

# Компьютерная контркриминалистика: состояние и перспективы

Суханов Максим

Group-IB (<http://group-ib.ru>)

Проект «Контр-форензика» (<http://anti-forensics.ru>)

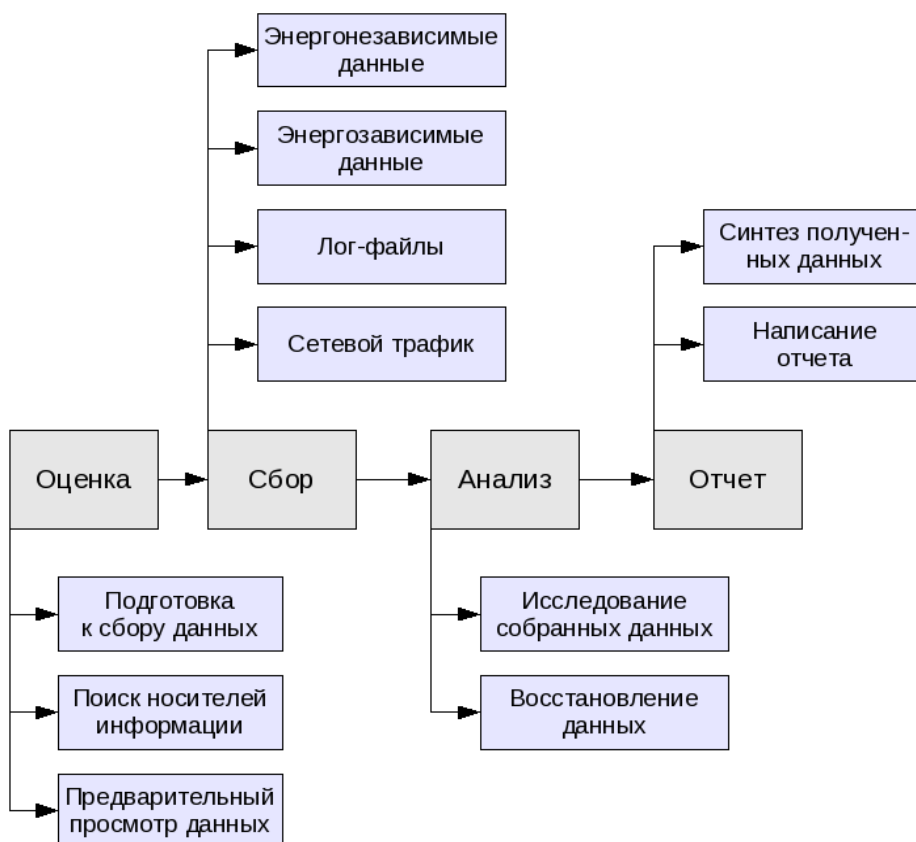
## Введение

Компьютерная контркриминалистика — противодействие методам поиска, обнаружения и закрепления доказательств в виде компьютерной информации. Иными словами, компьютерная контркриминалистика — дисциплина, направленная на противодействие расследованию компьютерных инцидентов и преступлений, а также на противодействие проведению криминалистических исследований и экспертиз компьютерной информации.

Данная статья написана с целью рассмотрения общих и некоторых перспективных методов и средств противодействия криминалистическим исследованиям компьютерной информации.

## Расследование инцидентов

Для начала следует детально рассмотреть процесс расследования инцидентов информационной безопасности. В общем случае он выглядит следующим образом:



### Стадия №1: оценка

На данном этапе происходит подготовка к сбору данных, имеющих отношение к

инциденту информационной безопасности, т. е. исследуется возможность проведения расследования (получается разрешение на проведение расследования, анализируются применимые политики и законы); определяется состав группы, которая будет проводить расследование; изучается топология сети, в которой произошел инцидент; определяются источники криминалистически значимой информации и т. д.

Кроме того, на этапе оценки определяется круг компьютерных носителей информации, имеющих отношение к инциденту. Для этого может производиться предварительный просмотр интересующих носителей информации, который заключается в проведении экспресс-исследования с целью ответа на следующие вопросы:

- Имеет ли данный компьютерный носитель информации отношение к инциденту?
- Имеются ли на данном компьютерном носителе информации сведения о других носителях или компьютерах, которые могут иметь отношение к инциденту?

## **Стадия №2: сбор**

На этой стадии собираются все данные, имеющие отношение к инциденту. Они включают в себя:

- Содержимое энергонезависимых носителей информации (жесткие диски, компакт-диски, накопители USB Flash и т. п.);
- Содержимое энергозависимых носителей информации (оперативная память);
- Лог-файлы сетевого оборудования, серверов;
- Сетевой трафик.

Сбор вышеперечисленных данных заключается в создании их копии специализированными средствами.

### *Содержимое энергонезависимых носителей информации*

Перед созданием копии энергонезависимого носителя информации необходимо обеспечить целостность (неизменность) его содержимого, для чего применяются программные и аппаратные блокираторы записи, а также специализированные операционные системы. Если компьютер, в котором установлен носитель информации, который нужно скопировать (или изъять), работает, то его работа завершается прерыванием электропитания (реже: средствами работающей системы, например, командой *poweroff*) после сбора энергозависимых данных, либо сразу, если энергозависимые данные собирать не надо; в особых случаях (например, при невозможности отключения критически важных серверов) допустимо копировать энергонезависимые данные с работающей системы.

Блокираторы записи позволяют подключить исследуемый носитель информации без риска записи на него каких-либо данных по вине операционной системы или сторонних программ.

В операционных системах Windows (Windows XP SP2 и более поздние версии) для блокировки записи на USB-носители можно использовать встроенные системные средства, которые активируются после изменения соответствующего ключа реестра<sup>1</sup>. Для блокировки записи на другие виды носителей информации в Windows нужно использовать стороннее программное обеспечение, например, SAFE Block (<http://www.forensicsoft.com/safeblock.php>). В операционных системах Linux для блокирования записи в процессе монтирования файловых систем следует использовать опции монтирования «ro,loop».

Аппаратные блокираторы записи выполняют свои функции вне зависимости от

1 См. [http://www.accessdata.com/media/en\\_us/print/papers/wp.USB\\_Write\\_Protect.en\\_us.pdf](http://www.accessdata.com/media/en_us/print/papers/wp.USB_Write_Protect.en_us.pdf)

применяемых для чтения данных операционных систем и программ. Примеры аппаратных блокираторов записи: продукты класса «forensic bridges» компании Tableau ([http://www.tableau.com/index.php?pageid=products&category=forensic\\_bridges](http://www.tableau.com/index.php?pageid=products&category=forensic_bridges)).

Специализированные операционные системы, как правило, применяются для копирования носителей информации без их извлечения из исследуемого компьютера за счет загрузки на его аппаратном обеспечении доверенной (криминалистической) программной среды. Обычно такие операционные системы загружаются с CD или накопителей USB Flash и включают в себя программные блокираторы записи, запускаемые в процессе загрузки. Примеры таких операционных систем:

- grml (<http://grml.org/>);
- CAINE Live CD (<http://www.caine-live.net/>);
- DEFT Linux (<http://www.deflinux.net/>);
- e-fense Helix3 Pro (<http://www.e-fense.com/helix3pro.php>).

Для непосредственного копирования данных могут применяться следующие программы:

- dd (входит в состав почти всех дистрибутивов Linux);
- dc3dd — модифицированная версия dd (<http://dc3dd.sourceforge.net/>);
- aimage (<http://afflib.org/>);
- FTK Imager (<http://accessdata.com/downloads.html>).

Кроме того, для копирования содержимого носителей информации могут использоваться аппаратные средства. Например:

- Tableau TD1 Forensic SATA/IDE Duplicator (<http://www.tableau.com/index.php?pageid=products&category=duplicators>);
- VOOМ HardCopy 3 (<http://www.voomtech.com/hc3.html>).

Следует отметить, что копирование содержимого энергонезависимых носителей информации перед исследованием не является обязательным шагом — в случаях, когда обеспечивается целостность содержимого оригинальных носителей (т. е. в случаях исправности носителей и при использовании блокираторов записи), исследование копий вместо оригиналов проводить нецелесообразно.

#### *Содержимое энергозависимых носителей информации*

Сбор энергозависимых данных производится с работающих систем перед их выключением. Как правило, процесс сбора энергозависимых данных заключается в копировании:

1. Содержимого оперативной памяти компьютера;
2. Содержимого примонтированных зашифрованных файловых систем и сетевых хранилищ;
3. Списков работающих процессов и сервисов;
4. Списков текущих сетевых соединений и открытых портов;
5. Сетевой конфигурации исследуемой системы;
6. Переменных окружения;
7. Изображения, которое видит пользователь на экране монитора (создание снимка экрана).

Для копирования этих данных к работающей исследуемой системе может подключаться внешний носитель, с которого производится запуск специализированной программы, собирающей данные. Иногда специализированная программа загружается в систему по сети. Скопированные данные могут сохраняться на внешний носитель или передаваться по сети на доверенный сервер.

Примеры программ, предназначенных для сбора энергозависимых данных:

- X-Ways Capture (<http://www.x-ways.net/capture/index-m.html>);
- EnCase FIM ([http://guidancesoftware.ru/EnCase\\_FIM/EnCase\\_FIM.html](http://guidancesoftware.ru/EnCase_FIM/EnCase_FIM.html));
- e-fense Helix3 Pro (<http://www.e-fense.com/helix3pro.php>);
- e-fense Live Response (<http://www.e-fense.com/live-response.php>);
- Microsoft COFEE;
- MoonSols Windows Memory Toolkit (<http://moonsols.com/product>).

В перспективе возможно использование для копирования оперативной памяти исследуемого компьютера аппаратных средств (с помощью устройств, подключаемых к шине PCI до инцидента<sup>2</sup>, или с помощью FireWire-устройств<sup>3</sup>, также возможен перенос охлажденных модулей памяти на другой компьютер с минимальной потерей энергозависимых данных<sup>4</sup>).

#### *Лог-файлы*

Копирование логов может производиться несколькими способами:

- Копированием только записей, имеющих отношение к инциденту (например, относящихся к определенному IP-адресу или промежутку времени);
- Копированием лог-файлов целиком;
- Копированием всего носителя информации.

Основными факторами при выборе того или иного способа копирования являются: степень доверия логам и, соответственно, объем исследования, направленного на определение степени корректности и неизменности лог-файлов. Если вероятность злонамеренного изменения или фальсификации лог-файлов мала, то допустимо копировать только лог-файлы или отдельные их записи. В противном случае целесообразно копировать содержимое всего носителя информации (для дальнейшего поиска следов несанкционированного доступа к системе, следов модификации лог-файлов и т. д.).

#### *Сетевой трафик*

Для создания копии (дампа) сетевых пакетов могут применяться следующие программы:

- *tcpdump* (<http://www.tcpdump.org/>);
- *Wireshark* (<http://www.wireshark.org/>).

При этом необходимо организовать подключение точки съема сетевого трафика в участке сети, который обеспечивает сбор всех криминалистически значимых потоков данных. В процессе создания дампа сетевых пакетов необходимо минимизировать обмен данными между узлом, который производит съем сетевого трафика, и узлами сети, которые имеют отношение к инциденту информационной безопасности.

2 См. <http://digital-evidence.org/papers/tribble-preprint.pdf>

3 См. [http://www.storm.net.nz/static/files/ab\\_firewire\\_rux2k6-final.pdf](http://www.storm.net.nz/static/files/ab_firewire_rux2k6-final.pdf) и <http://www.lostpassword.com/hdd-decryption.htm#imager>

4 См. <http://www.usenix.org/events/sec08/tech/halderman.html>

### Стадия №3: анализ

На этом этапе производится анализ всех собранных данных, который может проводиться по следующему алгоритму:

- Получение общих сведений об исследуемом объекте (диске, копии диска, дампе сетевого трафика и т. п.);
- Исследование данных в явном виде;
- Исследование данных в неявном (удаленном, скрытом, зашифрованном) виде.

Исследование энергонезависимых носителей информации и их копий в большинстве случаев заключается в исследовании содержимого файловых систем и в восстановлении данных. Криминалистическое исследование файловых систем заключается в анализе различного рода информационных следов, возникающих в результате действий злоумышленника, работы программного и аппаратного обеспечения исследуемой системы. Количество таких следов (как источников криминалистически значимой информации) в файловых системах велико (от временных меток создания, изменения, открытия файлов и фрагментов виртуальной памяти в файлах подкачки до MAC-адресов, записанных в ярлыках Windows), в связи с чем отсутствуют какие-либо исчерпывающие методики и алгоритмы проведения криминалистических исследований файловых систем при расследовании инцидентов.

Для криминалистического исследования файловых систем могут применяться следующие программные продукты:

- EnCase Forensic ([http://guidancesoftware.ru/EnCase\\_Forensic/EnCase\\_Forensic.html](http://guidancesoftware.ru/EnCase_Forensic/EnCase_Forensic.html));
- Forensic Toolkit (<http://accessdata.com/forensictoolkit.html>);
- The Sleuth Kit (<http://sleuthkit.org/>).

Для восстановления данных могут применяться следующие программы:

- foremost (<http://foremost.sourceforge.net/>);
- PhotoRec (<http://www.cgsecurity.org/wiki/PhotoRec>).

Анализ копий оперативной памяти заключается в воссоздании структур данных, которые различные операционные системы хранят в памяти. Для этого могут применяться следующие программные продукты:

- The Volatility Framework (<https://www.volatilesystems.com/default/volatility>);
- HBGary Responder Field Edition (<https://www.hbgary.com/products-services/responder-field-edition/>).

Данные программы позволяют извлекать из копий оперативной памяти большое количество криминалистически значимой информации, например: списки работающих процессов, списки открытых сетевых сокетов, списки активных сетевых соединений, списки загруженных модулей ядра.

Анализ дампов сетевых пакетов может использоваться:

1. Для определения характеристик сетевых пакетов и соединений (например, с целью поиска скрытых каналов передачи данных);
2. Для извлечения сообщений, передаваемых по сети (например, с целью поиска каналов утечки информации).

В первом случае могут применяться анализаторы сетевых пакетов, например:

- Wireshark;
- NetworkMiner (<http://networkminer.sourceforge.net/>).

Во втором случае, как правило, используются не анализаторы сетевых пакетов, а системы легального перехвата, которые позволяют автоматизировать процессы поиска, выделения и сохранения сетевых сообщений различных типов (сообщений электронной почты, Интернет-пейджеров и т. д.), а также производить поиск по ключевым словам и другим критериям в перехваченных данных.

#### **Стадия №4: отчет**

На данной стадии производится синтез всей информации, полученной на этапе анализа, с последующим написанием отчета в форме, понятной аудитории, для которой он предназначен. Отчет может включать в себя:

- Сведения о причинах возникновения инцидента;
- Сведения о лицах, причастных к инциденту;
- Хронологию инцидента;
- Детальное описание следов (доказательств), обнаруженных на этапе анализа;
- Сведения об использованных в процессе расследования методиках, программных и аппаратных средствах, обстоятельствах их применения;
- Рекомендации по предотвращению подобных инцидентов в будущем.

#### **Применимость в других областях**

Вышеприведенная схема расследования инцидентов информационной безопасности применима (с некоторыми ограничениями) и для других областей, например: судебные компьютерные и компьютерно-технические экспертизы (в этих случаях стадия оценки в представленном виде отсутствует, стадия сбора включает в себя работу *только* с представленными на экспертизу объектами<sup>5</sup>, а вместо отчета составляется заключение эксперта).

#### **Противодействие расследованию инцидентов**

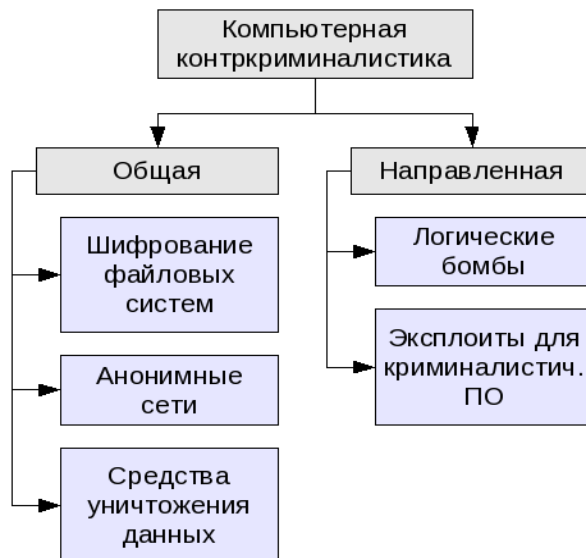
На любом этапе расследования инцидентов информационной безопасности можно встретить противодействие со стороны злоумышленника. Данное противодействие бывает двух видов: общее и направленное.

Общее противодействие не направлено на конкретный метод или конкретное средство криминалистического исследования и, как правило, реализуется средствами двойного назначения (например, программами для создания зашифрованных файловых систем или программами для шифрования сетевого трафика). Основная задача данного вида противодействия: защитить данные от криминалистического исследования путем их уничтожения, шифрования или сокрытия.

Направленное противодействие заключается в компрометации или обмане определенного криминалистического средства. Основные задачи этого вида противодействия: защитить данные от криминалистического исследования путем их уничтожения, сокрытия или

<sup>5</sup> Энергонезависимыми носителями информации и их копиями, а также копиями энергозависимых данных, сетевых пакетов и лог-файлов.

подмены; показать ненадежность криминалистических методов и средств с целью их компрометации в суде<sup>6</sup>. Другой задачей направленного противодействия может являться проникновение в сеть организации, занимающейся расследованием инцидента, с последующей компрометацией конфиденциальной информации различного рода (для этого могут использоваться уязвимости в программном обеспечении, приводящие к выполнению произвольного кода).



Наиболее популярными являются методы и средства общего противодействия, т. к. направленное противодействие расследованию инцидентов остается малоизученной областью информационной безопасности.

### Общие методы противодействия расследованию инцидентов

Наиболее популярными методами общего противодействия являются:

1. Защита данных на энергонезависимых носителях информации шифрованием, стеганографическим сокрытием или уничтожением (перезаписью).

Примеры программ для шифрования файловых систем:

- TrueCrypt (<http://www.truecrypt.org/>);
- DiskCryptor (<http://diskcryptor.net/>).

Для сокрытия данных может использоваться отрицаемое шифрование — особый метод компоновки зашифрованных данных, обеспечивающий правдоподобное отрицание их наличия (<http://www.truecrypt.org/docs/?s=hidden-volume>).

Примеры программ для перезаписи данных:

- Eraser (<http://eraser.heidi.ie/>);
- DBAN (<http://www.dban.org/>).

2. Защита данных, передаваемых по сети: шифрование и анонимизация сетевого трафика.

Примеры программ для шифрования сетевого трафика:

- The Onion Router (<https://www.torproject.org/>);

<sup>6</sup> Сценарии компрометации судебных программ описаны здесь: [https://www.isecpartners.com/files/Ridder-Evidentiary\\_Implications\\_of\\_Security\\_Weaknesses\\_in\\_Forensic\\_Software.pdf](https://www.isecpartners.com/files/Ridder-Evidentiary_Implications_of_Security_Weaknesses_in_Forensic_Software.pdf)

- OpenVPN (<http://www.openvpn.net/>) и другие реализации технологии виртуальных частных сетей.

Кроме того, в настоящее время набирают популярность методы противодействия, основанные на предотвращении создания криминалистически значимых данных: вредоносные программы, работающие только в оперативной памяти; загрузочные диски и виртуальные машины, направленные на обеспечение конфиденциальности (отсутствие следов работы пользователя) при работе с компьютером.

Данные методы и соответствующие программные средства в большинстве случаев разрабатываются с целью защиты конфиденциальной информации или поддержки свободы слова, но это не исключает их использование злоумышленниками в целях сокрытия или уничтожения доказательств в виде компьютерной информации и противодействия расследованию компьютерных преступлений.

Применение вышеуказанных методов является серьезным препятствием раскрытию компьютерных преступлений, однако существует ряд криминалистических методик, направленных на поиск скрытых данных (в том числе скрытых с применением отрицаемого шифрования), восстановление данных после попыток их перезаписи и извлечение данных из зашифрованных файловых систем. Возможность успешного противодействия общим контркриминалистическим методам заключается в плохой оценке их эффективности в среде злоумышленников. К примеру, для оценки эффективности применения средств дискового шифрования, как правило, используются только критерии надежности выбранного криптографического алгоритма и его реализации, иные критерии (физическая безопасность компьютера, безопасность программного окружения, особенности аппаратного и программного окружения, возможность работы с другими источниками информации в процессе расследования) полностью не используются<sup>7</sup>.

### **Направленные методы противодействия расследованию инцидентов**

Методы направленного противодействия используются для обнаружения и уничтожения (сокрытия, подмены) криминалистически значимых данных. Обнаружение криминалистического исследования носителей информации может быть реализовано различными способами: анализом сетевого трафика с целью поиска признаков работы сетевых криминалистических средств, анализом работающих программ на предположительно исследуемой системе и т. д. Уничтожение, сокрытие или подмена исследуемых данных реализуется либо применением логических бомб, либо применением эксплоитов для криминалистического программного обеспечения (эти средства могут использовать как ошибки программ, так и ошибки эксперта-криминалиста — нарушение методик исследования компьютерной информации). Для направленного противодействия расследованию инцидентов можно составить следующую цепочку «слабых мест» криминалистического исследования:

*метод — средство — действия*

Метод — совокупность приемов, используемых при исследовании компьютерной информации. Пример: загрузка криминалистической операционной системы с подключенным исследуемым носителем информации без применения аппаратной блокировки записи (например, с целью создания копии носителя информации).

Средство — программное или аппаратное обеспечение, применяемое на определенном этапе криминалистического исследования компьютерной информации. Пример: криминалистический Live CD grml.

Действия — последовательность операций, направленных на достижение результата для

<sup>7</sup> См. пример обсуждения: <http://fuckav.ru/showthread.php?t=4296>

конкретного этапа криминалистического исследования. Примеры: запуск программы для клонирования данных (результат: успешное копирование содержимого диска), запуск программы для индексирования данных (результат: возможность быстрого поиска информации по ключевым словам).

Для приведенной цепочки «слабых мест» можно выделить следующие методы направленного противодействия:

1. Противодействие с помощью аппаратных «закладок»: обнаружение признаков криминалистического исследования и подмена (сокрытие, уничтожение) данных аппаратными средствами;
2. Противодействие программными средствами (с помощью логических бомб и эксплоитов для криминалистических продуктов): активация логических бомб при нарушении методик проведения криминалистического исследования, эксплуатация ошибок различного класса в криминалистических программах;
3. Обнаружение факта проведения криминалистического исследования: обнаружение работающих криминалистических программ (как локально, так и в сети).

Кроме того, к этому пункту можно отнести методы поиска признаков выполнения кода в контролируемой среде, используемые некоторыми вредоносными программами: исследование идентификаторов подключенного оборудования (для обнаружения виртуальной машины), поиск запущенных отладчиков программ, анализ файловой активности пользователя (для обнаружения виртуальной машины или компьютера-«песочницы») и т. п.

### **Аппаратные «закладки»**

Наиболее универсальными с точки зрения противодействия широкому спектру криминалистических методов и средств являются аппаратные «закладки».

К примеру, применение «закладок», направленных на обнаружение признаков проведения криминалистического исследования с последующим уничтожением данных, встроенных в носители информации (например, в контроллеры жестких дисков) позволит успешно защитить данные от исследования с применением программных и аппаратных блокираторов записи, криминалистических Live CD. В качестве признака криминалистического исследования может выступать факт последовательного чтения секторов носителя информации (например, в процессе копирования данных программой *dd*) без отправки на него каких-либо команд записи. При обнаружении последовательного считывания данных и потенциальной блокировки записи, контроллер может инициировать уничтожение или сокрытие содержимого жесткого диска. К счастью, данный метод противодействия является перспективным, т. к. сегодня отсутствуют какие-либо работы, направленные на исследование и оценку эффективности его применения, но появление подобных аппаратных устройств-«закладок» должно полностью изменить современные криминалистические методы исследования носителей информации, которые базируются на доверии к аппаратной составляющей исследуемых накопителей.

Другим примером являются системы аппаратного уничтожения данных, срабатывающие при несанкционированном открытии крышки корпуса компьютера, извлечении жесткого диска или при нажатии «тревожной кнопки» и способные работать от батареи автономного электропитания в течение длительного времени<sup>8</sup>.

Кроме того, возможно противодействие созданию копий содержимого оперативной памяти с помощью аппаратных устройств, которое заключается в подмене участков памяти,

---

8 Пример подобного средства: <http://www.nero.ru/catalog30.html>

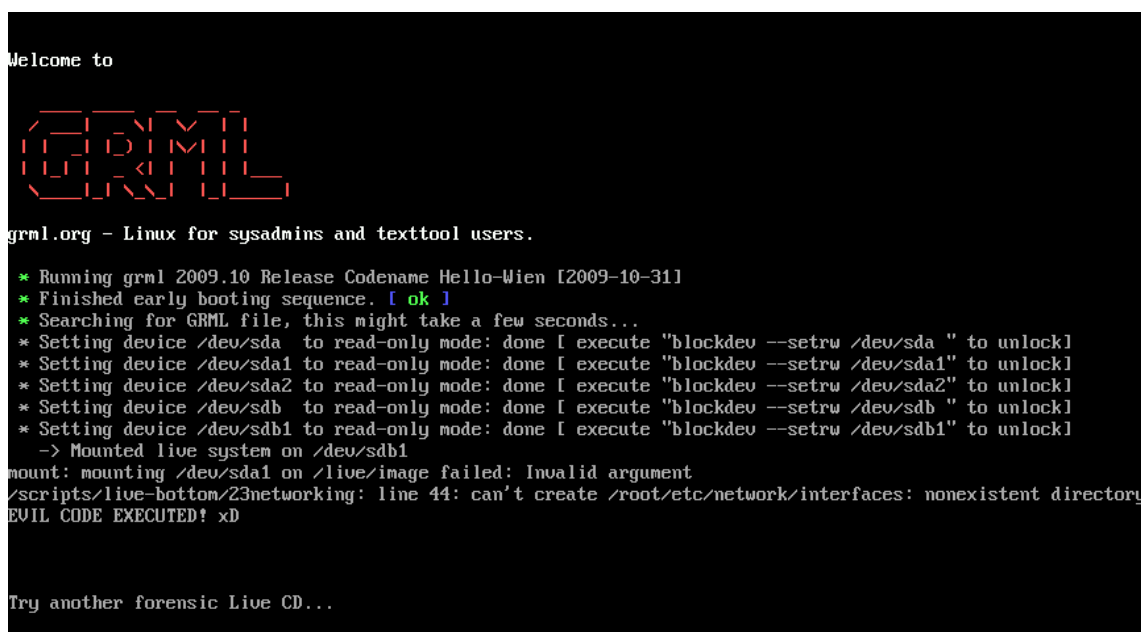
считываемых устройствами PCI и FireWire в системах с процессорами AMD<sup>9</sup>.

### Программные «закладки»

До недавнего времени программные «закладки» были эффективны только в случаях использования для исследования компьютерной информации недопустимых методов — например, при включении исследуемого компьютера с оригинальным носителем информации без использования блокировки записи<sup>10</sup> или при запуске исследуемых программ и скриптов на стендовом компьютере (т. е. на компьютере, с использованием которого производится исследование). Сегодня программное противодействие исследованию компьютерной информации фокусируется не только на методах, нарушающих рекомендации по исследованию компьютерных носителей информации, но и на конкретных средствах криминалистического исследования (которые используются для криминалистически правильной работы с исследуемой компьютерной информацией).

Наибольшую опасность криминалистическому исследованию представляют уязвимости «нулевого дня» в специализированном программном обеспечении (криминалистические Live CD, программы для исследования файловых систем, программы для обработки дампов сетевых пакетов и др.) и программном обеспечении «общего назначения» (программы для просмотра файлов различных форматов и т. д.). В частности, в программном обеспечении EnCase Forensic и Forensic Toolkit были найдены уязвимости обработки некоторых форматов файлов, приводящие к выполнению произвольного кода<sup>11</sup>, а в программе FTK Imager была найдена «особенность», позволяющая использовать уязвимости браузера Internet Explorer для противодействия предварительному просмотру исследуемых данных<sup>12</sup>.

Другим вектором атаки является выполнение произвольного кода, записанного на исследуемых носителях информации, в большинстве существующих криминалистических Live CD на основе Ubuntu, KNOPPIX и Debian из-за особенностей процесса поиска корневой файловой системы на стадии загрузки (отсутствует проверка подлинности выбранной в качестве корневой файловой системы)<sup>13</sup>.



```
Welcome to
GRML
grml.org - Linux for sysadmins and texttool users.
* Running grml 2009.10 Release Codename Hello-Wien [2009-10-31]
* Finished early booting sequence. [ ok ]
* Searching for GRML file, this might take a few seconds...
* Setting device /dev/sda to read-only mode: done [ execute "blockdev --setrw /dev/sda " to unlock]
* Setting device /dev/sda1 to read-only mode: done [ execute "blockdev --setrw /dev/sda1" to unlock]
* Setting device /dev/sda2 to read-only mode: done [ execute "blockdev --setrw /dev/sda2" to unlock]
* Setting device /dev/sdb to read-only mode: done [ execute "blockdev --setrw /dev/sdb " to unlock]
* Setting device /dev/sdb1 to read-only mode: done [ execute "blockdev --setrw /dev/sdb1" to unlock]
-> Mounted live system on /dev/sdb1
mount: mounting /dev/sda1 on /live/image failed: Invalid argument
/scripts/live-bottom/23networking: line 44: can't create /root/etc/network/interfaces: nonexistent directory
EVIL CODE EXECUTED! xD

Try another forensic Live CD...
```

*Выполнение произвольного кода в криминалистическом Live CD grml 2009.10*

9 См. <http://www.blackhat.com/presentations/bh-dc-07/Rutkowska/Presentation/bh-dc-07-Rutkowska-up.pdf>

10 Пример логической бомбы: <http://www.google.com/search?q=пищем+антиомон>

11 См. обсуждение: <http://blogs.sans.org/computer-forensics/2010/04/27/arbitrary-code-execution-examiner-systems-file-corruption/>

12 См. [http://intotheboxes.files.wordpress.com/2010/04/intotheboxes\\_2010\\_q1.pdf](http://intotheboxes.files.wordpress.com/2010/04/intotheboxes_2010_q1.pdf)

13 См. <http://computer-forensics-lab.org/lib/?cid=175>

## Обнаружение факта проведения криминалистического исследования

Раскрытие факта проведения расследования инцидента информационной безопасности может иметь негативные последствия: уничтожение криминалистически значимых данных на носителях информации, которые не были определены на этапе оценки по каким-либо причинам; уничтожение информационных улик на других сетевых узлах и т. д.

Криминалистическое исследование жестких дисков может быть обнаружено путем регулярной сверки некоторых параметров SMART: копирование содержимого жесткого диска с использованием аппаратных средств, либо загрузочных криминалистических операционных систем приводит к изменению общего числа циклов включения-выключения питания, а также к изменению общего времени работы диска<sup>14</sup>. Подобные сведения могут использоваться для обнаружения фактов проведения скрытых криминалистических исследований.

1	Raw_Read_Error_Rate	0x000f	115	099	006	Pre-fail	Always
-	83976741						
3	Spin_Up_Time	0x0003	095	093	000	Pre-fail	Always
-	0						
4	<b>Start_Stop_Count</b>	<b>0x0032</b>	<b>100</b>	<b>100</b>	<b>020</b>	<b>Old_age</b>	<b>Always</b>
-	80						
5	Reallocated_Sector_Ct	0x0033	100	100	036	Pre-fail	Always
-	1						
7	Seek_Error_Rate	0x000f	075	060	030	Pre-fail	Always
-	12990803690						
9	<b>Power_On_Hours</b>	<b>0x0032</b>	<b>084</b>	<b>084</b>	<b>000</b>	<b>Old_age</b>	<b>Always</b>
-	14481						

*Фрагмент вывода программы smartctl для жесткого диска  
(количество циклов вкл.-выкл. питания: 80; общее время работы: 14481 часов)*

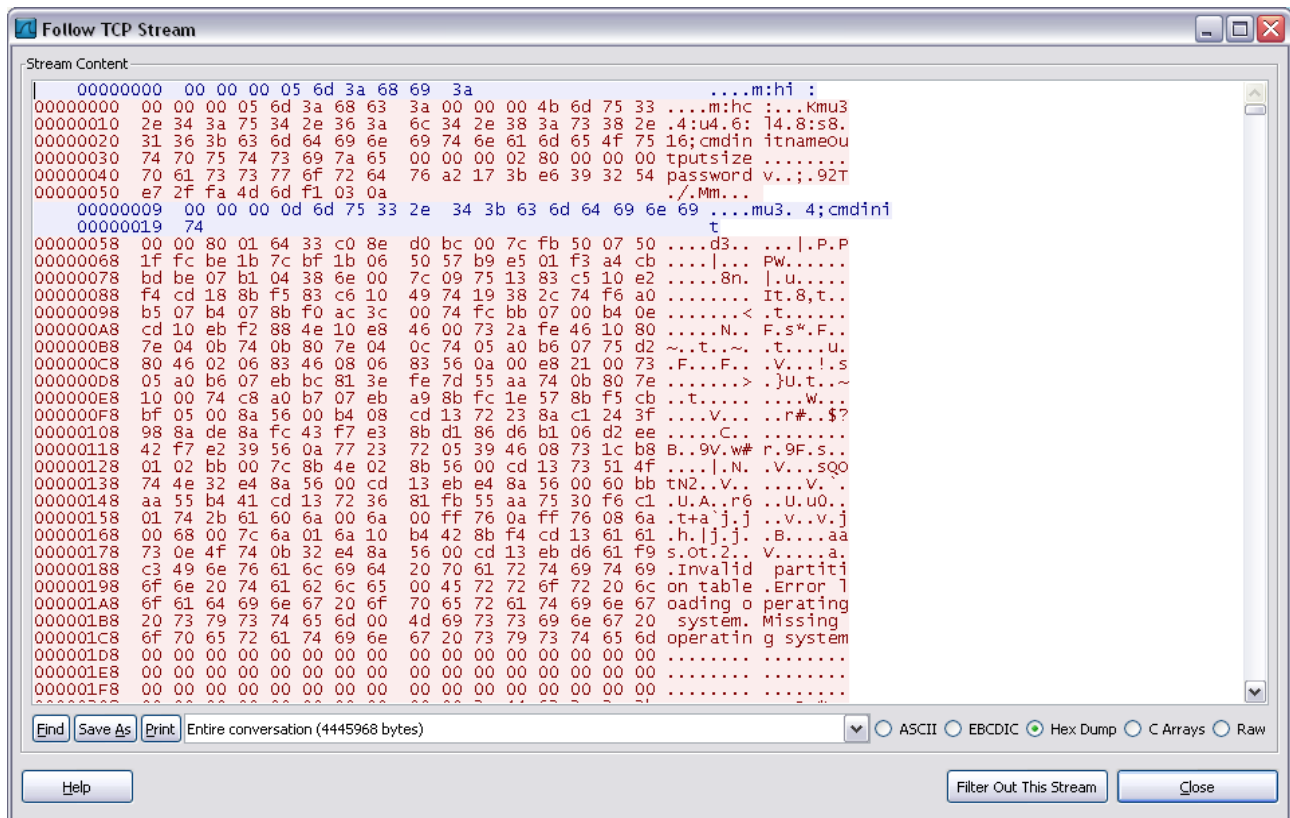
Кроме того, злоумышленники могут использовать документы, включающие в себя онлайн-содержимое, загрузка которого в процессе открытия файла при проведении криминалистического исследования позволит установить факт и место проведения расследования (если компьютер, с использованием которого производится исследование, не отключается от сети Интернет). В качестве таких файлов-«ловушек» могут выступать файлы формата ODF со встроенными фреймами.

Использование некоторых криминалистических средств может быть обнаружено с помощью пассивного или активного сканирования сетевых узлов, если в процессе исследования сетевое подключение компьютера не отключается (например, если копия содержимого жесткого диска передается по сети на доверенный узел). К таким средствам можно отнести большинство криминалистических Live CD на основе Linux, а также программное обеспечение, предназначенное для сбора данных по сети.

Загрузка большинства криминалистических Live CD на основе Linux приводит к автоматической активации сетевого подключения с последующей отправкой пакетов (пакетов поиска DHCP-сервера и т. п.). Данные пакеты обладают определенными свойствами, позволяющими отличить загружаемую на сетевом узле криминалистическую операционную систему, например: характером изменений значений IP ID пакетов DHCP (в операционных системах на основе Linux все идентификаторы таких пакетов равны нулю, в операционных системах Windows характер изменений инкрементальный) и начальными значениями IP TTL (так называемое «время жизни пакета»).

14 См. <http://www.forensicfocus.com/smart-anti-forensics>

Процесс передачи копий собранных данных по сети может быть обнаружен поиском специфических для криминалистических средств сетевых протоколов, поиском фрагментов собранных данных по каким-либо признакам (передаваемый образ диска может быть обнаружен по фрагментам загрузочного сектора и т. д.) и поиском «подозрительных» сетевых подключений.



### Специфичный для криминалистического CD Helix3 Pro 2009R2 протокол передачи незашифрованных образов дисков

Активное сетевое сканирование с целью обнаружения факта проведения криминалистического исследования может быть направлено на выявление интерфейсов взаимодействия криминалистических программ, к таким интерфейсам относятся:

- Интерфейсы удаленного управления криминалистической системой по протоколу SSH;
- Интерфейсы удаленного доступа к исследуемым дискам по протоколу iSCSI.

В криминалистическом дистрибутиве Helix3 Pro 2009R3 происходит автоматическая активация SSH-сервера (для доступа используется фиксированная, заданная разработчиком связка логин-пароль) и iSCSI-сервера в процессе загрузки, что делает возможным удаленное обнаружение факта проведения криминалистического исследования с применением данного программного продукта. Более того, использование для удаленного управления системой фиксированной связки логин-пароль (логин: «*helixclient*»; пароль: «*helix*») может привести к перехвату управления криминалистической системой со стороны злоумышленника (с последующим возможным уничтожением криминалистически значимых данных).

```
$ ssh -lhelixclient 192.168.56.101
helixclient@192.168.56.101's password: (пароль: helix)
Linux helix 2.6.28.9-helixpro #1 SMP Thu Jun 18 21:23:28 BST 2009 i686
```

The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/\*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

To access official Ubuntu documentation, please visit:  
<http://help.ubuntu.com/>

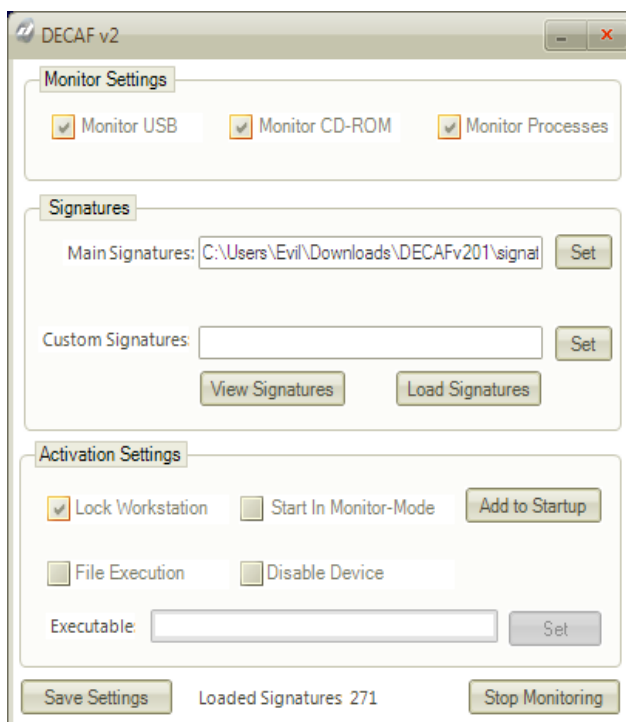
```
Last login: Sun Sep  5 19:39:29 2010 from 192.168.56.1
helixclient@helix:~$ su helix
Password: (пустой пароль)
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
helix@helix:/home/helixclient$ sudo su
root@helix:/home/helixclient# id
uid=0(root) gid=0(root) groups=0(root)
root@helix:/home/helixclient#
```

*Процесс получения root-доступа к загруженной операционной системе*

### *Helix3 Pro 2009R3*

Исследование работающих систем с сохранением собранных данных на локальный носитель информации может быть обнаружено путем наблюдения за запущенными процессами и подключаемыми накопителями (как средствами доставки криминалистической программы и хранилищами собранных данных). Для этих целей может использоваться программа DECAF (<http://decafme.org/>), которая при обнаружении криминалистических программ, предназначенных для сбора данных с работающих систем, производит заранее определенные действия: блокировку компьютера, запуск заданной программы и др.



*Окно программы DECAF v2*

## Заклучение

В данной статье были рассмотрены методы направленного противодействия криминалистическому исследованию компьютерной информации, представляющие серьезную угрозу существующим общепризнанным методикам проведения расследований компьютерных инцидентов.

Вероятность встретить направленное противодействие сегодня все еще мала, но не стоит забывать о высокотехнологичных противниках, которые могут использовать уязвимости в криминалистических программных продуктах с целью получения доступа к чувствительной информации команд по реагированию на инциденты информационной безопасности и организаций, расследующих компьютерные преступления, путем направления на исследование специально сформированных данных.

Автор надеется, что в ближайшее время разработчики будут уделять больше внимания обеспечению скрытности и безопасности применения криминалистических программных продуктов различных классов. Еще в 2007 году уязвимости в криминалистических программных продуктах, приводящие к выполнению произвольного кода, были теорией, а что будет завтра?

