Раздел V. Новые информационные технологии в энергетике

УДК 681.3: 681.323

В. В. Борисов

ОБ ОСОБЕННОСТЯХ ФИКСАЦИИ ИНФОРМАЦИОННЫХ СЛЕДОВ В ПРАКТИКЕ ЗАЩИТЫ ИНФОРМАЦИИ

Работа посвящена изучению новых принципов следообразования в сфере компьютерной информации. Введено понятие "информационного следа". Рассмотрен общий алгоритм фиксации информационных следов и особенности его технической реализации.

Защита информации; криминалистика; веб-ресурс; следообразование.

V. V. Borisov

THE FEATURES OF A FIXED INFORMATION TRACES THE PRACTICE OF INFORMATION SECURITY

The work is devoted to the analysis of the new principles in information traces fingerprinting. New definition of term "information trace" is placed. In the article new algorithm for information traces fixation is given and review of special technical features resulted.

Information security; criminology; web-site; fingerprinting.

Постановка задачи исследования. Возникновение следов имеет свои закономерности не только в реальном мире, но и в киберпространстве. Изучение данных закономерностей обеспечивает быстрое обнаружение и правильное использование следов в целях установления обстоятельств, имеющих значение для расследуемого дела. Особенно важным является изучение закономерностей процессов следообразования в сфере информационных технологий, поскольку компьютерная информация чрезмерно волатильна и наиболее легко подвержена изменениям и сокрытию.

Обращаясь к юридическим наукам, можно утверждать, что опытом криминалистики доказана невозможность совершения преступления без оставления при этом тех или иных следов. При этом, чем полнее познаны закономерности образования различных следов, тем скорее они могут быть обнаружены.

Данный факт, очевидно, имеет место и в информационно-вычислительной среде, особенно когда это касается вопросов защиты информации. Однако следообразование в сфере компьютерной информации имеет ряд существенных отличительных признаков, в корне меняющих представление о корректном взаимодействии со следами и их фиксации.

Понятие "информационных следов". Для удобства обозначения мы введем термин "информационный след", который обозначает некоторую информационную запись, сделанную на компьютерной технике подозреваемых в преступлении лиц с помощью специального программного средства и произведенную субъектом уголовно-процессуальной системы (например, следователем).

С одной стороны, процесс возникновения доказательств, как и всякий процесс отражения происходившей когда-либо действительности, является ситуационным. В этом смысле существующая трасологическая теория и практика в полной мере применима и к новейшим информационным технологиям. Именно по этой причине возникновение новых информационных технологий не послужило само по себе толчком к созданию нового направления в трасологии.

Но с другой стороны, информационные следы и сам процесс следообразования в компьютерной технике имеют ряд существенных отличий от аналогичных физических процессов, происходящих в реальной жизни. Например, имеют место следующие проблемы, стоящие перед специалистом, расследующим преступления в сфере компьютерной информации:

– неочевидность и нечеткая связь мест, в которых образуются следы той или иной деятельности, фиксируются результаты и промежуточные данные вычислительных процессов с происходящими событиями;

– легкость устранения информационных следов лицом, совершившим противоправное действие, в случае если он предпринимает такую попытку;

– сложность фиксации следов (редко удается сделать это в ручном режиме, силами самого следователя), и как следствие, необходимость разработки и применения специального программного обеспечения (которое позволяет фиксировать информационный след) на профессиональном уровне.

Информационные следы, также как и следы физические, могут быть использованы при решении как оперативно-розыскных, так и идентификационных задач. Особенно важна взаимосвязь информационных следов не только с точки зрения производства действий уголовно-процессуального характера в сфере компьютерной информации, но и в ходе осуществления других мер по повышению эффективности расследования.

Технические особенности формирования информационных следов. Рассмотрим практическую сторону процессов следообразования в сфере информационных технологий на примере веб-ресурсов. Информационные веб-ресурсы появляются в поле зрения оперативных работников, как правило, по причине размещения на них материалов, способствующих разжиганию ненависти и национальной вражды (действия, квалифицирующиеся по ст.282 УК РФ "Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства").

В ходе анализа веб-ресурсов внимание должно уделяться в первую очередь журнальным файлам и принятой системе журналирования. Журналирование в данном контексте − процесс записи информации о происходящих с каким-то объектом (или в рамках какого-то процесса) событиях в журнал (например, в файл). Важно знать, какое программное обеспечение и в каких модификациях установлено на веб-ресурсе. Данная информация позволяет выяснить наличие и месторасположения журнальных файлов и произвести их анализ.

Для операционных систем типа UNIX существует стандарт "syslog" отправки сообщений о происходящих в системе событиях (журналах), который использует протоколы TCP/IP. Протокол syslog достаточно прост: отправитель посылает короткое текстовое сообщение размером меньше 1024 байт получателю сообщения. Получатель при этом носит имя «syslogd», «syslog daemon», либо же, «syslog server». Сообщения могут отправляться как по протоколам UDP, так и по протоколам TCP. Как правило, такое сообщение отсылается в открытом виде. Протокол и соответствующая сетевая служба syslog используются для удобства администрирования и обеспечения информационной безопасности. Они реализованы под множество платформ и используются во множестве аппа-

ратных устройств. Использование syslog позволяет намного облегчить сбор журнальной информации от различных подсистем. Журнальные файлы почтового сервера (наиболее распространенным является "sendmail"), как правило, ведутся с помощью системы syslog.

Вместе с файлами системы syslog следует изучать журнальные файлы веб-сервера (как правило, это веб-сервер типа "apache"). Для того чтобы выяснить наличие и месторасположение самого веб-сервера, необходимо выяснить его название (получив листинг работающих программ, например, с помощью команды "ps"):

```
  PID  TT  STAT      TIME COMMAND
52166  ??  SJ     0:01.57 dovecot-auth
52167  ??  IJ     0:00.01 pop3-login
52168  ??  IJ     0:00.01 imap-login
61966  ??  SsJ    0:07.22 /usr/sbin/syslogd -ss
61972  ??  IsJ    0:39.86 /usr/local/sbin/named -u root -c ...
62048  ??  SsJ    1:21.03 /usr/local/sbin/httpd -DSSL
62075  ??  IJ     0:02.94 /usr/local/sbin/httpd -DSSL
62078  ??  IJ     0:00.01 /bin/sh /usr/local/bin/mysqld_safe --
defaults...
```

В листинге выше подчеркнут вариант названия веб-сервера ("httpd"), найденный в листинге. Затем следует проверить несколько возможных вариантов размещения конфигурационных файлов программы веб-сервера – это могут быть каталоги "/usr/local/www", "/usr/apache", "/usr/local/etc/apache" для операционной системы FreeBSD или "/var/www" для операционной системы Linux.

Оставленный в журнальных файлах информационный след представляет собой запись, содержащую информацию о сетевом адресе, локальном времени формирования записи, запрошенных данных и т.п. параметрах, характеризующих действия пользователя, обратившегося к веб серверу ресурса:

```
123.165.123.164 - - [08/Oct/2008:14:41:45 +0300] "GET /forum/ HTTP/1.1"
200 1458 "http://www.google.com.tr/search?ndsp=20&um=1&hl=tr&q=&ie=UTF-
8&sa=N&tab=iw" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
```

Значение 123.165.123.164 представляет адрес пользовательского компьютера, пославшего запрос в 14 часов 41 минуту 45 сек. 8 октября 2008 года на получение страницы с веб-адресом "http://ИМЯВЕБРЕСУРСА/forum/". При этом пользователь не набирал этот веб адрес в адресной строке браузера, а указал его при переходе со страницы на веб-ресурсе "www.google.com.tr" – турецком шлюзе поисковой системы Google.

Таким образом, данная запись свидетельствует о том, что пользователь осуществлял поиск по определенным ключевым словам, описывающим анализируемый веб-ресурс и, следовательно, занимался целенаправленным поиском информации определенного рода.

Следует отметить, что журнальные файлы обычно формируются в простом текстовом формате, не имеют каких-либо служебных пометок и сохраняются "как есть", без проверки предыдущих записей и контрольных сумм. Все это позволяет с легкостью имитировать несуществующие записи, удалять и изменять уже существующие.

В журнале почтового сервера аналогичный пример записей выглядит приблизительно так:

```
May 25 09:45:55 www sm-mta[9037]: n4P8jsua009037:
from=<teinb@questdiagnostics.com>, size=3824, class=0, nrcpts=3,
```

```
msgid=<000d01c9dd15$3322f330$6400a8c0@teinb>, proto=ESMTP, daemon=IPv4,
relay=[92.84.125.102]
May 25 09:45:55 www sm-mta[9059]: n4P8jsua009037:
to=\\virtuser_1002,\\virtuser_1003,\\virtuser_1001, delay=00:00:00, xde-
lay=00:00:00, mailer=local, pri=94018, relay=local, dsn=2.0.0, stat=Sent
May 25 10:04:35 www sm-mta[38980]: n4P94Xk1038980:
from=<ebkwoyfbgrqn@borderlinks.com>, size=4236, class=0, nrcpts=3,
msgid=<000d01c9dd17$c4e925d0$6400a8c0@ebkwoyfbgrqn>, proto=ESMTP, dae-
mon=IPv4, relay=[86.58.65.5]
```

В листинге выше показан пример журнальных записей, в которых указывается на получение писем электронной почты пользователями virtuser_1001, virtuser_1002 и virtuser_1003 от абонента "teinb@questdiagnostics.com", датированной 25 мая текущего года, в 9 часов 45 минут.

Важно также изучить конфигурационные настройки средств работы с журнальными файлами – зачастую системные утилиты осуществляют так называемую "ротацию" журнальных файлов. Ротация означает удаление файлов, период существования которых больше, чем заданный временной промежуток (как правило, 24 часа). Устаревшие файлы сначала архивируются, а по истечении еще одного заданного промежутка времени, удаляются навсегда из системы.

Алгоритм фиксации информационных следов. На сегодняшний день существует множество специальных программ, которые позволяют следить за неизменностью файлов данных на рабочих станциях и серверах. Однако специфика формирования журнальных файлов не позволяет использовать данное программное обеспечение, поскольку содержимое журнальных файлов и такие характеристики, как время создания, модификации и доступа, размер и атрибуты безопасности, являются динамическими для журнальных файлов.

По этой причине актуальна задача фиксации информационных следов таким образом, чтобы зафиксированные информационные следы отвечали следующим требованиям:

– должны фиксироваться не только параметры, описывающие объект информационного следа, но и ;

– должны фиксироваться контрольные суммы различных значимых фрагментов файлов, а не только всего файла (например, для текстового журнала – каждой строки, чтобы в дальнейшем можно было обеспечить поиск измененных данных);

– средства фиксации не должны изменять значения фиксируемых параметров (не должны изменяться сами файлы, атрибуты безопасности, временные характеристики – насколько это возможно в условиях существующих ограничений);

– должна приниматься во внимание универсальность информационного объекта для фиксации (журнальные файлы могут быть не только текстовыми, но и бинарными, графическими и т.п.).

Таким образом, алгоритм фиксации информационных следов можно определить как последовательность следующих шагов:

1. В случае, если интересны информационные следы для конкретного пользователя, то выполнить следующие действия:

а) определить время входа в систему и время выхода из системы пользователя под своей учетной записью;

б) выявить все объекты, созданные, модифицированные, удаленные (там, где это возможно) во время работы пользователя под своей учетной записью;

в) исключить из этого перечня записи, сделанные системой автоматически и без участия пользователя − прямого или косвенного;

г) использовать копирование и расчет контрольных сумм для этих файлов, согласно требованиям, указанным выше.

2. В противном случае, когда область поиска информационных следов распространена на весь веб-ресурс, следует выполнить следующие действия:

а) определить места журналирования различных системных и прикладных событий, сетевых процессов, выяснить не используется ли дополнительное специальное программное обеспечение журналирования, которое может способствовать идентификации информационных следов;

б) зафиксировать сами журналы, используя копирование и расчет контрольных сумм для этих файлов, согласно требованиям, указанным выше;

в) проанализировать с помощью материалов журнальных записей причастность отдельных пользователей к совершенным действиям.

Заключение. В работе введено понятие "информационного следа", отличающееся от других значений тем, что в качестве определяющего фактора используется журнальная запись, сделанная на компьютерной технике подозреваемых в преступлении лиц с помощью специального программного средства. Рассмотрен общий алгоритм фиксации информационных следов и особенности его технической реализации. Представленный алгоритм и анализ особенностей его применения позволяет ограничить область технических задач, возникающих при построении и эксплуатации систем защиты информации. Кроме того, в работе представлен способ анализа журнальных файлов веб-серверов и систем электронной почты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Зима В.М., Молдовян А.А., Молдовян Н.А*. Безопасность глобальных сетевых технологий. – СПб.: БХВ-Петербург, 2000. − 380 с.

2. *Климовский А.А*. К анализу подходов классификации компьютерных атак // Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. – М.:МЦНМО, 2006. – С.114-116.

3. Криминология: Учебник/под ред. проф. Малкова В.Д. – М: ЗАО Юстицинформ, 2004. − 277 с.

4. *Крылов И.Ф*. Криминалистическое учение о следах. СПб.: Изд-во Ленинградского университета, 1976. − 120 с.

5. *Щербаков А.Ю. и др*. Программирование алгоритмов защиты информации, М: Нолидж, 2002. − 240 с.

Борисов Владимир Владимирович
Федеральное государственное научное учреждение Научно-исследовательский институт «СПЕЦВУЗАВТОМАТИКА».
E-mail: borisovjojoba@gmail.com
414025, Астрахань, Татищева ул., 16. Тел: 8863 241-12-28

Borisov Vladimir Vladimirovich
Ministry of education and science of Russian Federation "SPETSVUZATOMATIKA"
E-mail: borisovjojoba@gmail.com
16, Tatisheva, Astrakhan, 414025 .Phone: 8863 241-12-28