

3. Следственные действия

Осмотр компьютера

Особенности

Когда следы совершенного преступления и возможные доказательства находятся в цифровой форме (в форме компьютерной информации), их получение, фиксация и документирование представляют определенную сложность.

В отличие от многих иных видов доказательств, компьютерная информация не может восприниматься человеком непосредственно — глазами, ушами, пальцами. Воспринимать ее можно только через посредство технических аппаратных и программных средств. Причем количество и сложность этих технических посредников настолько велики, что связь между исходной информацией и тем, что мы видим на экране, не слишком прямая и далеко не всегда очевидная. А порой эта связь и вовсе условна и зыбка до невозможности (см. главу «Общенаучные методы»).

Следует признать, что осмотр компьютерной информации — это не вполне осмотр (от слова «смотреть»), а скорее инструментальная проверка, требующая определенных знаний об используемых технических средствах, принцип действия которых не всегда очевиден. Вероятность ошибиться и увидеть не то, что есть на самом деле, при этом повышенная, даже при отсутствии целенаправленного воздействия противника.

Высказывалось мнение, что на основании вышеизложенного осмотр компьютерной информации вообще недопустим, а следует всегда проводить экспертизу.

Практика же никак не позволяет принять это утверждение. Провести компьютерно-техническую экспертизу (КТЭ) не всегда возможно даже в тех случаях, когда она точно нужна. Замена экспертизы осмотром позволяет сэкономить очень много времени и сил. Порой перед следователем стоит выбор: или проводить вместо КТЭ осмотр компьютерной информации, или вовсе прекращать дело.

Кроме того, есть и такое соображение. Для проведения КТЭ все равно необходимо изъять носитель информации или скопировать его содержимое. А эти действия по своей сложности и по применению специальных знаний не сильно отличаются от осмотра компьютерной информации на месте. Все равно нужен специалист. Все равно желательны квалифициро-

ванные понятия. Все равно действия эксперта сведутся к просмотру и распечатке нужных данных. Так не проще ли произвести эти же действия в порядке осмотра (ст. 176-177 УПК)?

Стандарты

Правила сбора и фиксации цифровых доказательств (то есть компьютерной информации, используемой в качестве доказательства) не закреплены в законе. Нет и ведомственных нормативных актов, закрепляющих такие правила. А потом в суде возникает вопрос: были ли доказательства собраны надлежащим образом, который обеспечивал их достоверность и неизменность? Оценить правильность примененных процедур без специальных знаний невозможно. Когда же существуют официальные или, по крайней мере, общепризнанные правила обращения с цифровыми доказательствами, обосновать достоверность и неизменность значительно проще.

В отношении других видов доказательств, которыми криминалисты занимаются давно, такие правила существуют.

Закрепление стандартов обращения с цифровыми доказательствами в законодательстве невозможно в силу быстрой изменчивости компьютерных систем. Новые устройства, новые носители, новые протоколы, для которых потребны новые процедуры, появляются несколько раз в год. Ежегодно появляются принципиально новые устройства, которые требуют принципиально иного подхода при обнаружении и изъятии цифровых доказательств. Ведомственные методики [85, 86] можно менять достаточно часто. Однако их разработка в нашей стране затруднена отсутствием грамотных технических специалистов в этих ведомствах.

Столкнувшись с необходимостью подобных стандартов, специалисты предложили зафиксировать их на уровне рекомендаций научных или общественных профессиональных организаций. Исполнение таких стандартов, безусловно, снимет ряд возможных вопросов со стороны суда и участников процесса. Автор рекомендует три подобных документа [W28, 7, 11], изданных достаточно авторитетными в области форензики организациями. Изложенный в них опыт учтен при написании разделов 2 и 3 настоящей книги.

Автор предлагает соблюдать при проведении следственных действий требования таких документов и в дальнейшем ссылаться на них для подтверждения «соблюдения общепринятых и признанных ведущими специалистами правил и стандартов».

Лог-файлы, доказательная сила логов

Определение

Лог (компьютерный лог, компьютерный журнал регистрации событий) — это организованная в виде файла, базы данных или массива в оперативной памяти совокупность записей о событиях, зафиксированных какой-либо программой, группой программ, информационной системой. Лог ведется автоматически, без участия человека. Как правило, соблюдается принцип: одно событие — одна запись. Как правило, каждая запись снабжается меткой времени. Обычно записи сохраняются по мере их генерирования, по возможности, независимо от генерирующей их программы, чтобы они оказались доступны для изучения даже в случае сбоя или аварийного завершения программы.

Форма записей может быть произвольной, на усмотрение создателя программы или оператора, производившего ее настройку. Записи лога могут иметь более «гуманитарную» форму, то есть ориентироваться на восприятие человеком. Записи могут быть машинно-ориентированными, то есть предназначаться для легкого восприятия другой программой. Чаще придерживаются промежуточной формы.

Ведение логов может осуществляться самой генерирующей программой, а может быть передано специализированной (логирующей) программе, такой как «syslogd». Ведение логов (логирование) включает: запись их в соответствующий файл или базу данных, снабжение меткой времени и идентификатором источника, агрегирование (объединение одинаковых или схожих записей), своевременное удаление старых записей и т.д.

Примеры

Ниже автор счел полезным привести образцы некоторых логов, чтобы те читатели, которые редко с ними сталкивались, чувствовали себя более уверенно при изучении дальнейшего материала.

Фрагмент лога сервера электронной почты «sendmail» версии 8.13.3:

```
Dec 14 14:43:12 aihs sm-mta[5156]: kBEDhBbL005156: from=<sonya95wen-king@barnhallrfc.com>, size=6093, class=0, nrcpts=1, msgid=<9bd701c71f85$6f70e79a$93c9135a@barnhallrfc.com>, proto=SMTP, daemon=IPv4, relay=ayc250.internetdsl.tpnet.pl [83.18.106.250]
```

```
Dec 14 14:43:16 aihs sm-mta[5157]: kBEDhBbL005156: to=fnn@home.fnn, delay=00:00:04, xdelay=00:00:04, mailer=esmtpl, pri=36347, relay=home.fnn. [80.94.84.26], dsn=2.0.0, stat=Sent (kBEDhG4D014447 Message accepted for delivery)
```

```
Dec 14 14:44:17 aihs sm-mta[5171]: kBEDiFQH005171: from=<vt@prostimenya.com>, size=8217, class=0, nrcpts=1, msgid=<0458524863.20061214073716@prostimenya.com>, bodytype=8BITMIME,
```

```
proto=SMTP, daemon=IPv4, relay=customer.klimatstroy.195.sls-hosting.com [204.14.1.195]
```

```
Dec 14 14:44:17 aihs sm-mta[5172]: kBEDiFQH005171: to=/dev/null, ctladdr=bit-bucket (26/0), delay=00:00:01, xdelay=00:00:00, mailer=*file*, pri=38486, dsn=2.0.0, stat=Sent
```

```
Dec 14 14:44:39 aihs sm-mta[5173]: kBEDiZU2005173: from=<terri2546zelig@barbary.com>, size=6089, class=0, nrcpts=1, msgid=<848e01c71f85$0df14333$eb8ddf52@barbary.com>, proto=SMTP, daemon=IPv4, relay=[59.24.163.104]
```

```
Dec 14 14:44:39 aihs sm-mta[5174]: kBEDiZU2005173: to=/dev/null, ctladdr=bit-bucket (26/0), delay=00:00:03, xdelay=00:00:00, mailer=*file*, pri=36311, dsn=2.0.0, stat=Sent
```

```
Dec 14 14:50:12 aihs sm-mta[5190]: kBEDoAM6005190: from=<yhky@vampismo.com>, size=8177, class=0, nrcpts=1, msgid=<9454295755.20061214074311@vampismo.com>, bodytype=8BITMIME, proto=SMTP, daemon=IPv4, relay=customer.klimatstroy.195.sls-hosting.com [204.14.1.195]
```

```
Dec 14 14:50:12 aihs sm-mta[5191]: kBEDoAM6005190: to=/dev/null, ctladdr=bit-bucket (26/0), delay=00:00:01, xdelay=00:00:00, mailer=*file*, pri=38444, dsn=2.0.0, stat=Sent
```

```
Dec 14 14:53:42 aihs sm-mta[5192]: kBEDrduu005192: from=<vvvaldiswwh@gmail.com>, size=8704, class=0, nrcpts=1, msgid=<67a901c71f88$5e3e54e$00600ff@gmail.com>, bodytype=8BITMIME, proto=ESMTP, daemon=IPv4, relay=msk-m10-st01.rtcmm.ru [213.59.0.34]
```

```
Dec 14 14:53:42 aihs sm-mta[5193]: kBEDrduu005192: to=/dev/null, ctladdr=bit-bucket (26/0), delay=00:00:03, xdelay=00:00:00, mailer=*file*, pri=38935, dsn=2.0.0, stat=Sent
```

```
Dec 14 14:54:17 aihs sm-mta[5194]: kBEDsGgS005194: from=<ynrripinahov@yahoo.com>, size=8734, class=0, nrcpts=1, msgid=<7fee01c71f8e$052ada06$eb62a1f3@yahoo.com>, bodytype=8BITMIME, proto=ESMTP, daemon=IPv4, relay=msk-m10-st01.rtcmm.ru [213.59.0.34]
```

```
Dec 14 14:54:17 aihs sm-mta[5195]: kBEDsGgS005194: to=/dev/null, ctladdr=bit-bucket (26/0), delay=00:00:01, xdelay=00:00:00, mailer=*file*, pri=38963, dsn=2.0.0, stat=Sent
```

```
Dec 14 14:54:31 aihs sm-mta[5196]: kBEDsTLt005196: from=<iwmn6@bellsouth.net>, size=7116, class=0, nrcpts=1, msgid=<6.0.0.22.1.20061214165536.072e7710@bellsouth.net>, proto=SMTP, daemon=IPv4, relay=84-123-178-52.onocable.ono.com [84.123.178.52]
```

```
Dec 14 14:54:33 aihs sm-mta[5197]: kBEDsTLt005196: to=fnn@home.fnn, delay=00:00:03, xdelay=00:00:02, mailer=esmtpl, pri=37368, relay=home.fnn. [80.94.84.26], dsn=2.0.0, stat=Sent (kBEDsZ8K014471 Message accepted for delivery)
```

Первые три поля каждой записи — это метка времени. Следующие два идентифицируют источник сообщений. Причем эти метки ставятся не генерирующей лог программой («sendmail»), а логирующей программой. Оставшаяся часть сообщений принадлежит уже генерирующей программе.

Можно заметить, что записи лога группируются попарно: каждая пара записей имеет одинаковый идентификатор (группа символов после двоеточия, например, «kBEDsTLt005196»). Пара записей соответствует двум этапам обработки сообщения электронной почты — прием и отправка.

Далее приведен образец лога веб-сервера «Apache» версии 2.1.9-beta. Этот сервер ведет несколько видов логов. Ниже приводится фрагмент лог-файла «access.log» — в этом логе фиксируются обработанные запросы протокола HTTP:

```
83.222.198.130 - - [28/Nov/2006:14:46:35 +0300] «GET /cgi-bin/allip_note.pl HTTP/1.0» 401 475
83.222.198.130 - fnn [28/Nov/2006:14:46:40 +0300] «GET /cgi-bin/allip_note.pl HTTP/1.0» 500 605
83.222.198.130 - fnn [28/Nov/2006:14:47:27 +0300] «GET /cgi-bin/allip_note.pl HTTP/1.0» 200 1053
83.222.198.130 - fnn [28/Nov/2006:14:49:10 +0300] «GET /cgi-bin/allip_note.pl?ip_id=2 HTTP/1.0» 200 2087
83.222.198.130 - fnn [28/Nov/2006:14:49:40 +0300] «GET /cgi-bin/allip_note.pl?ip_id=3 HTTP/1.0» 200 2087
83.222.198.130 - fnn [28/Nov/2006:14:49:49 +0300] «GET /cgi-bin/allip_note.pl?ip_id=4 HTTP/1.0» 200 2087
83.222.198.130 - fnn [28/Nov/2006:14:50:05 +0300] «GET /cgi-bin/allip_note.pl?ip_id=5 HTTP/1.0» 200 2087
83.222.198.130 - fnn [28/Nov/2006:14:56:58 +0300] «POST /cgi-bin/allip_note.pl HTTP/1.0» 200 1101
83.222.198.130 - fnn [28/Nov/2006:14:57:46 +0300] «POST /cgi-bin/allip_note.pl HTTP/1.0» 200 1203
83.222.198.130 - - [28/Nov/2006:16:21:58 +0300] «GET / HTTP/1.0» 401 475
83.222.198.130 - amak [28/Nov/2006:16:22:33 +0300] «GET / HTTP/1.0» 200 360
83.222.198.130 - amak [28/Nov/2006:16:22:34 +0300] «GET /cgi-bin/allip.cgi HTTP/1.0» 404 289
83.222.198.130 - amak [28/Nov/2006:16:23:24 +0300] «GET /cgi-bin/allip-view.pl HTTP/1.0» 404 293
83.222.198.130 - amak [28/Nov/2006:16:23:34 +0300] «GET /cgi-bin/allip-view.pl HTTP/1.0» 404 293
83.222.198.130 - amak [28/Nov/2006:16:23:52 +0300] «GET /cgi-bin/allip-view.pl HTTP/1.0» 404 293
83.222.198.130 - amak [28/Nov/2006:16:24:22 +0300] «GET /cgi-bin/allip_view.pl HTTP/1.0» 200 1260
83.222.198.130 - amak [28/Nov/2006:16:24:56 +0300] «GET /cgi-bin/allip_add.pl?instype=ip HTTP/1.0» 200 2481
```

На данном веб-сайте включена авторизация. Как можно видеть, в 1-й и 10-й записях третье поле содержит «-», то есть логин и пароль пользователя не были переданы серверу. Соответственно, код ответа веб-сервера в

этих случаях — 401 (см. предпоследнее поле). Последующие записи уже содержат имя пользователя (в третьем поле — «fn» и «amak»). То есть, получив в первый раз ответ 401, браузер предлагает пользователю ввести логин и пароль и последующие запросы уже снабжает аутентификационной информацией, отчего они проходят успешно (код 200).

В большинстве записей код ответа веб-сервера 200, что означает успешную обработку. Однако можно заметить коды 500 (внутренняя ошибка сервера) и 404 (страница не найдена).

Последнее поле каждой записи указывает длину ответа веб-сервера в байтах. Как можно заметить, в случае ошибок (401, 404, 500) ответ короткий, а в случае успеха (200) более длинный, поскольку передается веб-страница.

Чтобы верно интерпретировать этот лог, нужно знать значение каждого поля записи. Нетрудно догадаться, например, что первое поле — это IP-адрес клиента, четвертое поле — это время с указанием на часовой пояс. А вот о значении последнего поля догадаться нельзя; о том, что это длина ответа, необходимо знать из документации к веб-серверу.

Лог межсетевого экрана «Netscreen», версия ОС 5.3.0:

```
Dec 14 09:41:09 ns01 moscow-sg2: NetScreen device_id=moscow-sg2 [Root]system-notification-00257(traffic): start_time="2006-12-14 09:41:08" duration=0 policy_id=320001 service=icmp proto=1 src zone=Null dst zone=self action=Deny sent=0 rcvd=540 src=81.16.112.4 dst=81.16.115.162 icmp type=8 session_id=0
```

```
Dec 14 09:41:10 ns01 moscow-sg2: NetScreen device_id=moscow-sg2 [Root]system-notification-00257(traffic): start_time="2006-12-14 09:41:09" duration=0 policy_id=320001 service=icmp proto=1 src zone=Null dst zone=self action=Deny sent=0 rcvd=540 src=81.16.112.4 dst=81.16.115.162 icmp type=8 session_id=0
```

```
Dec 14 09:41:26 ns01 moscow-sg2: NetScreen device_id=moscow-sg2 [Root]system-notification-00257(traffic): start_time="2006-12-14 09:41:22" duration=3 policy_id=2 service=dns proto=17 src zone=Trust dst zone=Untrust action=Permit sent=90 rcvd=389 src=172.23.36.115 dst=81.16.112.5 src_port=1025 dst_port=53 src-xlated ip=81.16.115.169 port=3975 dst-xlated ip=81.16.112.5 port=53 session_id=128000
```

```
Dec 14 09:41:30 ns01 moscow-sg2: NetScreen device_id=moscow-sg2 [Root]system-notification-00257(traffic): start_time="2006-12-14 09:41:24" duration=5 policy_id=2 service=http proto=6 src zone=Trust dst zone=Untrust action=Permit sent=803 rcvd=1422 src=172.23.69.67 dst=217.212.227.33 src_port=10088 dst_port=80 src-xlated ip=81.16.115.166 port=3982 dst-xlated ip=217.212.227.33 port=80 session_id=128009
```

```
Dec 14 09:41:30 ns01 moscow-sg2: NetScreen device_id=moscow-sg2 [Root]system-notification-00257(traffic): start_time="2006-12-14 09:41:23" duration=6
```

```
policy_id=2 service=http proto=6 src zone=Trust dst zone=Untrust  
action=Permit sent=455 rcvd=3166 src=172.23.69.67 dst=216.127.68.107  
src_port=10087 dst_port=80 src-xlated ip=81.16.115.167 port=3969 dst-xlated  
ip=216.127.68.107 port=80 session_id=127975
```

```
Dec 14 09:41:30 ns01 moscow-sg2: NetScreen device_id=moscow-sg2 [Root]sys-  
tem-notification-00257(traffic): start_time="2006-12-14 09:41:26" duration=3  
policy_id=2 service=dns proto=17 src zone=Trust dst zone=Untrust  
action=Permit sent=90 rcvd=389 src=172.23.36.115 dst=81.16.112.5  
src_port=1025 dst_port=53 src-xlated ip=81.16.115.165 port=3965 dst-xlated  
ip=81.16.112.5 port=53 session_id=128000
```

```
Dec 14 09:41:30 ns01 moscow-sg2: NetScreen device_id=moscow-sg2 [Root]sys-  
tem-notification-00257(traffic): start_time="2006-12-14 09:41:23" duration=6  
policy_id=2 service=http proto=6 src zone=Trust dst zone=Untrust  
action=Permit sent=1341 rcvd=7164 src=172.23.69.67 dst=217.212.227.33  
src_port=10085 dst_port=80 src-xlated ip=81.16.115.168 port=4030 dst-xlated  
ip=217.212.227.33 port=80 session_id=127991
```

В этом логе форма представления данных более «человечная», присутствуют метки, позволяющие легко догадаться, к чему относятся приводимые числа. Такие аббревиатуры, как `proto`, `src_port`, `dst_port`, `src-xlated`, говорят специалисту все, что нужно.

Обратите внимание, что в каждой записи присутствуют две метки времени. Одна из них после идентификатора `start_time` ставится генерирующей лог программой (ОС межсетевого экрана), а другая — в начале строки логирующей программой (`syslogd`).

Лог как доказательство

Логи, как правило, не являются непосредственным источником доказательств, но опосредованным. В качестве посредника выступает мнение эксперта или специалиста. Вместо самих логов в качестве доказательств используются: заключение эксперта, заключение специалиста, а также показания изучавших логи свидетелей специалиста, эксперта, понятых. То есть компьютерные логи не являются очевидным доказательством, которое само себя объясняет (такие доказательства, не нуждающиеся в интерпретации, в англоязычной литературе именуют термином «self-evident»). Логи нуждаются в интерпретации.

Автор полагает, что интерпретация логов во всех случаях требует специальных знаний.

Некоторые возражают против доказательности логов, аргументируя это тем, что логи легко фальсифицировать и не существует никакой методики определения истинности логов, отсутствия фальсификации. Это не совсем так [W24].

Во-первых, множество следов других типов фальсифицировать тоже можно. И некоторые — даже проще, чем логи. Волосы, отпечатки зубов,

ворсинки ткани, пороховой нагар и прочее. Не только можно фальсифицировать, но такие попытки регулярно случаются. Несмотря на это, доказательствами все такие следы признаются. Чем логи хуже?

Во-вторых, фальсификацию логов в ряде случаев можно выявить. И чем больше информации в распоряжении эксперта, тем больше вероятность обнаружения подлога.

Цепочка доказательности

Доказательная сила логов базируется на двух столпах — **корректности и неизменности**. А именно — она распадается на следующую цепочку элементов:

- 1) корректность фиксации событий и генерации записей генерирующей программой;
- 2) неизменность при передаче записей от генерирующей программы к логирующей программе;
- 3) корректность обработки записей логирующей программой;
- 4) неизменность при хранении логов до момента изъятия;
- 5) корректность процедуры изъятия;
- 6) неизменность при хранении после изъятия, до осмотра, передачи на экспертизу;
- 7) корректность интерпретации.

В том случае, когда генерирующая программа сама ведет свои логи (не применяется специализированная логирующая программа), пункт 2 выпадает, а пункты 1 и 3 объединяются.

Подчеркнем, что вышеперечисленные пункты составляют именно цепочку, то есть при выпадении одного звена лишаются опоры последующие звенья. В англоязычной литературе используется термин «custodial chain».

Рассмотрим каждый из пунктов по отдельности и укажем, какие меры обеспечивают действительность каждого из них.

Корректность генерирующей программы

Любая программа может содержать ошибки. Ошибки эти могут возникать sporadически или систематически. В первом случае запись может быть верной или неверной, в зависимости от сочетания случайных или псевдослучайных факторов. Во втором случае ошибка будет носить регулярный характер. Вероятность ошибки в программе зависит от ее производителя. Считается, что она в целом ниже для производителей, применяющих передовые технологии производства программного обеспечения, организовавшими процесс производства в соответствии с современными рекомендациями и сертифицировавшими этот процесс по стандарту ISO-9001. Тем не менее ни у какого производителя вероятность ошибки нельзя считать пренебрежимо малой величиной.

Примеры

В качестве иллюстрации систематических ошибок в логах приведем примеры из практики автора.

Программа «акроп3д» — сервер доставки электронной почты (MDA).

Вот фрагмент лог-файла «maillog», в котором собираются логи как от «акроп3д», так и от сервера электронной почты (MTA) «sendmail»:

```
Dec 12 21:34:28 home sm-mta[4045]: kBCIYOxr004045: from=<chadwicks_coupon@1-coupon.com>, size=3494, class=0, nrcpts=1, msgid=<01c71e1c$7a5d7050$6c822ecf@chadwicks_coupon>, proto=ESMTP, daemon=IPv4, relay=aihs-tun [10.5.0.1]
Dec 12 21:34:39 home sm-mta[4046]: kBCIYOxr004045: to=<fnn@home.fnn>, delay=00:00:12, xdelay=00:00:11, mailer=local, pri=33713, relay=local, dsn=2.0.0, stat=Sent
Dec 12 21:38:15 home sm-mta[4051]: kBCICrW004051: from=<Most@anderson-agency.net>, size=49465, class=0, nrcpts=1, msgid=<000c01c71e1c$a3249630$00000000@eigenaarih63rh>, proto=ESMTP, daemon=IPv4, relay=aihs-tun [10.5.0.1]
Dec 12 21:38:17 home sm-mta[4052]: kBCICrW004051: to=<fnn@home.fnn>, delay=00:00:03, xdelay=00:00:02, mailer=local, pri=79666, relay=local, dsn=2.0.0, stat=Sent
Dec 12 21:39:08 home акроп3д[1353]: Connection from 0.80.7.40:1033
Dec 12 21:39:08 home акроп3д[4054]: Authenticated fnn
Dec 12 21:41:01 home акроп3д[4054]: Connection closed
Dec 12 21:45:16 home sm-mta[4076]: kBCIJBAE004076: from=<dthickling@comi-damexicana.com>, size=5985, class=0, nrcpts=1, msgid=<000101c71e82$e4adb7ab$9eb3b218@comidamexicana.com>, proto=ESMTP, daemon=IPv4, relay=aihs-tun [10.5.0.1]
Dec 12 21:45:21 home sm-mta[4077]: kBCIJBAE004076: to=<fnn@home.fnn>, delay=00:00:09, xdelay=00:00:05, mailer=local, pri=36186, relay=local, dsn=2.0.0, stat=Sent
```

В логе зафиксирован доступ по протоколу POP с адреса 0.80.7.40 (см. строку 5), хотя на самом деле доступ был с адреса 10.0.0.2 (в этом сегменте присутствует вообще единственный клиентский компьютер). Подобная запись повторяется в логе из раза в раз. Очевидно, что в программе «акроп3д» имеется систематическая ошибка, приводящая к некорректной записи в лог. Скорее всего, в программе происходит непредусмотренный побитовый сдвиг или данные считываются по неверному адресу памяти.

Другая иллюстрация систематических ошибок в логах. Операционная система межсетевого экрана «Cisco PIX». Для протокола DNS/UDP вместо номера порта показывается ID запроса. Объявлена в версии 4.4(2), исправлена в версии 6.0(1), идентификатор ошибки (caveats) — «CSCdt72080». Всего в системе учета ошибок (Bug Toolkit) фирмы «Cisco Systems» зарегистрировано 312 ошибок, связанных с логами. Общее число ошибок за весь период жизни ПО — десятки тысяч.

Справедливости ради следует отметить, что ПО «Cisco Systems» пользуется хорошей репутацией и имеет далеко не самое высокое удельное число ошибок, которые к тому же исправно учитываются и своевременно исправляются.

Итак, следует признать, что генерирующая логи программа может допускать ошибки. Однако само по себе это обстоятельство не может служить обоснованием для сомнений¹. Таковым обоснованием является лишь наличие известной ошибки, которая удовлетворяет одновременно трем условиям:

а) подтверждена службой техподдержки производителя, его уполномоченного представителя (дистрибьютора, реселлера) или компетентной организацией, занимающейся учетом ошибок и уязвимостей, либо установлена в результате КТЭ;

б) имеет отношение к генерации логов и может привести к их некорректности, что подтверждается заключением или показаниями эксперта или специалиста;

в) может возникнуть именно в тех записях лога, которые имеют значение для дела, что также должно быть подтверждено заключением или показаниями эксперта или специалиста.

При неисполнении хотя бы одного из трех условий ошибка в программе не является основанием для исключения соответствующего лога из числа доказательств по делу.

Неизменность при передаче

При передаче записей от генерирующей программы к логирующей программе ошибки, приводящие к искажению информации, можно не рассматривать. Их вероятность пренебрежимо мала. Зато не мала вероятность недоставки одной или нескольких записей от генерирующей программы к логирующей. Особенно когда эта доставка происходит по протоколу syslog [55], который не имеет механизма подтверждения приема сообщения.

То есть на этом этапе не следует сомневаться в корректности записи о событии, но стоит предусмотреть возможность пропуска одной или нескольких записей. Особенно если при экспертном исследовании были установлены факты пропуска отдельных сообщений при тех же условиях передачи.

Также целостность лога может быть нарушена при записи в файл. При выключении компьютера методом обесточивания и некоторых других критических ситуациях может произойти сбой файловой операции, в результате чего потеряется одна или несколько последних записей лог-файла.

¹ Имеются в виду не любые сомнения, а именно те сомнения, которые упоминаются в презумпции невиновности (ч. 3 ст. 14 УК).

Корректность логирующей программы

Вероятность ошибки, связанной с искажением записи, весьма мала, хотя и не нулевая. Зато весьма существенной является вероятность ошибки, связанной с меткой времени. Время события может содержаться в самой сгенерированной записи, а может и не содержаться. Эта запись передается логирующей программой, которая обычно добавляет свою собственную метку времени. Часы на разных компьютерах могут показывать разное время. Ошибка в установке часов компьютера может быть небольшой, вследствие естественной их неточности; такая случайная ошибка обычно не превышает 1-3 минут. Она может быть большой вследствие ошибочной установки часов, намеренно сдвинутого времени или путаницы часового пояса; такая регулярная ошибка может исчисляться часами, годами и даже десятилетиями.

В связи с изложенным при осмотре и экспертном исследовании необходимо фиксировать показания часов обоих компьютеров — где работает генерирующая логи программа и где работает логирующая программа.

Неизменность при хранении логов

Логи обычно хранятся в текстовом файле, бинарном файле или базе данных. Собственно процесс хранения не чреват ошибками и искажениями содержания логов. Следует учитывать лишь два фактора: возможную намеренную фальсификацию логов каким-либо лицом и уничтожение некоторых записей по истечении установленного срока хранения.

Поэтому во время изъятия логов или при изучении их экспертом необходимо отметить права доступа на запись для различных пользователей, а также настройки систем хранения, ротации и чистки логов.

Сомнения по поводу намеренного искажения логов не могут возникнуть лишь в силу существования самой технической возможности их искажения. Для обоснованности сомнений требуется наличие признаков, свидетельствующих о факте доступа на запись к логам.

Корректность изъятия

Когда логи осматриваются и изымаются «на месте», без передачи компьютера целиком на экспертизу, возможны следующие ошибки.

Логи могут иметь достаточно большой размер — миллионы записей и больше. Просмотреть глазами и распечатать на бумаге такие логи невозможно. Для их просмотра приходится применять фильтры, например, программу **<grep>**. Задать «фильтрующие» выражения — задача простая лишь на первый взгляд. Здесь легко ошибиться даже для специалистам.

Например, мы осматриваем лог веб-сервера **<Apache>**. Сервер активно используется в основном локальными пользователями из сети 10.0.0.0/16. Есть сведения, что злоумышленник осуществлял несанк-

ционированный доступ к этому серверу, используя IP-адрес из другой сети, какой именно, неизвестно. В суточном логе пара сотен тысяч записей, и просмотреть или распечатать его целиком нельзя.

Участвующий в осмотре специалист, особенно не задумываясь, набирает команду, которая на первый взгляд очевидна. Она должна отфильтровать обращения со всех местных IP-адресов, начинающихся на **<10.0.>**, оставив только «чужие» IP-адреса:

```
grep -v " 10.0." /data/apache/logs/access.log
```

(показать все записи лога, кроме тех, где встречается подстрока, указанная в кавычках; перед **<10>** поставлен пробел, чтобы не попали записи, где **<10>** — это второй или третий октет IP-адреса).

В результате происходит незамеченная, но фатальная ошибка! Не обнаруженными оказываются все записи, в которых метка времени соответствует заданному шаблону. То есть все записи в период с 10:00:00 до 10:09:59. В эти-то десять минут злоумышленник и осуществил свой доступ. Специалист забыл, что в шаблоне команды **<grep>** символ **<.>** означает не точку, а любой одиночный символ.

Эту ошибку можно обнаружить постфактум, если в протоколе осмотра точно воспроизведена примененная команда. Эту ошибку можно не только обнаружить, но и исправить, если кроме распечатки выдержки из лога полный лог был скопирован на компакт-диск и приложен к протоколу.

Логи могут храниться в нескольких местах, например, в нескольких файлах. Причем содержимое разных лог-файлов может (а) совпадать, (б) являться подмножеством одно другого, (в) частично пересекаться, (г) взаимно дополнять друг друга без пересечения. Поэтому при изъятии следует зафиксировать настройки, отвечающие за распределение записей по местам хранения. Также важно не упустить какой-либо лог, который может храниться в нестандартном месте.

В протоколе осмотра должны быть указаны сведения, относящиеся как к корректности, так и к полноте осмотра. То есть желательно описать все возможные места хранения логов, привести настройки программ, отвечающих за их хранение, осмотреть и приложить к протоколу в бумажном виде наиболее существенные записи, а все прочие логи, программы, настройки в полном объеме скопировать на диск и приложить к протоколу.

Когда есть такая возможность, лучше произвести полное копирование всего содержимого жесткого диска на самом низком из возможных уровней. Например, при помощи программы **<dd>** или специальным аппаратным дубликатором дисков.

Неизменность после изъятия

Изъятые логи либо распечатываются на бумаге и прилагаются к протоколу, либо записываются на компьютерный носитель, который опечатывается и хранится в деле. Лучше совместить оба способа: наиболее существенные записи лога распечатать, а лог целиком записать на компакт-диск.

Еще одной гарантией корректности осмотра логов и неизменности информации после изъятия является участие в следственном действии специально подобранных понятых. В соответствии с УПК понятой призван удостоверить факт производства следственного действия, а также его содержание, ход и результаты (ст. 60 УПК). Для тех действий, которые проводятся **непосредственно**, понятой не должен обладать какими-то особыми свойствами, кроме исправности зрения, слуха, а также дееспособности. Но действия с компьютерной информацией проводятся отнюдь не непосредственно, а при посредстве разнообразных технических средств. Для применения этих технических средств, разумеется, нужен специалист. Но понятые также должны понимать смысл проводимых действий, их содержание и последствия. Рекомендуется для участия в таких следственных действиях привлекать понятых, обладающих познаниями относительно осматриваемых аппаратных и программных средств, о чем сделать запись в протоколе.

Корректность интерпретации

В ряде случаев записи лога интерпретируются следователем. Иногда спрашивают совета специалиста.

Вспоминается случай, когда материал относительно неправомерного доступа принесли одному генералу. Большую часть материалов составляли разнообразные логи. Также были приложены распечатки записей из базы данных RIPE (регистратора IP-адресов) относительно встречавшихся в логах IP-адресов. Посмотрев бумаги с умным видом, генерал приказал задержать и допросить хакера. Когда опер ему возразил, что злоумышленник пока еще не установлен, генерал заявил, что доказательства, конечно, еще предстоит собрать и оформить, но мы-то хакера уже знаем: вот в логах его фамилия, адрес и телефон — и ткнул пальцем в запись типа «**person**» в распечатке из **whois**.

Автору представляется, что интерпретация лога как такового, без предварительного ознакомления с программами, его создавшими и обработавшими, а также их настройками — некорректна. Поэтому следует документировать не только сами логи, но также имеющие к ним отношение программы, их настройки и окружение. Кроме того, следует получить мнение специалиста или эксперта относительно интерпретации логов на основании вышеуказанной информации.

Процедура приобщения логов

Итак, на основании вышеописанной «цепочки доказательности логов» дадим рекомендации по процедуре получения и приобщения к делу соответствующих доказательств.

Предположим, имеются основания считать, что на известном сервере в логах зафиксированы события, связанные с преступлением и позволяющие установить и изобличить преступника. Как провести следственные действия?

Понятно, что нет возможности доказать отсутствие всех ошибок во всех программах и настройках, нет возможности доказать отсутствие любых фальсификаций со стороны любых лиц. Однако это не означает, что следует ударяться в противоположную крайность и вовсе никак не проверять и не удостоверять корректность и неизменность информации из логов. Вредны обе крайности — как вообще не проверять условий и окружения, так и требовать полного аудита безопасности осматриваемого сервера.

Степень строгости и подробности зависит от возможностей следствия и от судебной практики. Автор предлагает три варианта, отличающиеся строгостью доказывания — нестрогий, промежуточный и строгий. Назовем их соответственно.

Деревенский вариант

Следователь или оперуполномоченный совместно со специалистом (из числа сотрудников, обслуживающих осматриваемый сервер) и понятыми проводит осмотр содержимого сервера. При этом используются штатные программные и аппаратные средства. Составляется протокол осмотра, где отражается следующее:

- характеристики сервера, версия ОС;
- наличие и рабочее состояние программы генерирующей и программы, обрабатывающей логи;
- наличие файлов с логами, их временные метки;
- права доступа к лог-файлам;
- учетные записи (аккаунты) пользователей, имеющих права на запись в лог-файлы.

Нужные записи из нужных логов выбираются при помощи соответствующих фильтров, распечатываются на принтере и прилагаются к протоколу осмотра.

Все листы протокола и приложений подписываются участниками осмотра.

Провинциальный вариант

Для участия в следственном действии приглашается независимый специалист. Представитель владельца сервера (желательно из числа тех-

нических сотрудников) также участвует в осмотре. Понятые приглашаются не любые, а квалифицированные. В протоколе делается запись, что «понятые имеют необходимую квалификацию в области ИТ, знания по осматриваемой технике и ПО и поэтому полностью понимают смысл всех производимых в ходе осмотра действий».

Помимо указанных в предыдущем варианте данных также собираются и отражаются в протоколе следующие:

- сведения о защищенности системы, ее проверке на наличие вредоносных программ, сведения об установленных обновлениях (патчах*);
- подробные данные о генерирующей логи программе, всех ее настройках и окружении (чтобы можно было узнать о выявленных ошибках и оценить вероятность невыявленных);
- данные о протоколе и параметрах передачи логов от генерирующей программы к логирующей;
- подробные данные о логирующей программе, в том числе настройки касательно размещения, срока хранения и ротации логов;
- сведения, помогающие интерпретировать логи, например, описания используемых программ.

Существенные записи из логов выбираются и в печатном виде прилагаются к протоколу. При этом полные логи, задействованные программы и их настройки копируются на компакт-диск типа CD-R или DVD-R (однократная запись), который опечатывается и в случае необходимости отправляется на экспертизу.

Столичный вариант

При участии следователя, квалифицированных понятых, специалиста и представителя владельца сервера нужный сервер отключается, опечатывается должным образом (см. главу «Тактика обыска») и отправляется на экспертизу.

Перед экспертом ставятся вопросы касательно содержания логов, их интерпретации, а также вопросы об известных ошибках, приводящих к некорректности логов, о защищенности системы, о следах возможной фальсификации или несанкционированного удаления логов.

Переносной дубликатор жестких дисков «ImageMASSter Solo-3 IT». Позволяет снять полную, пригодную для экспертного исследования копию содержимого НЖМД прямо на месте происшествия. Поддерживает интерфейсы IDE (ATA), SATA и SCSI



Снятие копии диска

В качестве альтернативы изъятию сервера целиком возможно снятие на месте полной копии его дисков при помощи специализированного аппаратного устройства или программным способом. Копия диска или образа диска (конечно, имеется в виду побитовая копия, «сектор в сектор», «bitstream image») затем передается на экспертизу с такими же вопросами, как если бы передавался сам диск.

Существует несколько моделей аппаратных дубликаторов жестких дисков и несколько программных. К программным относятся «EnCase», «FTK», «SMART», «dd» и его вариации («dd_rescue», «DCFLDD» и др.), «NED». Самый простой из программных дубликаторов — это программа «dd», входящая в состав любой операционной системы класса Unix/Linux.

Естественно, для снятия копии диска надо иметь с собой жесткий диск или несколько дисков суммарной емкостью не меньше, чем копируемый диск.

Копию диска осматриваемого компьютера на месте происшествия можно сделать четырьмя способами:

- из выключенного компьютера извлечь НЖМД, подключить его к компьютеру специалиста (желательно смонтировать в режиме read-only или подсоединить через аппаратный блокиратор записи) и программными средствами, имеющимися на компьютере специалиста, сделать копию;
- из выключенного компьютера извлечь НЖМД, подключить его к аппаратному автономному устройству для дубликации дисков и сделать копию;
- к осматриваемому компьютеру подключить дополнительный НЖМД или иное внешнее устройство и скопировать информацию на него, воспользовавшись программными средствами, имеющимися на осматриваемом компьютере, а лучше — средствами, принесенными специалистом;
- установить с осматриваемого компьютера сетевое соединение с удаленным компьютером (сервером) специалиста и скопировать образ диска туда по сети, воспользовавшись программными средствами, имеющимися на осматриваемом компьютере, а лучше — взятыми с удаленного сервера.

Выбор способа предпочтительно оставить на усмотрение специалиста. При выборе он будет исходить не только из имеющихся в распоряжении средств, но и принимать во внимание другие обстоятельства. Например, насколько вероятно наличие на осматриваемом компьютере руткита* или логической бомбы*, какие последствия повлечет остановка работы исследуемого компьютера и т.п.

Стерильность

В случае, когда копирование дисков производится по схеме «сектор в сектор», очень важно, чтобы целевой диск (на который копируется) был предварительно очищен. То есть все его сектора без исключения должны быть перезаписаны нулями или случайными байтами. В противном случае эксперт, думая, что исследует копию одного диска, на самом деле найдет там остатки предыдущей копии, которые не сможет различить. То, что все сектора целевого диска предварительно очищены, должно быть зафиксировано в протоколе.

Следует помнить, что не все программы, предназначенные для «очистки диска», корректно выполняют свою функцию. Даже не говоря о случаях наличия ошибок и недоработок в программе. Такая программа может не поддерживать (или не вполне корректно поддерживать) текущую файловую систему. Программы, работающие из-под ОС «Windows», могут просто не получить доступ к некоторым областям диска по воле ОС или драйвера. Бывает, что ОС переадресует обращения к некоторым секторам диска на другие секторы. В результате диск очистится не полностью. Для постоянного использования на своем компьютере с целью, например, обеспечения приватности это не страшно. Но для «стерилизации» диска, на который предполагается копировать информацию для последующего исследования, это неприемлемо. Для полной очистки следует применять программы под ОС DOS или UNIX.

В случае, когда копирование дисков производится по схеме «диск в файл», предпринимать меры по предварительной очистке целевого диска не обязательно.

Для той же цели — застраховаться от возможной «нестерильности» целевого диска — при копировании полезно вычислять хэш-функции или контрольные суммы копируемых секторов (групп секторов) и заносить их в протокол. В дальнейшем эксперт может перевычислить значение этих функций для исследуемой копии и тем самым убедиться в ее точности.

Тактика обыска

Когда искомые доказательства могут содержаться на компьютерных носителях, обыск следует проводить согласно нижеизложенным правилам, чтобы обеспечить законность и доказательную силу.

К компьютерным носителям информации относятся съемные и несъемные магнитные диски, компакт-диски (CD), DVD-диски, флэш-накопители, оптические диски, магнитные карты, цифровые кассеты и некоторые другие. Такие носители могут содержаться в персональных компьютерах, серверах, коммуникационном оборудовании, наладонных компьютерах (КПК, PDA), коммуникаторах, смартфонах, мобильных те-

лефонах, цифровых фотоаппаратах и видеокамерах, плеерах и иной другой подобной технике — вся такая техника со встроенными носителями изымается целиком.

Другие виды техники не содержат доступных пользователю носителей компьютерной информации, поэтому ее изымать или исследовать не обязательно. Таковыми являются: принтеры, сканеры, факс-аппараты, а также клавиатуры, мониторы, мыши, джойстики, звуковые колонки. Следует помнить, что техника стремительно развивается и доступные пользователю носители могут завтра появиться в составе таких устройств, какие еще сегодня их не имеют. Стоит вспомнить, например, что в 2000 году аудиоплеер не следовало рассматривать как носитель компьютерной информации, а ныне почти все аудиоплееры (MP3-плееры) по совместительству являются пользовательскими переносными накопителями. В ближайших планах производителей оснастить встроенными компьютерами всю бытовую технику — холодильники, кондиционеры, кофеварки, стиральные машины и т.д. Компьютер в составе бытовой техники, скорее всего, будет включать встроенный или съемный носитель и сетевой интерфейс для удаленного доступа.

Итак, для начала изложим базисные принципы обращения с информационными носителями и компьютерной техникой при проведении обыска, а затем более подробно опишем правила проведения обыска при наличии такой техники.

Принципы

1. Во время изъятия компьютерной техники не должна изменяться никакая содержащаяся на изымаемых носителях информация. На следствии лежит обязанность доказать, что представленная эксперту или суду компьютерная информация не изменялась. Ни в процессе обыска, ни при последующем хранении.

2. Доступ к информации и исследование ее «на месте» допустимы лишь в тех случаях, когда невозможно изъять носитель и отправить его на экспертизу. Такой доступ должен производиться компетентным специалистом, который в состоянии понять и объяснить смысл и все последствия производимых им действий.

3. Должны протоколироваться все действия с компьютерной техникой так, чтобы независимый исследователь мог бы их повторить и получить такие же результаты.

Общие правила изъятия компьютерной техники при обыске

1. Возьмите под контроль помещение, где установлена техника, а также электропитание. Не позволяйте никому, кроме вашего специалиста, дотрагиваться до техники и устройств электропитания. В крайнем случае, ес-

ли отстранить местный персонал от техники невозможно, фиксируйте все их действия.

В тех редких случаях, когда есть основания полагать, что о проведении обыска известно расторопным сообщникам, находящимся вне вашего контроля, то как можно скорее следует отключить сетевые соединения компьютеров. Для этого вытащить из компьютеров кабели локальной сети и отключить модемы. За те несколько минут, пока фотографируют и подготавливают к выключению технику, сообщник, в принципе, может успеть соединиться по сети с компьютером и уничтожить на нем существенную информацию.

2. Выключенные устройства не включайте.

3. Сфотографируйте или снимите на видео компьютерную технику. В крайнем случае, можно зарисовать схему. Уделите внимание кабелям — какой куда подключен. Подключение кабелей также желательно сфотографировать или снабдить их ярлыками для идентификации мест подключения. Всю подключенную к компьютеру периферию следует сфотографировать и/или описать в протоколе, чтобы было ясно, как все было соединено.

4. Если на момент обыска компьютер включен, сфотографируйте или иным образом зафиксируйте изображение на мониторе.

С включенным, но «спящим» компьютером можно поступить двояко: либо сразу, не трогая его, выключить, как описано ниже, либо сначала активизировать, слегка сдвинув мышь, сфотографировать содержимое экрана, а уже затем выключить. Выбор варианта остается за руководителем операции. При «пробуждении» или активизации компьютера может оказаться, что выход из «спящего» режима или из скринсейвера* защищен паролем. Тогда после сдвигания мыши вместо содержимого экрана вы увидите запрос пароля. В таком случае компьютер надо выключить описанным ниже способом.

5. Найдите и соберите листочки, на которых могут быть записаны пароли, сетевые адреса и другие данные, — часто такие записи лежат на рабочем месте, приклеены к монитору, висят на стене.

6. Если принтер что-то печатает, дождитесь окончания печати. Все, что находится в выходном лотке принтера, описывается и изымается наряду с другими носителями компьютерной информации.

7. После этого компьютеры надо выключить. Это должен сделать компетентный специалист. Не позволяйте делать это местному персоналу или владельцу изымаемой техники, не принимайте их советов. Если с вами нет специалиста, выключение настольного компьютера следует производить вытаскиванием шнура питания из корпуса компьютера (не из стенной розетки). Выключение ноутбука следует производить вытаскиванием электрического шнура и извлечением его аккумулятора без закрывания крышки.

Иногда можно ошибиться, приняв включенный компьютер за выключенный. При гибернации («засыпании») экран гаснет, приостанавливаются некоторые функции компьютера. Могут погаснуть или изменить цвет светодиодные индикаторы. Тем не менее у включенного, хотя и «заснувшего» компьютера обязательно горит индикатор питания на системном блоке. У выключенного, напротив, все индикаторы на системном блоке погашены, хотя может гореть индикатор на мониторе. Подробнее о выключении — в параграфе «Как выключать?» главы «Короткоживущие данные».

8. Техника опечатывается таким образом, чтобы исключить как физический доступ внутрь корпуса, так и подключение электропитания. Это обстоятельство отражается в протоколе.

9. Изъятая техника упаковывается сообразно с хрупкостью и чувствительностью к внешним воздействиям. Особо чувствительны к вибрации жесткие магнитные диски (НЖМД); их механическое повреждение (например, из-за перевозки в багажнике) приводит к полной недоступности данных.

10. Опросите всех пользователей на предмет паролей. Надо постараться узнать у каждого сотрудника все известные ему пароли (точнее, пары логин-пароль), имеющие отношение к изъятой технике. Пароли не следует воспринимать на слух. Их надо записать по символам, обращая внимание на алфавит и регистр каждого символа и выверить у источника. Пароли допустимо не вносить в протокол допроса или объяснение, а записать просто на бумажке. Их доказательное значение от этого не снижается.

Особенности

Относящаяся к делу компьютерная информация и иные цифровые следы криминальной деятельности могут содержаться во множестве цифровых устройств и носителей. Во время обыска нужно постараться обнаружить все такие устройства и носители, быстро решить, может ли в них содержаться интересующая информация, и изъять их, если может.

Для обнаружения таких носителей или устройств необходимо участие специалиста.

На случай, когда специалиста нет, на последующих иллюстрациях приведены наиболее распространенные устройства, могущие содержать в себе компьютерную информацию.

Ниже приводятся рекомендации по обращению с некоторыми видами компьютерной техники. Ими следует руководствоваться только при отсутствии в вашей группе технического специалиста. Специалист должен знать, как следует обращаться с каждой конкретной моделью техники, чтобы сохранить информацию в неизменном виде. В присутствии специалиста надо следовать его указаниям.

Ноутбук (лэптоп, переносной компьютер)

Если ноутбук включен на момент начала обыска, то прежде всего следует сфотографировать или иным образом зафиксировать содержимое экрана, как это указывалось выше.

Чтобы выключить ноутбук, недостаточно вытащить из него шнур питания; при этом ноутбук перейдет на питание от аккумулятора. Для обесточивания надо извлечь аккумулятор. При этом не следует закрывать крышку ноутбука, складывать его. При складывании обычно активизируется функция гибернации («засыпания»), а это означает внесение изменений в информацию на диске, что нарушит вышеозначенные принципы.

Наладонный компьютер (КПК)

К данному классу относятся: КПК, PDA (Personal Digital Assistant), palmtop, pocket PC, органайзеры, смартфоны, коммуникаторы, электронные дневники [51, 84, 93].

Особенностью этого класса компьютеров является то, что значительная часть пользовательских данных хранится у них в оперативной, энергозависимой памяти. При отключении питания наладонника вся такая информация безвозвратно пропадет.

Штатное состояние «выключен» у наладонника фактически означает не выключение, а режим «засыпания» или гибернации. При этом электроэнергия расходуется только на поддержание оперативной памяти. Храниться в таком состоянии он может до нескольких дней, в зависимости от текущего состояния аккумулятора.

Если наладонник включен (активен) на момент начала обыска, то прежде всего следует сфотографировать или иным образом зафиксировать содержимое экрана, как это указывалось выше. При неактивности экран автоматически гаснет, а наладонник переходит в режим гибернации через



Наладонный компьютер, сменный модуль памяти (SD), крэлл и стилус к нему

несколько минут. После фотографирования можно выключить его вручную кнопкой «power», если есть такая кнопка.

Касаться экрана наладонника нельзя, поскольку экран у него является чувствительным; каждое прикосновение к экрану воспринимается как команда.

Извлекать аккумулятор из наладонника нельзя.

Вместе с ним обязательно следует изъять крэлл (подставку с устройством питания и сопряжения) либо иное зарядное устройство. Хранить наладонник сам по себе, без подзарядки, можно недолго, обычно несколько дней. Длительность хранения зависит от первоначального состояния аккумулятора. После его истощения содержимое оперативной памяти будет утрачено. Лучше не рисковать и после изъятия как можно быстрее передать компьютер эксперту. А до такой передачи, по возможности, хранить его вставленным в крэлл, чтобы аккумулятор не истощался. В крэлле (который, естественно, должен быть подключен к электросети) хранить наладонник можно неограниченно долго. Правда, хранение в крэлле несовместимо с опечатыванием компьютера.

В протоколе обыска (изъятия, личного досмотра) следует указать примерно следующее: «При осмотре и изъятии наладонного компьютера его кнопки не нажимались, экрана не касались, аккумулятор или съемные накопители не извлекались. Наладонный компьютер в состоянии гибернации (засыпания) был упакован и опечатан так, чтобы исключить всякий доступ к органам его управления (клавиши, экран) и к его разъемам без повреждения печатей».

Принтеры

Современные принтеры (за очень редким исключением) не имеют доступных пользователю носителей компьютерной информации. Поэтому изымать принтеры нет необходимости. Надо только изъять все распечатки, обнаруженные в выходном лотке принтера или подле него, поскольку такие распечатки также содержат компьютерную информацию. Кроме того, некоторые фотопринтеры имеют разъем для непосредственного подключения носителей информации типа флэш-накопителей. Если такой накопитель оставлен в разъеме принтера, его нужно изъять, а принтер можно не трогать. При проведении осмотра или обыска следует отразить в протоколе наличие принтера и способ его подключения к компьютеру.

Из этого правила есть одно исключение — дела о подделке документов.

Принтеры очень часто используются для изготовления поддельных документов, поскольку их разрешающая способность (от 600 точек на дюйм и больше) превышает разрешающую способность человеческого глаза. То есть фальшивку, отпечатанную на современном принтере, отличить на глаз нельзя.

Экспертиза может установить, что поддельный документ был напечатан именно на этом конкретном принтере или с использованием конкретного картриджа.

Когда в деле фигурируют поддельные документы, то кроме компьютеров и машинных носителей информации следует также изымать:

- принтеры;
- картриджи для принтеров (кроме, может быть, новых в упаковке) и иные расходные материалы (тонер, ленты, чернила);
- все обнаруженные распечатки;
- чистую бумагу и пленку, приготовленные для использования в принтере.

Принтер следует опечатать так, чтобы сделать невозможным подключение электропитания и доступ к печатающему узлу без нарушения упаковки. Этот факт отразить в протоколе. Иные изъятые материалы также следует опечатать.

Сканеры

В сканерах так же, как и в принтерах, нет доступных носителей информации. Изымать их нет смысла.

К сожалению, нет возможности установить, было ли то или иное изображение (скан-копия) получено с конкретного сканера.

При проведении осмотра или обыска следует лишь отразить в протоколе наличие сканера и способ его подключения к компьютеру.

Флэш-накопители

Накопители на флэш-памяти выпускаются в виде самостоятельных устройств, а также в составе других устройств, таких как аудиоплееры или цифровые фотоаппараты. Форма и размер устройств с флэш-накопителями также весьма разнообразны. Чаще всего такие накопители снабжены интерфейсом типа USB, по которому их и можно опознать.

Такие накопители не теряют данные при отсутствии электропитания, поэтому их можно хранить долгое время. При изъятии следует опечатать так, чтобы исключить доступ к USB-разъему и органам управления (если такие органы есть).

Снять копию флэш-накопителя на месте, в принципе, можно. Как это сде-



Флэш-накопитель в виде брелка



Флэш-накопитель в составе аудиоплеера



Флэш-накопитель в часах



Электронная фоторамка со встроенным флэш-накопителем

лать, рассказано в разделе «Компьютерно-техническая экспертиза». Но особой необходимости в таком копировании нет, поскольку флэш-накопитель все равно изымается, когда есть основания полагать, что на нем может содержаться существенная для дела информация. Затем он передается на экспертизу. Снимать копию на месте логично в тех случаях, когда ждать результатов экспертизы нет времени и нужно быстро получить информацию для продолжения расследования. В таких случаях специалист снимает копию с накопителя на месте, сам накопитель опечатывается, изымается и откладывается ждать экспертизы, а его копия подвергается исследованию с целью получения неофициальной, зато срочной информации.

Мобильные телефоны

Перед тем, как рассмотреть изъятый мобильный телефон в качестве носителя компьютерной информации, следует решить, требуется ли получить с него материальные следы — отпечатки пальцев, следы наркотиков, иные.

Следует помнить, что некоторые методы снятия отпечатков могут привести телефон в негодность.

В большинстве случаев при изъятии нужно выключить мобильный телефон, чтобы исключить потерю имеющихся данных вследствие поступления новых вызовов и новых SMS. Аккумулятор вынимать не следует.

Однако в некоторых случаях руководитель операции может решить, что контролировать поступающие вызовы важнее. Тогда телефон надо оставить включенным и подзаряжать его по мере необходимости.

Выключенный телефон упаковывается в жесткую упаковку и опечатывается так, чтобы исключить доступ к органам его управления. Это отмечается в протоколе.

При выключении телефона не надо беспокоиться о PIN-коде на доступ к данным в SIM-карте телефона. У оператора связи в любой момент можно узнать PUK (PIN unlock key) и с его помощью получить доступ к SIM-карте.

О полевом и лабораторном исследовании информации из мобильных телефонов есть достаточно много технической литературы [60].

Коммутаторы и маршрутизаторы

Обычно коммутатор* (switch) имеет внутреннюю энергонезависимую память, в которой помещается только операционная система и файл конфигурации. Именно конфигурация может быть предметом интереса следствия. Мелкие коммутаторы могут не иметь доступной пользователю памяти, хотя свою конфигурацию (настройки) все же сохраняют. Совсем мелкие коммутаторы для домашнего использования и хабы могут не иметь даже настроек.

Маршрутизатор* (router), в зависимости от своего назначения, может иметь столь же небольшую память, как и коммутатор, где хранится лишь относительно небольшой файл конфигурации, а может иметь и более существенное устройство хранения, например, жесткий диск.

Конфигурация маршрутизатора или коммутатора может заинтересовать следствие лишь при некоторых специфических типах преступлений. В большинстве случаев их конфигурация не представляет интереса.

Снять всю конфигурацию с маршрутизатора или коммутатора специалист может на месте, если знать пароль для доступа.

Включенные коммутаторы и маршрутизаторы следует при изъятии отключать вытаскиванием электрического шнура либо аппаратным пе-

реключателем (рубильником), который находится прямо на встроенном блоке питания.

Автомобильные компьютеры

Бортовым компьютером оснащены практически все современные модели автомобилей. Основное его предназначение — оптимизация режима двигателя с целью экономии горючего. Компьютер собирает многочисленные данные с различных устройств автомобиля. В случае аварии в нем можно найти сведения о нескольких последних секундах — скорость, обороты, позиции педалей газа и тормоза, режим стеклоочистителей, осветительных приборов и т.п.

Кроме того, бортовой компьютер выполняет навигационные функции либо для этого установлен отдельный навигационный компьютер. В нем фиксируется расположение автомобиля в разные моменты времени, вычисляются возможные маршруты следования до заданных точек.

К сожалению, бортовые компьютеры не унифицированы, как персональные. Расположение компьютера и его запоминающего устройства зависит от модели автомобиля. Для изъятия или копирования носителей компьютерной информации следует пригласить специалиста из фирменного (авторизованного) центра техобслуживания соответствующего автопроизводителя.



Образец автомобильного навигационного компьютера

Модемы

В некоторых модемах хранится пользовательская информация — настройки сети или телефонные номера провайдера. Если нет специалиста, который может указать, какая именно модель модема здесь присутствует — с памятью или без, — то модем надо отключить от электропитания, опечатать и изъять.

Цифровые фотоаппараты

Практически все цифровые фотоаппараты (фотокамеры) имеют сменный и встроенный накопитель достаточно большой емкости. Этот накопитель доступен пользователю не только для чтения, но и для записи. Поэтому кроме отснятых фотографий и видеороликов там можно найти и иную пользовательскую информацию. Иногда цифровой фотоаппарат используется в качестве переносного USB-накопителя.



Цифровые фотоаппараты могут иметь форму как традиционную, так и непривычную

Сменные накопители

Есть несколько стандартных типов таких накопителей. Это ныне уже устаревшие и выходящие из употребления гибкие магнитные диски (ГМД) или дискеты, магнитооптические диски, компакт-диски (CD), DVD-диски, сменные флэш-карты, а также НЖМД, выполненные в отдельном корпусе.



Различные типы сменных накопителей на основе флэш-памяти

Короткоживущие данные

В этой главе мы рассмотрим, как специалист при проведении следственного действия должен обращаться с короткоживущими, или волатильными данными. Этим термином обычно именуют такую информацию, которая недолговечна и существует лишь до момента выключения компьютера или до завершения определенной программы.

Перечень

Вот некоторые из типов короткоживущих данных:

- содержимое ОЗУ*, то есть все исполняемые в текущий момент программы (задачи, процессы), системные и прикладные (пользовательские);
- прежнее содержимое ОЗУ в областях оперативной памяти, которые на текущий момент считаются свободными;
- список открытых файлов со сведениями, какой процесс каким файлом пользуется;
- информация о пользовательских сессиях, то есть вошедших в систему (залогиненных, зарегистрированных) пользователях;
- сетевая конфигурация — динамически присвоенный IP-адрес, маска подсети, ARP-таблица, счетчики сетевых интерфейсов, таблица маршрутизации;
- сетевые соединения — информация о текущих соединениях (коннекциях) по различным протоколам, о соответствующих динамических настройках межсетевого экрана* или пакетного фильтра;
- текущее системное время;
- список назначенных заданий (scheduled jobs);
- кэш доменных имен и NETBIOS-имен;
- загруженные модули ядра (LKM);
- монтированные файловые системы, подключенные сетевые диски;
- файл или область подкачки* (swap-файл) на диске — информация о текущем состоянии виртуальной части ОЗУ, а также ранее находившиеся там данные;
- временные файлы, которые автоматически стираются при штатном завершении работы ОС или при загрузке ОС.

Все перечисленные данные, кроме последних двух пунктов, хранятся в ОЗУ.

Кроме того, к короткоживущим данным можно причислить образцы сетевого трафика* в обоих направлениях — с исследуемого компьютера и на него. Проанализировать устройство и функции программы по содержимому ОЗУ (дампу памяти*) бывает довольно сложно. Зато по генерируемому программой трафику во многих случаях нетрудно определить ее

функции. Поэтому образец трафика компьютера за какой-то разумный период времени будет хорошим дополнением для исследования работы неизвестных программ.

Понятно, что короткоживущие данные (кроме области подкачки*) можно снять лишь с работающего компьютера. После выключения все такие данные будут утрачены. То есть снятие короткоживущих данных производится не экспертом при проведении КТЭ, а специалистом во время следственного действия. Исключение — экспертиза КПК* (наладонного компьютера), который обычно хранится во включенном состоянии, но в режиме гибернации*.

Стоит ли пытаться снять с работающего компьютера короткоживущие данные? С одной стороны, среди них могут оказаться полезные и даже очень ценные, например, запись о текущей ТСР-сессии с атакуемым узлом или ключ для доступа к криптодиску*. С другой стороны, при снятии содержимого ОЗУ невозможно не изменить информацию на компьютере, в том числе на его диске. Это может отрицательно повлиять на оценку достоверности последующей экспертизы. В каждом случае это решает специалист, оценивая, какой аспект важнее для дела — сохранность долгоживущей информации или возможность получить короткоживущую критичную. Разумеется, для этого специалист должен быть проинформирован о существенных обстоятельствах дела.

Например, при использовании подозреваемым криптодиска получить доступ к его содержимому можно либо как-то узнав пароль, либо застав компьютер во включенном состоянии с активированным (монтированным) криптодиском. После демонтажа криптодиска узнать пароль непросто. В практике автора было несколько случаев, когда у подозреваемого удавалось выяснить пароль к его криптодиску путем изощренного обмана или примитивного запугивания. Однако грамотный в области ИТ пользователь знает четко: если он не сообщит пароль, то расшифровать данные на криптодиске невозможно. Остается второй способ. Надо каким-то образом прорваться к включенному компьютеру и, пока доступ к криптодиску открыт, снять с него все данные или извлечь из ОЗУ ключ шифрования.

Стоит ли пытаться снять короткоживущую информацию, рискуя при этом существенно изменить данные на нем или сразу выключить компьютер, — решает специалист, исходя из материалов дела.

В любом случае, настоятельно рекомендуется снять минимально возможную без риска короткоживущую информацию — сфотографировать или описать текущее изображение на экране включенного компьютера.

Снятие

Для сбора короткоживущей информации из ОЗУ и свопа* есть различные программные инструменты под различные ОС. Специалисту предпочтительно не надеяться, что такие инструменты найдутся на исследуемом компьютере, а пользоваться своими собственными программами, которые заранее приготовлены на дискете, компакт-диске или флэш-накопителе. Чаще всего используют компакт-диск.

Кроме того, следует приготовить еще один носитель — для записи результатов снятия короткоживущей информации. Предпочтителен флэш-накопитель. Для сброса результатов вместо флэш-накопителя или иного устройства можно подключить в качестве сетевого диска диск удаленного компьютера. Таковым может служить переносной компьютер специалиста, принесенный им с собой и подключенный к тому же сегменту ЛВС, или стационарный компьютер специалиста, доступный через Интернет. Сбрасывать полученные короткоживущие данные на жесткий диск исследуемого компьютера категорически не рекомендуется. Этим можно уничтожить некоторую существенную для дела информацию и поставить под сомнение результаты последующей экспертизы.

Корректность работы программных инструментов по снятию информации с работающего компьютера зависит не только от самих этих инструментов. На результат может влиять также состояние исследуемого компьютера. Например, если он заражен вредоносной программой типа руткит*, то специалист может и не получить корректную информацию, даже при безупречной работе его инструментов.

Вот некоторые полезные программы для сбора короткоживущих данных:

- Утилиты «PMDump», «userdump», «dd» позволяют снимать содержимое ОЗУ компьютера (дамп памяти). Запуск любой программы изменяет содержимое ОЗУ, поэтому результат работы таких утилит будет не вполне «чистый». Но это неизбежная погрешность.
- Утилиты «ifconfig», «ipconfig», «arp», «route», «netstat», «ipfw», «ipfilter», «ipchain», «iptables» снимают текущую сетевую конфигурацию компьютера.
- Утилиты «netstat», «nmap» снимают информацию о текущих сетевых соединениях и открытых портах.
- Утилиты «Task manager», «pslist», «ps», «top» дают список текущих процессов — исполняемых программ.
- Утилиты «lsof» дают список открытых в текущий момент файлов.
- Утилиты «w», «last» дают список пользователей, вошедших в систему.
- Утилиты «date», «nlsinfo» дают информацию о текущем системном времени.

- Утилиты «ethereal», «tcpdump» дают возможность снять текущий сетевой трафик компьютера.
- Утилиты «lsmode», «kldstat» показывают список загруженных модулей ядра.

Какую именно короткоживущую информацию собирать и в каком порядке? Зависит от характера доказательств, которые мы предполагаем найти.

Когда речь идет о «взломе» исследуемого компьютера или заражении его вредоносной программой, следует собирать: содержимое ОЗУ, список процессов, список открытых портов, список пользователей, сетевую конфигурацию, образец трафика.

Когда дело касается электронной переписки или незаконного контента, возможно хранящегося на исследуемом компьютере, следует собирать: список процессов, информацию о криптодисках*, текущее время, возможно, сетевую конфигурацию.

Когда речь идет о неправомерном доступе, предположительно осуществленном с исследуемого компьютера, следует собирать: список процессов, информацию о текущих сетевых соединениях, образец трафика.

По делам о нарушении авторских прав следует собирать: список процессов, текущее время, содержимое временных файлов и области подкачки*.

Вообще-то, если есть возможность, лучше собирать всю доступную короткоживущую информацию.

Порядок сбора информации рекомендуется такой, чтобы сначала собирать самую короткоживущую. А именно — собирать ее в такой последовательности:

- текущие сетевые соединения;
- текущие пользовательские сессии;
- содержимое ОЗУ;
- список процессов;
- открытые файлы;
- образец трафика;
- ключи и пароли;
- сетевая конфигурация;
- текущее время.

Когда сетевые моменты не важны (например, компьютер не подключен к сети в текущий момент), содержимое ОЗУ (дампы памяти) следует снимать в первую очередь — для его наименьшего искажения, поскольку, как уже указывалось, запуск любой программы изменяет состояние оперативной памяти ЭВМ.

Прежде чем снимать короткоживущую информацию с включенного компьютера, бывает необходимо преодолеть препятствия в виде:

- активного скринсейвера* (заставки) с парольной (парольно-биометрической) защитой;
- недостаточных привилегий текущего пользователя;
- заблокированных, отключенных или отсутствующих возможностей для подключения внешних устройств (порт USB, CD-привод).

Имеет ли право специалист задействовать для преодоления такой защиты специальные средства — программы, относящиеся к средствам несанкционированного доступа, вредоносным программам или средствам обхода защиты авторских прав?

Вообще-то имеет. Кроме вредоносных программ, использование которых противозаконно в любом случае.

Как выключать?

Каким способом следует выключать компьютер, который подлежит изъятию и который застали во включенном состоянии?

По большому счету, выбор сводится к двум вариантам: воспользоваться штатной командой выключения или выключить прерыванием электропитания. Рассмотрим преимущества и недостатки каждого из методов.

Команда завершения работы и выключения компьютера имеется в составе почти всех ОС. Часто та же команда не только завершает работу ОС, но и выключает электропитание. Иногда только завершает работу, а блок питания надо будет выключить вручную.

Во время процедуры завершения работы закрываются все открытые файлы, стираются временные файлы, иногда очищается область подкачки* (своп). Кроме того, всем текущим процессам посылается сигнал завершения работы. Что именно будет делать программа, получив такой сигнал, в общем случае сказать нельзя. Большинство программ просто завершают работу. Некоторые сохраняют промежуточные варианты данных. Другие, напротив, стирают свои временные файлы. Ряд вредоносных программ, таких как троян* или руткит*, могут при сигнале завершения работы целенаправленно уничтожить следы своего присутствия.

Если перед выключением специалист снял короткоживущие данные, как это описано выше, то почти все недостатки этого метода выключения можно считать компенсированными.

Кроме того, при завершении работы может сработать специально установленная логическая бомба*, которая уничтожит самые важные данные. Такие бомбы (к тому же связанные с командой завершения работы) встречаются редко, но все же...

Прерывание электропитания осуществляется вытаскиванием электрического шнура из компьютера. Причем лучше вытаскивать тот конец,

который подключен к компьютеру, а не тот, который к стенной розетке. Дело в том, что между розеткой и компьютером может оказаться источник бесперебойного питания*. Он не только станет поддерживать напряжение, но и может дать компьютеру команду завершения работы. Для ноутбуков, кроме того, следует извлечь аккумулятор.

В случае прерывания электропитания все временные файлы остаются нетронутыми. Но зато может быть нарушена целостность файловой системы, если прерывание электропитания застанет компьютер в момент проведения файловой операции. Испорченная файловая система в большинстве случаев может быть потом восстановлена, но не все экспертные системы поддерживают такую операцию, а экспертное изучение испорченной файловой системы затруднено. Кроме того, могут появиться локальные дефекты в некоторых открытых на запись файлах, например лог-файлах.

Вариант выключения выбирает специалист, исходя из обстоятельств дела: насколько важны временные файлы, можно ли предполагать наличие вредоносных программ. При отсутствии специалиста или при неясности указанных обстоятельств следует избрать метод выключения прерыванием электропитания.

Стоит ли упоминать, что примененный метод выключения компьютера должен быть указан в протоколе?

Некоторые криминологи даже советуют поступать следующим образом [52]. Если подозреваемый, в доме или на рабочем месте которого производится обыск, настаивает на «правильном» выключении компьютера, то согласиться для виду, но не позволять ему проделывать такую операцию. Вместо этого попросить написать или нарисовать необходимую последовательность действий. Этот документ приобщить к делу, а компьютер выключить методом обесточивания. При последующей экспертизе, если эксперт установит, что описанная подозреваемым последовательность действий должна была привести к уничтожению существенной для дела информации, это будет лишним доказательством вины и, возможно, отягчающим обстоятельством.

Автор относится скептически к такому совету и полагает, что применить его вряд ли удастся. Тем не менее следует помнить о возможности подобного обмана со стороны подозреваемого.

Например, многие модели криптодисков* имеют штатную возможность под названием «пароль для работы под контролем». Это альтернативный пароль, при вводе которого вместо подключения криптодиска безвозвратно уничтожается ключ шифрования¹, так что все защищенные

¹ Ключ шифрования не совпадает с паролем. Обычно пароль или производный от него ключ используется для зашифровки основного ключа шифрования. Таким образом, при уничтожении основного ключа пароль остается бесполезным, а данные — недоступными.

данные становятся недоступны навек. При этом либо имитируется внешний сбой, либо вместо истинного криптодиска подключается имитационный, с безобидными данными. Еще раз напомним, что «работа под контролем» — это не кустарная поделка, а штатная возможность всякой добротной сделанной системы защиты.

Работа с потерпевшими

Компьютерная информация имеет свойство легко и быстро утрачиваться. Задержка при сборе доказательств может привести к их неполучению. Поэтому потерпевших и свидетелей надо опросить на предмет таких доказательств как можно быстрее, не дожидаясь официального допроса.

У потерпевших и очевидцев следует узнать следующее.

Преступления, связанные с электронной почтой:

- адреса электронной почты — корреспондента и его собственный;
- сохранилось ли сообщение электронной почты (письмо), где именно оно сохранено;
- если сообщение сохранено, попросите передать его так, чтобы были доступны ВСЕ служебные заголовки, как это сделать, зависит от используемой программы-клиента;
- какая программа-клиент использовалась либо какой веб-интерфейс¹.

Преступления, связанные с веб-сайтами:

- каков адрес (URL) веб-сайта;
- услугами какого интернет-провайдера пользуется потерпевший;
- в какое время (желательно точнее) он посещал веб-сайт;
- сохранилась ли у него копия или скриншот* этого веб-сайта.

Преступления, связанные с телеконференциями (newsgroups):

- услугами какого интернет-провайдера пользуется потерпевший;
- каково имя телеконференции;
- через какой ньюс-сервер осуществлялся доступ к телеконференциям;
- какое использовалось ПО для доступа к телеконференциям, не осуществлялся ли этот доступ через веб-гейт;
- каков subject и другие данные сообщения;
- сохранилось ли сообщение телеконференции, где именно оно сохранено;
- если сообщение сохранено, попросите передать его так, чтобы были доступны ВСЕ служебные заголовки, как это сделать, зависит от используемой программы-клиента.

¹ Некоторые пользователи никогда не работали с клиентами электронной почты, а использовали только лишь веб-интерфейс. Они могут не понимать разницы между ними или быть уверены, что не существует иного способа работать с электронной почтой, чем при помощи браузера.

Заключение к разделу 3

Хотя многие устройства, несущие компьютерную информацию, а также многие программы предназначены для обычных пользователей, проводить с ними следственные действия нужно всегда с участием специалиста. Пользоваться — это далеко не то же самое, что изымать или проводить осмотр, фиксировать доказательства. При простом пользовании электронным прибором или программой происходит неконтролируемое изменение данных. Такое скрытое изменение нисколько не вредит функциональности устройства, оно заранее предусмотрено производителем. Но для следственных действий любое неконтролируемое или неявное изменение компьютерной информации недопустимо. Не допустить его может только специалист.

Чтобы обеспечить упоминавшуюся цепочку доказательности (корректность и целостность от момента начала следственного действия до момента завершения экспертизы), требуется участие специалиста, знакомого с особенностями хранения и обработки данных соответствующими электронными устройствами или программами.