПО. Такая экспертиза совершенно необходима для доказывания нарушения авторских прав (ч.ч. 2 и 3 ст. 146 УК), где квалифицирующим признаком является стоимость контрафактных экземпляров или прав на использование произведения. Понятно, что обычный экономист не знаком с особенностями ценообразования на программные продукты, с существующей практикой в этой области. Поэтому ему надо дать в помощь эксперта по ИТ.

2. Участие специалистов в проведении следственных действий, имеющих отношение к компьютерной информации, — обыска, выемки, осмотра места происшествия и т.д. Например, такая элементарная задача, как выключение компьютера, который подлежит изъятию. Нет однозначного способа выключения. Чтобы правильно его выключить, нужно проанализировать обстоятельства дела, взвесить вероятности разных событий и, только исходя из этого, избрать способ выключения. А некоторые типы компьютерной техники вообще выключать нельзя.

3. Участие специалиста в проведении ОРМ. Наиболее востребованное в обсуждаемой области мероприятие — снятие информации с технических каналов связи — проводится не просто «при участии», а только самим специалистом.

4. Участие специалиста в судебном заседании. Эта форма, предусмотренная УПК, стала активно использоваться лишь при рассмотрении дел по компьютерным преступлениям. В таких делах специальные знания требуются очень часто. Без разъяснений специалиста иногда невозможно правильно понять не только заключение эксперта, но также показания свидетелей, имеющиеся в деле справки, вопросы участников процесса. Специалист в зале суда может действовать наподобие переводчика, разъясняя участникам процесса значения терминов, поясняя значение тех или иных технических деталей и так далее.

5. Снабжение оперативных работников и следователей техническими средствами, которые те могут использовать в работе самостоятельно, без участия специалиста.

6. Обучение пользователей и технических специалистов предприятий (то есть потенциальных потерпевших) методам первичной фиксации цифровых доказательств, их предохранения от уничтожения. Значительная часть компьютерных преступлений остается нераскрытой только из-за того, что оператор информационной системы, которая стала целью злоумышленника, не позаботился о сбережении логов*, электронных сообщений, использованных программ и иных потенциальных доказательств. Либо не знал, как их правильно сберечь, чтобы в дальнейшем такие доказательства имели силу, либо вообще не подозревал о существовании некоторых цифровых следов.

Привлечение специалистов

Специалист или эксперт должен привлекаться к расследованию или проведению ОРМ в тех случаях, когда требуются специальные знания («специальные познания» в терминологии предыдущей редакции УПК) в какой-либо области.

Несмотря на повсеместное распространение компьютерной техники, знания об этой технике не распространяются вслед за ней, столь же повсеместно.

Современная парадигма ИТ предусматривает отчуждение пользователя от управления работой ЭВМ. Развитие идет в направлении всё большего и большего абстрагирования пользовательского интерфейса от процессов в компьютере. Пользователь 1960-х и 1970-х годов мыслил байтами и логическими операциями. Пользователь 1980-х — символами и файлами. Пользователь 1990-х — окнами, «папками» и событиями. В текущем десятилетии типичный пользователь думает такими объектами, как «документ» и «рабочий стол». То есть для идеального пользователя никаких специальных знаний о внутренних процессах в вычислительной технике не требуется.

Криминалистическое же исследование предполагает как раз глубокое проникновение в суть процессов, происходящих в ЭВМ и компьютерных сетях. Чем глубже погружается исследователь в подробности функционирования, тем больше он обнаруживает следов действий пользователя.

К примеру, оценивая следы при просмотре пользователем веб-сайта, неспециалист (скажем, следователь) может заключить, что следы (доказательства) следует искать в двух местах — на персональном компьютере пользователя и на сервере, на котором расположен веб-сайт. И это будет ошибкой. Не обладая знаниями, глубже определенного, положенного для пользователя уровня, следователь упускает из виду обращение к DNS-резолверу пользователя, а также рекурсивные обращения этого резолвера к нескольким DNS-серверам. Такие обращения могут логироваться и служить полноценными (то есть не косвенными, не дополнительными, а вполне самостоятельными) доказательствами посещения определенной веб-страницы. Еще десяток видов следов при таком простом действии, как просмотр веб-страницы, перечислен в главе «Исследование логов веб-сервера» раздела 2.

Автор полагает, что при любых ОРМ или следственных действиях, связанных с компьютерной информацией, привлечение специалиста обязательно. Ибо специальные знания в сфере ИТ позволяют видеть неочевидное, находить бесследно пропавшее и обманывать безошибочное. И попутно еще опровергать все утверждения из «инструкции для пользователя», ибо обычный среднеквалифицированный пользователь работает

с компьютером на определенном, предназначенном для него уровне, а всё, что глубже, ему знать «не положено».

Хакеры на службе?

Отдельного разговора заслуживает тема привлечения киберпреступников для противодействия другим киберпреступникам — в качестве работников служб информационной безопасности или даже сотрудников правоохранительных органов.

Тот, кто совершает преступления, конечно же, хорошо представляет себе методы их совершения, лучше видит возможности, уязвимости, знает психологию киберпреступников, ориентируется на черном рынке соответствующих услуг. Этим он ценен для борьбы с преступностью, своими знаниями.

Но знания — дело наживное. Обучить соответствующей специальности можно почти любого человека, особенных способностей тут не требуется.

Кроме знаний киберпреступник отличается также специфическими наклонностями. В их число входит неприятие многих социальных институтов, пренебрежение интересами иных лиц и общества в целом. Иногда также патологическая склонность к антисоциальному поведению [W27]. Если знаниям можно обучить, то подобным наклонностям невозможно «разучить» человека. Именно поэтому нигде в мире на службу в правоохранительные органы не берут преступников, даже бывших (во всяком случае, автору такая практика не известна). Их используют в качестве агентов или консультантов, но не более.

Французская уголовная полиция «Сюртэ» считается самой первой в мире службой уголовного розыска. Ее основатель и первый руководитель, Эжен-Франсуа Видок был многократно судимым профессиональным вором. И первый штат, который он набрал, также целиком состоял из бывших профессиональных преступников [68]. Результаты работы подразделения Видока впечатляли. Такой статистикой раскрытых преступлений, как у него (811 раскрытых преступлений в год на 12 человек), не могла похвастаться ни одна спецслужба ни в XIX, ни в XX веке. Это, пожалуй, единственный удачный пример привлечения бывших уголовников на правоохранительную службу. Для всех последующих политических и государственных деятелей лояльность полиции была несравненно важнее ее эффективности. Впрочем, и эффективность службы бывших преступников также иногда ставится под сомнение.

Автор также в свое время отдал должное этой идее. Но результаты поиска возможностей привлечения хакеров к деятельности по защите информации оказались неудовлетворительными. Оказалось, что среди киберпреступников попросту нет достаточно квалифицированных кадров.

Зарплата рядового сисадмина в Москве в 1999 году была в разы выше, чем средний доход спамера*, вирусписателя или интернет-мошенника. (Правда, с кардерами* ситуация была иная, но для этой криминальной профессии особые технические навыки и не требуются.) Иными словами, много выгоднее быть законопослушным. С тех пор ситуация изменилась. Количество денег и иных материальных интересов в Интернете (в частности, в российском его сегменте) сильно возросло. Ныне ремесло киберпреступника уже в состоянии прокормить хорошего специалиста. Правда, и средние доходы честного онлайн-бизнесмена также выросли.

Тем не менее автор согласен с общепринятым мнением, что привлекать киберпреступников для борьбы с киберпреступностью допустимо лишь в качестве осведомителей, в крайнем случае — консультантов.

Вовлечение общественности

Да не смутит читателя этот заголовок, созвучный с пустыми пропагандистскими заклинаниями советских времен. Речь пойдет о совсем другом вовлечении другой общественности.

Для расследования компьютерных преступлений необходимо сотрудничество со стороны потерпевшего, а также со стороны свидетелей. Необходимо как-то узнать о самом факте совершения преступления. В ряде случаев необходимо получить официальное заявление от потерпевшего.

Свидетели и потерпевшие для компьютерных преступлений — это чаще всего пользователи ЭВМ и профессиональные ИТ-специалисты. Потерпевшим также часто являются предприятия, от лица которых принимают решения те же ИТ-специалисты. Но среди данной категории граждан не принято обращаться в правоохранительные органы по поводу инцидентов безопасности. И, напротив, при обращении органов к ним они не склонны сразу идти на сотрудничество, стараются уклониться от дачи показаний и не ожидают ничего хорошего от такого взаимодействия.

Статистика опросов говорит нам, что до 80% инцидентов безопасности попросту скрывается сотрудниками даже от своего начальства, не говоря уже о правоохранительных органах.

Общественные связи (пиар)

Полезность общественных связей для раскрытия, расследования, а также предупреждения преступлений уже никем не ставится под сомнение. В отношении компьютерных преступлений такое утверждение также справедливо. Особенность в том, что аудитория традиционных СМИ не вполне соответствует интересующей нас специфической группе — корпоративные ИТ-специалисты, ведущие бизнес в Интернете предпринима-

тели и простые пользователи персональных компьютеров. Для эффективного взаимодействия с этой аудиторией целесообразно использовать иные средства — сетевые СМИ, блоги, интернет-рекламу.

В газетах и телепередачах довольно часто рассказывается о совершенных и раскрытых преступлениях. Эти публикации вызывают интерес читателей и зрителей. Пользуясь таким интересом, правоохранные органы проводят собственные пиар-мероприятия. Но когда в специфических онлайн-СМИ публикуется сообщение о каком-либо компьютерном преступлении или интервью с представителем правоохранительных органов на тему киберпреступности, реакция аудитории бывает и негативной. Автор изучил десятки подобных публикаций с комментариями на них. Положительных и нейтральных отзывов — ничтожное количество. Большинство комментариев либо ругательные, либо ехидные, либо указывающие на некомпетентность источника в том или ином техническом вопросе. Совершенно очевидно, что пиар-стратегия для онлайн-СМИ в отношении компьютерных преступлений должна быть иной, не такой же, как для традиционных СМИ в отношении традиционных преступлений. Специфика аудитории (высокая квалификация в технических вопросах) и специфика способа коммуникации (моментальные комментарии) требуют особого подхода.

Потерпевший

Во многих случаях для расследования компьютерного преступления бывает очень полезно привлечь потерпевшего.

Классическая виктимология не склонна была рассматривать потерпевшего как опору следствия и источник существенной помощи (за исключением предоставления информации). Современная виктимология сменила точку зрения [62, 63]. Жертва преступления, оказывается, имеет хороший потенциал и мотивацию для активных действий. Следствию было бы неразумно не использовать эти возможности. В рамках закона, естественно. Ныне зарубежные криминологи рекомендуют привлекать потерпевшего к активным действиям по расследованию как данного, так и других аналогичных преступлений.

Сказанное выше касается традиционных, не компьютерных преступлений. А в нашем случае полезность потерпевшего может быть еще выше. Для неправомерного доступа к компьютерной информации, корпоративного мошенничества, кардерства и некоторых других высокотехнологичных видов преступлений потерпевшие (или работники предприятия-потерпевшего) имеют достаточно высокую квалификацию в области ИТ. Часто эта квалификация выше, чем у сотрудников правоохранительных органов, которые занимаются расследованием. Кроме квалификации есть и мотивация.

Автор неоднократно сталкивался с ситуацией, когда руководитель фирмы, пострадавшей от действий кардера*, ассигновал значительные средства, чтобы содействовать привлечению виновного к ответственности. Вовсе не потому, что надеялся получить с осужденного преступника компенсацию причиненного ущерба. Это далеко не главный мотив. Оправдаться перед клиентами, которые доверили свои персональные данные, перед акционерами, перед партнерами, компенсировать ущерб деловой репутации фирмы. Предотвратить возможные рецидивы или месть злоумышленника, который остался безнаказанным. Всё это заставляет потерпевшее предприятие предлагать свою помощь следствию — информацией, техникой, специалистами, разными услугами.

Физические лица, оказывавшиеся потерпевшими, также склонны содействовать обнаружению преступника. Автору неоднократно приходилось уговаривать пострадавших ИТ-специалистов отказаться от самостоятельного поиска и наказания преступника, чем они намеревались заняться, не веря в возможности правоохранительных органов или просто не вспоминая об их существовании. Бывали случаи, когда такой специалист не просто оказывал помощь милиции, а фактически преподносил им на блюде раскрытое преступление.

Роль экспертно-криминалистических подразделений

Как можно понять из главы «Привлечение специалистов», роль специалистов и экспертов при раскрытии и расследовании компьютерных преступлений является ключевой. Без их участия расследовать такое преступление невозможно вообще.

Особенность состоит в том, что экспертно-криминалистические подразделения правоохранительных органов таких специалистов не имеют. В текущих условиях минимальная зарплата ИТ специалиста «на гражданке» в разы превышает максимальную зарплату сотрудника экспертно-криминалистического подразделения в органах внутренних дел, юстиции или ФСБ. Старых же кадров, на которых держатся другие направления криминалистики, для форензики попросту не существует, поскольку обескураживающая отрасль знания сама по себе очень молода.

Номинальное существование подразделений компьютерно-технической экспертизы в некоторых ЭКУ может ввести кого-то в заблуждение, но только до первой встречи с этими номинальными «экспертами» или их трудами.

Выход состоит в привлечении к расследованию гражданских специалистов и экспертов из числа сотрудников операторов связи, программистов, инженеров по коммуникационному оборудованию, системных администраторов. Многие из них готовы сотрудничать с органами внутрен-

них дел совсем безвозмездно или за... скажем так, на иных взаимно приемлемых условиях.

Нечто вроде экспертно-криминалистических отделов существует в некоторых коммерческих организациях, которым часто приходится проводить расследования инцидентов безопасности или которые специализируются на проведении экспертиз по гражданским делам.

Штатным же ЭКО стоит поручать лишь простейшие, типовые виды компьютерных экспертиз, для которых есть готовые алгоритмы действий и образцы заключений.

Современное состояние

В развитых странах форензика как прикладная наука существует полноценно: издан ряд научных трудов, имеются кафедры и учебные курсы, практические работники при раскрытии компьютерных преступлений обязаны следовать официальным рекомендациям, написанным соответствующими специалистами [7].

В прочих (не относящихся к развитым) странах форензика находится пока в зачаточном состоянии. Россия принадлежит к числу таковых. В то же время качественные характеристики российских компьютерных специалистов находятся на передовом уровне, не уступая развитым странам. Особенности советской системы высшего образования, особенно ее исследовательский уклон в подготовке кадров, привели к тому, что российские специалисты отличаются от западных креативностью, способностью быстро осваивать новые знания, критичностью мышления — это как раз то, что требуется для успешного совершения компьютерных преступлений и их раскрытия.

Однако привлечение таких специалистов на службу в правоохранительные органы или на работу в научные криминалистические учреждения сильно затруднено. Во-первых, уже упоминавшаяся низкая оплата по сравнению с ИТ-компаниями. Во-вторых, в какой-то мере естественная инертность научных кругов и медленная смена поколений в научной и ведомственной иерархии. Все это не позволяет новым специалистам влиться в криминалистическую науку, а уже существующие работники не в состоянии переквалифицироваться.

Характерный пример. Некоторое время назад знакомый автора уволился из органов внутренних дел, где он служил оперуполномоченным в управлении «К» (ранее — УБПСВТ) одного из субъектов Федерации. Он давно уже жаловался на службу, при этом основная претензия состояла в том, что все сотрудники управления, кроме него, разбирались в компьютерной информации крайне слабо. В результате этот знакомый автора всю работу отдела исполнял сам и в награду выслушивал некомпетент-

ные упреки начальства. Впрочем, начальник, надо отдать ему должное, хотя и не понимал в компьютерах, хотя и поругивал, но не давал в обиду своих подчиненных более высокому начальству, прокуратуре и УСБ. Досидев наконец до пенсии, он ушел. Понятно, что рассчитывать на повышение единственному грамотному специалисту не стоило — не выслужил положенного срока. Прислали нового начальника. Это был старый и опытный кадр. Хорошо зарекомендовавший себя на предшествующей должности — командира конвойного батальона. Учитывая, что до пенсии ему оставалось еще долго, знакомый с сожалением покинул службу, после чего в этом «К» не осталось вообще ни одного сотрудника, знающего, что такое IP-адрес.

Изучение имеющихся трудов в данной области показало, что значимые книги по компьютерной криминалистике издавались только в США (см. список литературы). На русском языке вышло несколько мелких работ [8, 9, 10], при чтении которых автор постоянно испытывал экстремальные эмоции: над юридической их частью плакал, над технической — смеялся. Когда, например, атрибутом файла называют «расширение, то есть примечание, содержащее не более трех символов», это смешно. Но когда средство обхода технических средств защиты авторских прав (ст. 48.1 ЗоАП) объявляют вредоносной программой (ст. 273 УК) — это грустно, и автор сам в период работы над книгой видел на скамье подсудимых не один десяток людей, поплатившихся собственной судьбой за такую вольную трактовку законодательства отечественными «криминалистами».

Вернемся к современному состоянию форензики. Одним из показателей развития является серийный выпуск техники и программного обеспечения, специально предназначенных для сбора доказательств, для обеспечения целостности данных при изъятии и исследовании, для других подобных характерных задач. Номенклатура подобных средств в специализированных магазинах Европы включает около десятка типов, да еще несколько моделей каждого типа. В России такая техника не производится и даже не закупается.

Другим показателем можно считать наличие общественных или межведомственных ассоциаций, обществ, иных профессиональных объединений компьютерных криминалистов или судебных экспертов. Приведем в качестве примера ассоциацию «International Association of Computer Investigative Specialists» (IACIS). Это общественная организация, базирующаяся в США, состоящая из сотрудников правоохранительных органов и занимающаяся преимущественно обучением и просвещением в области форензики. Подобных общественных организаций существует несколько. В нашей стране нет ни одной, нет даже отделения зарубежной. Это говорит о том, что соответствующих специалистов у нас пока мало.

Специальные технические средства

Компьютерный криминалист вполне может обойтись без специальной криминалистической техники вообще. Компьютер сам по себе — достаточно универсальный инструмент. Среди многообразного периферийного оборудования и программного обеспечения найдутся все необходимые для исследования функции. Некоторые программные инструменты можно легко создать или модифицировать своими руками.

Однако специальная техника сильно облегчает работу. Впрочем, карманы она облегчает еще сильнее.

На сегодняшний день на рынке имеются следующие криминалистические инструменты:

- устройства для клонирования жестких дисков и других носителей (в том числе в полевых условиях);
- устройства для подключения исследуемых дисков с аппаратной блокировкой записи на них;
- программные инструменты для криминалистического исследования содержимого дисков и других носителей, а также их образов;
- переносные компьютеры с комплексом программных и аппаратных средств, ориентированных на исследование компьютерной информации в полевых условиях;
- наборы хэшей (hash sets) для фильтрации содержимого изучаемой файловой системы;
- аппаратные и программные средства для исследования мобильных телефонов и SIM-карт [W01, 60, 90];
- программные средства для исследования локальных сетей;
- и некоторые другие.

В целях криминалистического исследования можно эффективно применять не только специально для этого предназначенные средства, но также некоторые средства общего или двойного назначения [W02].

С другой стороны, аппаратные и программные инструменты, которые автор назвал криминалистическими, могут быть использованы не только для правоохранительных целей. У них есть и ряд «гражданских» применений:

- тестирование компьютеров и их сетей, поиск неисправностей и неверных настроек;
- мониторинг с целью обнаружения уязвимостей и инцидентов безопасности;
- восстановление данных, утраченных вследствие неисправностей, ошибок, иных незлоумышленных действий;
- копирование носителей с архивными целями или для быстрой установки/дубликации программного обеспечения;



Серийно выпускаемое криминалистическое компьютерное оборудование

- поиск скрытой или стертой информации для борьбы с утечкой конфиденциальных данных.

Аппаратные средства

Учитывая, что современные компьютеры являются универсальными устройствами, в которых используются в основном открытые стандарты и протоколы, специальных аппаратных средств для исследования самих компьютеров и компьютерных носителей информации не требуется. То есть универсальным инструментом является сам компьютер, а все его функции можно задействовать через соответствующие программные средства.

Немногочисленные аппаратные криминалистические устройства сводятся к дубликаторам дисков и блокираторам записи. Первые позволяют снять полную копию НЖМД* в полевых условиях, но это с тем же успехом можно сделать при помощи универсального компьютера. Вторые позволяют подключить исследуемый диск с аппаратной блокировкой записи на него. Но то же самое позволяет сделать программно любая операционная система (кроме Windows). То есть аппаратные криминалистические устройства для компьютеров и компьютерной периферии служат лишь удобству специалиста или эксперта.

Совсем другое дело — криминалистические устройства для иной техники, отличной от универсальных компьютеров. Мобильные телефоны, цифровые фотоаппараты и видеокамеры, бортовые компьютеры, коммутаторы, маршрутизаторы, аппаратные межсетевые экраны — все эти устройства не являются технологически открытыми и вовсе не стремятся к универсальности. Для полного доступа к компьютерной информации, хранящейся в них, не всегда бывает достаточно компьютера и программных инструментов.

Разнообразие таких устройств соответствует разнообразию выпускаемых электронных устройств, способных нести компьютерную информацию. У каждого производителя — свои проприетарные протоколы, свои интерфейсы. Приобретать такие устройства заранее вряд ли целесообразно. Исключение, пожалуй, составляют ридеры для SIM-карт мобильных телефонов и ридеры для стандартных банковских карт — эти криминалистические устройства всегда полезно иметь в своем арсенале.

Экспертные программы

Такие программы предназначены в основном для исследования содержимого компьютерных носителей информации (прежде всего НЖМД) во время проведения экспертизы.

Они работают не только на уровне файловой системы, но и ниже — на уровне контроллера НЖМД, что позволяет восстанавливать информацию после удаления файлов.

Перечислим несколько популярных экспертных программ:

- Семейство программ ProDiscover (подробнее <http://computer-forensics-lab.org/lib/?rid=22>)

- SMART (Storage Media Analysis Recovery Toolkit) (<http://computer-forensics-lab.org/lib/?cid=18>)
- Forensic Toolkit (FTK) фирмы «AccessData» (<http://computer-forensics-lab.org/lib/?rid=26>)
- Encase — экспертная система
- ILook Investigator (<http://www.ilook-forensics.org>)
- SATAN (System Administrator Tools for Analyzing Networks) — средство для снятия полной информации с компьютеров для ОС Unix
- DIBS Analyzer 2 (<http://www.dibsusa.com/products/dan2.html>)
- Helix — экспертный комплект на загрузочном компакт-диске на основе ОС Linux

Наборы хэшей

Так называемые «hash sets» — наборы хэшей — предназначены для облегчения исследования содержимого файловой системы больших носителей, в основном компьютерных жестких дисков.

Предположим, эксперту поступил для исследования изъятый при обыске у подозреваемого НЖМД, на котором установлена операционная система и имеются пользовательские данные. Эти данные могут быть разбросаны по различным директориям, могут содержаться внутри файлов с настройками, даже могут быть скрыты методами стеганографии внутри файлов, содержащих с виду совсем другие данные. Современные ОС включают в свой состав тысячи файлов, популярные приложения — тоже сотни и тысячи. Таким образом, в файловой системе обычного компьютера может находиться, например, 30 000 файлов, из которых только 500 — это файлы, созданные пользователем или измененные им. Чтобы отделить это «меньшинство» пользовательских файлов от заведомо не содержащего ничего интересного «большинства», предназначен набор хэшей.

Хэш, хэш-сумма или однонаправленная хэш-функция* файла представляет собой длинное число, вычисляемое из содержимого файла по особому алгоритму. Хэш-сумма похожа на контрольную сумму, но имеет одно существенное отличие: это однонаправленная функция [18]. То есть по файлу легко вычислить его хэш-функцию, но под заданную хэш-функцию подобрать соответствующий ей файл невозможно.

Хэши известных (то есть входящих в серийное ПО различных производителей) файлов позволяют, не рассматривая подробно содержание этих файлов, отбросить их и быть уверенным, что эти файлы не содержат пользовательской информации. После их исключения эксперту остается исследовать относительно небольшое число файлов. Этот тип наборов именуется «knowngoods».

Существуют и наборы хэшей, выполняющие обратную задачу. Они именуются «knownbads» и соответствуют не заведомо безобидным файлам, а наоборот, заведомо вредоносным, содержащим порнографию, вирусы или иной криминальный контент.

Обычно набор хэшей — это отдельный продукт, приобретаемый у ответственного производителя (включая подписку на обновления) и подключаемый к экспертному ПО. Он может содержать сотни тысяч и миллионы хэш-функций с соответствующими сведениями о файлах. Все популярные экспертные системы позволяют подключать и использовать «внешние» наборы хэшей.

Архивирование

Копирование и долговременное хранение копий данных сначала применялось лишь с целью восстановления в случае утраты — так называемое «страховочное копирование» или «холодное резервирование».

В последнее время архивирование применяется и с иными целями — для расследования инцидентов безопасности, могущих произойти или обнаружиться в будущем. То есть данные копируются не по принципу «наиболее ценные, наиболее чувствительные данные, утрата которых нанесет ущерб», а по совсем иному принципу: копируются данные и области носителей, где могут оставаться следы злоумышленных действий.

Например, в отношении служебного персонального компьютера для целей восстановления архивируются файлы пользователя и отдельные его настройки. Операционная система и прикладные программы страховочному копированию не подлежат, поскольку легко восстанавливаются из дистрибутива. Все резервное копирование производится на уровне файловой системы. А для целей расследования инцидентов копируется весь жесткий диск (НЖМД) компьютера, причем не на уровне файловой системы, а на уровне контроллера диска, то есть чтобы включалась удаленная и скрытая информация.

Страховочная копия малополезна для расследования инцидентов. Напротив, «инцидентная» копия не подходит для восстановления на случай вирусной атаки или аварии. Это разные копии — и технически, и по назначению. Средства для архивирования на случай расследования инцидентов — это специальные криминалистические средства. Они могут собирать и хранить не только копии НЖМД, но также копии сетевого трафика, копии электронной почты и некоторые другие виды данных.

Значение спецсредств

Следует отметить, что ни одно из криминалистических средств не обеспечивает правильности, корректности, неизменности собранных доказательств, отсутствия их искажений, случайных или намеренных.

Всё упомянутое обеспечивают специалисты или эксперты, применяющие эти средства. Распространенная ошибка при оценке доказательств состоит в том, что придается излишнее значение качествам криминалистической техники (включая ПО), но принижается значение специалистов.

На самом деле ненадлежащие или несовершенные технические устройства вряд ли смогут «испортить» собираемые или интерпретируемые с их помощью цифровые доказательства. В то время как малоквалифицированный специалист — это в любом случае повод усомниться в доказательной силе соответствующих логов, сообщений, иных доказательств в форме компьютерной информации, независимо от того, какими инструментами они были собраны или исследованы.

Бывает, что судья или защитник, желая подвергнуть сомнению доказательства, основанные на компьютерной информации, ставит вопрос о том, какими средствами эти доказательства были собраны, решены ли к применению эти средства, сертифицированы ли, не являются ли контрафактными и т.д. Подобная постановка вопроса представляется автору нерациональной. Практика не знает случаев, чтобы судебная ошибка произошла из-за ошибки в криминалистическом программном средстве. Чтобы подвергнуть сомнению цифровые доказательства или результаты компьютерно-технической экспертизы, нужно ставить не вопрос «чем?», а вопрос «кто?». Кто проводил исследование или изъятие компьютерной информации. В практике имеется немало примеров, когда малоквалифицированный специалист, используя «правильные», общепризнанные, должным образом сертифицированные средства, получал «результаты» не просто ошибочные, а не имеющие никакого отношения к исследуемому объекту. Обратных примеров, когда грамотный специалист ошибался из-за использования им «неправильных» криминалистических средств, практика не знает.

Криминалистические информационные системы

Указанные системы не используются напрямую для поиска и изучения доказательств. Они выполняют обеспечивающие функции в работе по раскрытию и расследованию преступлений. Но традиционно относятся к криминалистической технике. Криминалистические информационные системы выполняют ряд близких задач. А именно:

- облегчают и/или ускоряют оформление различных документов для ОРМ, предварительного следствия, судебных целей;
- позволяют работникам правоохранительных органов быстрее найти необходимые нормативные акты, комментарии, прецеденты, получить консультации;

- облегчают и ускоряют доступ сотрудников ко всевозможным базам данных, учетам, справочникам — как публичным, так и закрытым;
- ускоряют и автоматизируют проведение ОРМ, связанных с перехватом сообщений.

Иногда к криминалистической технике причисляют также средства связи и навигации, используемые в работе правоохранительных органов.

Полезно упомянуть следующие информационные системы:

- Глобальная информационно-телекоммуникационная система (ГИТКС) НЦБ Интерпола;
- Единая информационно-телекоммуникационная система органов внутренних дел (ЕИТКС ОВД).

Этапы

Криминалистический процесс, который проводят специалисты и эксперты, принято [11] делить на четыре этапа:

- 1) сбор;
- 2) исследование;
- 3) анализ;
- 4) представление.

На первом этапе происходит сбор как информации самой по себе, так и носителей компьютерной информации. Сбор должен сопровождаться атрибутированием (пометкой), указанием источников и происхождения данных и объектов. В процессе сбора должны обеспечиваться сохранность и целостность (неизменность) информации, а в некоторых случаях также ее конфиденциальность. При сборе иногда приходится предпринимать специальные меры для фиксации недолговечной (волатильной) информации, например, текущих сетевых соединений или содержимого оперативной памяти компьютера.

На втором этапе производится экспертное исследование собранной информации (объектов-носителей). Оно включает извлечение/считывание информации с носителей, декодирование и вычленение из нее той, которая относится к делу. Некоторые исследования могут быть автоматизированы в той или иной степени. Но работать головой и руками на этом этапе эксперту все равно приходится. При этом также должна обеспечиваться целостность информации с исследуемых носителей.

На третьем этапе избранная информация анализируется для получения ответов на вопросы, поставленные перед экспертом или специалистом. При анализе должны использоваться только научные методы, достоверность которых подтверждена.

Четвертый этап включает оформление результатов исследования и анализа в установленной законом и понятной неспециалистам форме.

Контр-форензика

Противодействие методам поиска, обнаружения и закрепления цифровых доказательств развивается не столь активно, как сама форензика. Дело в том, что спрос на соответствующие контрметоды ограничен. Почему ограничен? Для понимания этого давайте посмотрим, кому и для чего может потребоваться противодействовать обнаружению компьютерной информации.

Во-первых, то, что первым приходит в голову, — киберпреступники. Те, кто имеет основания опасаться закона и прятать следы своей криминальной деятельности. Понятно, что это очень узкий рынок сбыта, работать на нем сложно, крупные высокотехнологичные компании вряд ли станут выпускать оборудование и ПО для этого сегмента, даже если будет спрос.

Во-вторых, контрметоды являются составной частью защиты информации. Везде, где имеется подлежащая защите конфиденциальная информация, должны использоваться методы для предотвращения ее утечки. Часть этих методов по борьбе с утечками ориентированы на исключение или затруднение восстановления информации противником.

В-третьих, право граждан на тайну частной жизни (приватность) может обеспечиваться в числе прочих и компьютерно-техническими мерами, которые фактически являются мерами контркриминалистическими [5, 74]. Правда, применение слишком сложных средств и методов здесь невозможно, поскольку указанная самозащита гражданами своего права на тайну частной жизни ограничена квалификацией среднего пользователя. Соответствующие методы не могут требовать высокой квалификации в области ИТ, соответствующие программы должны быть просты в управлении и работать под ОС «Windows», соответствующее оборудование не может быть дорогим. Поэтому здесь обычно ограничиваются довольно примитивной защитой.

Видно, что значительная часть антикриминалистической техники — непрофессиональная, а то и вовсе кустарная. Видно, что антикриминалистический рынок значительно меньше криминалистического. В случае если антикриминалистическая продукция окажется недоброкачественной, предъявлять претензии к производителю, скорее всего, будет некому. Для преуспевания на этом рынке вовсе не требуется выпускать качественное, сложное оборудование и ПО. Требуется лишь хорошо рекламировать свою продукцию или услуги. Чем производители и занимаются.

К защитным антикриминалистическим средствам можно отнести следующие:

- программы и аппаратно-программные устройства для шифрования хранимой информации;

- программы и аппаратно-программные устройства для шифрования трафика;
- программы для очистки дисков и других носителей;
- устройства для механического уничтожения информации на магнитных носителях;
- программы для сокрытия присутствия информации на диске (манипуляция с атрибутами файлов, запись в нестандартные места, стеганография);
- системы и сервисы для анонимизации сетевой активности;
- программы и аппаратно-программные устройства для затруднения копирования произведений, представленных в цифровой форме, затруднения исследования исполняемого кода и алгоритмов программ.

Многие из названных средств будут описаны ниже.

Противодействие указанным средствам также является задачей форензики.

Заключение

Автор должен признаться, что русский термин «форэнзика» пока нельзя признать устоявшимся. Наряду с ним используются также «компьютерная криминалистика» и «компьютерная форензика». Даже в английском, откуда произошло заимствование, нет полного единообразия: «computer forensics», «digital forensics» и «network forensics».

Тем не менее автор полагает приемлемым использовать слово «форензика» без обязательных оговорок. Новая наука обычно сама для себя выбирает название, то есть название дисциплины (как и вся прочая специфическая терминология) зависит от того, как ее будут называть исследователи-первопроходцы, к числу коих автор и надеется быть причисленным.