УДК 681.3.06(075)

С.Д. Прокопенко,
С.Р. Коженевский

ОСОБЕННОСТИ СЪЕМА И ВОССТАНОВЛЕНИЯ ДАННЫХ НА СОВРЕМЕННЫХ ЦИФРОВЫХ ВИДЕОРЕГИСТРАТОРАХ ПРИ РАССЛЕДОВАНИИ ИНЦИДЕНТОВ

Статья посвящена съему и восстановлению данных на современных цифровых видеорегистраторах (DVR) при расследовании инцидентов. В работе приведены сведения о конструкции и принципах функционирования DVR, описаны проблемы получения доступа к видеозаписям. Проанализированы способы съема и восстановления информации с видеорегистраторов и их особенности. Также приведены практические рекомендации по организации съема данных с цифровых видеорегистраторов.

Ключевые слова: *цифровой видеорегистратор, DVR, съем данных, расследование IT инцидентов, восстановление информации, компьютерная криминалистика.*

Статтю присвячено зніманню та відновленню даних на сучасних цифрових відеореєстраторах (DVR) при розслідуванні інцидентів. У роботі наведено відомості про конструкцію та принципи функціонування DVR, описано проблеми отримання доступу до відеозаписів. Проаналізовано способи знімання та відновлення інформації з відеореєстраторів та їх особливості. Також наведено практичні рекомендації щодо організації знімання даних з цифрових відеореєстраторів.

Ключові слова: *цифровий відеореєстратор, DVR, знімання даних, розслідування IT інцидентів, відновлення інформації, комп'ютерна криміналістика.*

Paper considers forensic data acquisition and data recovery of modern digital video recorders. It gives an information about DVR design and operation, describes the problems of the accessing to video records. Methods of DVR data acquisition and data recovery as well as their characteristics are analyzed. Several practical advices, concerning the process of DVR forensic data acquisition, are suggested.

Keywords: *digital video recorder, DVR, data acquisition, computer forensics, data recovery, computer criminalistics.*

В настоящее время широкое распространение получили цифровые системы видеонаблюдения, центральным элементом которых являются цифровые видеорегистраторы (DVR, Digital Video Recorder). При возникновении того или иного инцидента данные с DVR могут служить важным источником информации в корпоративном или судебном расследовании. Однако кажущаяся на первый взгляд несложной задача съема данных с видеорегистратора влечет за собой ряд проблем, связанных с особенностями их построения и функционирования.

Принципы построения цифровых видеорегистраторов

Сегодня на рынке доступно большое количество цифровых видеорегистраторов. Они характеризуются тем, что видео- и аудиосигналы с камер наблюде-

ния и микрофонов сохраняются в цифровой форме на жестких дисках, иногда на флэш-накопителях (обычно применяются в портативных автомобильных регистра-торах). С точки зрения конструктивного исполнения современные DVR можно разделить на две группы.

Видеорегистраторы на базе ПК

Такие системы обычно работают под управлением ОС Windows или Linux, захват и обработка видео осуществляется с помощью специализированных плат видеозахвата и программного обеспечения. Основными преимуществами компьютерных регистраторов являются гибкость конфигурации, простота модернизации (наращивания емкости и количества каналов), удобный пользовательский интерфейс и сравнительно невысокая стоимость. К их недостаткам можно отнести относительно сложную установку и настройку, достаточно жесткие требования к аппаратной части ПК, возможность двойного использования ПК (что крайне нежелательно в системах видеонаблюдения), зависимость от надежности используемой ОС, большие размеры.

Для хранения данных подавляющее большинство компьютерных видеорегистраторов используют возможности поддерживаемых в ОС файловых систем (NTFS для Windows, Ext3 для Linux). Другими словами, видеозаписи сохраняются в виде файлов, доступ к которым можно получить с помощью традиционных средств операционной системы. Только очень небольшое количество моделей регистраторов требуют предварительной собственной разметки дисков, не используя традиционных файловых систем.

Наиболее популярными в Украине видеорегистраторами этого типа являются программно-аппаратные комплексы iLDVR, DigiNet и др.

Автономные видеорегистраторы

Представляют собой специализированные устройства, которые разработаны для сохранения записей видеонаблюдения и не требуют для работы подключения к ПК. Для некоторых видов автономных регистраторов могут использоваться выделенные термины, например, NVR – сетевой видеорегистратор, HDVR – гибридный видеорегистратор, Car DVR – автомобильный видеорегистратор. Однако во многих случаях для них используют общее название DVR, под которым подразумевают именно автономные регистраторы независимо от их области применения.

К основным преимуществам автономных DVR относятся: высокая надежность, простота в настройке и управлении, небольшие размеры. Сравнительным недостатком является невозможность (или ограниченные возможности) модернизации.

В автономных видеорегистраторах применяется специализированное аппаратное и программное обеспечение. Поэтому в большинстве случаев для хранения видеозаписей не используются традиционные компьютерные файловые системы. Жесткие диски в системе должны быть специальным образом инициализированы и размечены для использования в конкретной модели DVR. В последнее время растет количество регистраторов, использующих в качестве управляющего ПО встраиваемые (embedded) версии Linux. Для хранения видеозаписей такие DVR могут применять модифицированные варианты файловой системы Ext.

В Украине популярны автономные видеорегистраторы производства AVTech, Hikvision, EverFocus и др.

Проблемы съема и восстановления данных на DVR

Наблюдающийся в последние годы большой спрос на цифровые системы видеонаблюдения при отсутствии стандартизации приводит к тому, что на рынке присутствуют сотни моделей DVR с различными функциональными возможностями. Видеозаписи в них могут сохраняться на одном или нескольких отдельных жестких дисках; в некоторых случаях несколько HDD в системе могут быть объединены в один виртуальный диск; для сжатия видеопотока обычно используются нестандартные кодеки и алгоритмы; часто применяется парольная защита и шифрование видеозаписей.

В результате DVR сильно отличаются по методам записи и возможностям по экспорту данных. При этом зачастую видеорегистраторы не обеспечивают простого быстрого доступа к сохраненным видеоданным в форме, приемлемой для специалиста по расследованию ИТ-инцидентов.

Среди основных технических и организационных проблем съема данных с цифровых видеорегистраторов можно выделить следующие.

Значительный объем видеоданных

Современные видеорегистраторы строятся по многоканальной схеме, обеспечивая возможность одновременного сохранения видео с нескольких камер. Обычно DVR имеют 4, 8/9 и 16 видеовходов, на рынке доступны также 6, 12, 24 и 32-канальные DVR. При этом средняя емкость жестких дисков, устанавливаемых в регистраторы, непрерывно растет, а качество сжатия видео повышается.

Эти факторы приводят к тому, что регистраторы могут вмещать большое количество информации, накопленной с разных видеокамер за значительный период времени.

При этом при расследовании инцидента не всегда требуется анализировать всю сохраненную информацию, достаточно ограничиться временем инцидента и теми камерами, на которых он зафиксирован. Однако далеко не все модели DVR обеспечивают возможность выбора заданных временных интервалов и камер при экспорте видеозаписей. Существуют видеорегистраторы, предоставляющие возможность экспорта только в режиме захвата видеотрансляции по локальной сети. При этом время, требуемое для съема данных, будет равно длительности записи, умноженной на количество камер и может составлять дни и даже недели. Конечно, это является исключением из правил, но при съеме данных с DVR необходимо учитывать то, что процедура может отнимать достаточно много времени.

Ограничение способов экспорта видеоданных

Большинство современных видеорегистраторов поддерживают возможность экспорта (архивирования) видеозаписей. В автономных DVR для этого могут использоваться следующие способы и их комбинации:

- запись на CD/DVD;
- запись на USB Flash накопитель;
- запись на USB HDD;
- экспорт по Ethernet.

В то же время существуют сложности, ограничивающие применимость того или иного способа экспорта. Оптические диски имеют небольшую емкость и сравнительно небольшую скорость записи, что при большом объеме видеоданных может требовать неприемлемо больших временных затрат. При использовании USB Flash может возникнуть проблема подбора совместимой модели флэш-накопителя из-за ограниченной поддержки USB-устройств в некоторых DVR.

Экспорт через сеть обычно требует применения специального клиентского ПО, которого может не оказаться под рукой при съеме данных на выезде. В большинстве случаев оптимальным с точки зрения скорости съема и объема архивируемых данных является запись на внешние USB HDD, однако эта возможность реализована далеко не во всех DVR, кроме того, что, как и для флэш-накопителей, существует проблема совместимости.

В литературе рассматривается способ экспорта данных, основанный на оцифровке аналогового сигнала с выхода видеорегистратора. Однако на современных DVR такой способ требует значительных временных затрат и приводит к ухудшению качества изображения, появлению шумов и артефактов. Кроме того, в этом случае не удовлетворяются требования к полноте и точности копии, обязательные для съема данных. Поэтому такой способ возможно применять только в крайних случаях, когда DVR не обеспечивает других возможностей по съему данных.

Нестандартные алгоритмы сжатия и форматы файлов

Все цифровые видеорегистраторы при записи используют тот или иной алгоритм сжатия видеоинформации для уменьшения требуемой емкости хранилища. Наиболее часто применяются алгоритмы, основанные на MJPEG, MPEG-2, MPEG-4, H.264.

В то же время при отсутствии единых стандартов практически каждый производитель использует собственные форматы сохранения видеозаписей. В некоторых моделях DVR даже в различных версиях прошивки могут использоваться несовместимые между собой форматы файлов и способы хранения записей. Обычно эти форматы файла, кроме непосредственно видеопотока, предполагают хранение метаданных (например, даты и времени записи, номера камеры). Наборы метаданных и их расположение в структуре файла также не стандартизованы.

Большинство DVR осуществляют экспорт в собственных форматах файлов, поддержка которых отсутствует в операционных системах. Для их воспроизведения требуются специальные кодеки и/или плейеры.

Ряд видеорегистраторов позволяют экспортировать данные в традиционные для ПК форматы файлов (avi, mpg). Однако при этом ухудшается качество изображения из-за перекодирования видеопотока.

Нетрадиционные файловые системы

Подавляющее большинство автономных DVR не используют традиционных для ПК файловых систем. Поэтому извлечение жесткого диска из видеорегистратора и подключение его к ПК не позволяет получить доступ к видеозаписям.

Производители разрабатывают собственные специализированные “файловые системы” для хранения видеозаписей, достаточно сильно различающиеся между собой. В некоторых моделях регистраторов в таких “файловых системах” существует разделение между областями, в которых хранится видеопоток, и областями служебных данных – индексами для осуществления быстрого поиска, метаданными, протоколом работы DVR и т.п. Другие DVR могут при записи последовательно чередовать блоки служебной и видеоинформации. Логические структуры данных, описывающие такие “файловые системы”, необязательно располагаются в начале диска, как это принято в традиционных компьютерных файловых системах, на практике встречаются ситуации, когда они находятся в конце или середине дискового пространства.

Некоторые видеорегистраторы поддерживают многодисковые конфигурации. При этом несколько жестких дисков в системе могут быть объединены в один общий виртуальный диск (аналогично RAID массивам на ПК). Также на практике встречаются ситуации, когда они используются как отдельные накопители с общей для всех или отдельной для каждого жесткого диска файловой системой.

Ряд недавних моделей видеорегистраторов используют в качестве управляющего ПО встраиваемые версии Linux. В таких DVR для хранения видеозаписей могут применяться модифицированные варианты файловой системы Ext. В некоторых случаях такой жесткий диск можно смонтировать в систему и получить доступ к видеозаписям. Но такая возможность есть не всегда – некоторые DVR обрабатывают часть логических структур файловой системы во внутренней флэш памяти, не сохраняя их на HDD.

Парольная защита и шифрование видеозаписей

Многие современные видеорегистраторы имеют достаточно развитые средства защиты сохраненной видеоинформации, основанные на применении средств разграничения прав доступа и шифрования.

Так, в DVR на основе встраиваемых версий Linux поддерживается возможность создания пользователей с различными правами доступа (например, только просмотр видео, экспорт записей, права администратора и т.п.). Аутентификация пользователей осуществляется с помощью паролей, которые могут вводиться как со встроенной клавиатуры регистратора, так и удаленно, через локальную сеть или терминальное подключение.

Сведения о пароле не всегда могут быть доступны при проведении расследования инцидента, например, из-за того, что подозреваемый в инциденте скрывает эту информацию. При этом не существует общей процедуры получения доступа к данным в таком случае, а обнуление пароля может приводить к форматированию жесткого диска и потере всех сохраненных видеозаписей.

В ряде моделей DVR применяется дополнительный способ защиты данных путем установки ATA пароля на жесткий диск, на который осуществляется сохранение видеозаписей.

Некоторые видеорегистраторы используют шифрование видеопотока, что существенно осложняет или делает невозможным съем данных с них при отсутствии пароля доступа. Такая функция чаще встречается в видеорегистраторах, построенных на базе ПК.

Невысокое качество исполнения и поддержки

К сожалению, значительная доля представленных в Украине моделей видеорегистраторов относится к недорогим DVR неизвестных китайских производителей, не обладающих высоким качеством исполнения и поддержки. Для многих из них обычной практикой является неточная, неполная или полностью отсутствующая документация.

Из-за этого в некоторых случаях оказывается затруднительно даже просто скопировать видеозаписи с исправного регистратора, а восстановление информации представляет собой сложнейшую нетривиальную задачу.

Недостаточное количество квалифицированных специалистов

Еще одной характерной для Украины проблемой является недостаточное количество квалифицированных специалистов. Съем и восстановление данных могут быть доверены сотрудникам, имеющим весьма отдаленное представление о принципах работы и хранения видеозаписей на современных регистраторах.

Вследствие их неквалифицированных действий нередки случаи повреждения, модификации, нарушения целостности видеозаписей.

Наиболее часто на практике встречается ситуация, когда по тем или иным причинам вместо съема данных через имеющийся в регистраторе интерфейс (запись на DVD или USB Flash накопитель, экспорт по сети и т.п.) жесткий диск извлекается из DVR и подключается к ПК под управлением ОС Windows без использования блокиратора записи. При этом данные на HDD модифицируются системой, что приводит к повреждению специфической разметки на нем. Такой модифицированный диск перестает распознаваться DVR, а в ОС Windows данные недоступны из-за использования нестандартной файловой системы. В результате это приводит к потере данных и необходимости выполнения сложных работ по их восстановлению. Нередки также случаи, когда данные на DVR повреждаются вследствие форматирования HDD или попыток снять установленный пароль.

Иногда потеря данных бывает связана с непониманием принципов записи данных на DVR. Многие видеорегистраторы начинают запись в фоновом режиме непосредственно после включения питания. Если требуемая видеозапись была сделана в начале цикла перезаписи регистратора, она может быть затерта (перезаписана) новой записью и, в таком случае, восстановлению не подлежит.

Особенности съема и восстановления данных на DVR

В настоящее время на рынке систем видеонаблюдения отсутствуют единые стандарты на способы хранения, обработки и экспорта видеозаписей. Используемые в DVR программные и аппаратные средства, методы кодирования видеопотока и возможности переноса информации на внешние носители значительно отличаются у разных производителей.

Вследствие этого оказывается невозможным выработать общую стандартную процедуру съема и восстановления данных, которая была бы применима для всех ситуаций и рынке моделей видеорегистраторов. Таким образом, оптимальный способ извлечения видеоинформации с DVR должен выбираться экспертом отдельно для каждого случая.

Операции по съему и восстановлению данных с видеорегистратора можно разделить на пять основных категорий.

1. Экспорт видеозаписей с помощью встроенных средств DVR.

Такие операции позволяют сравнительно быстро перенести имеющиеся на DVR видеозаписи на внешние носители, но не обеспечивает возможности съема данных в случае их удаления или повреждения. Экспорт осуществляется по одному из доступных интерфейсов (USB, Ethernet, запись на CD/DVD). Приоритет следует отдавать сохранению данных в исходном формате, однако при этом могут потребоваться специальные кодеки и плейеры для воспроизведения записей.

2. Логический съем (копирование) файлов видеозаписей.

Такие операции обычно выполняются при работе с видеорегистраторами на базе ПК, но применимы и для отдельных автономных DVR, сохраняющих видео в традиционных файловых системах. В большинстве случаев при логическом съеме данных не обеспечивается возможность восстановления удаленных или поврежденных видеозаписей. Для воспроизведения сохраненных файлов могут требоваться специальные кодеки и плейеры.

3. Создание посекторной копии данных накопителей, установленных в DVR.

Такая операция обеспечивает наиболее полные возможности по анализу сохраненной информации, включая восстановление удаленных или поврежденных видеозаписей, съем данных в обход установленных паролей и т.п. Для создания посекторной копии необходимо выключение и вскрытие корпуса видеорегистратора, что не всегда возможно. Необходимо отметить, что из-за использования в DVR нестандартных форматов файлов и нетрадиционных файловых систем, анализ и интерпретация скопированных данных могут быть затруднены.

4. Захват аналогового видеопотока с выхода DVR.

Операцию следует осуществлять только в случаях, когда DVR не имеет встроенных средств экспорта данных и отсутствует возможность создания полной посекторной копии. При захвате аналогового видео ухудшается качество изображения, не обеспечивается возможность восстановления удаленных или поврежденных видеозаписей.

5. Перекодирование видеоданных в традиционные компьютерные форматы.

Некоторые видеорегистраторы поддерживают возможность экспорта не в собственном внутреннем формате, а в традиционные компьютерные форматы файлов (avi, mpg). Иногда доступны утилиты, выполняющие аналогичное конвертирование форматов видео. Однако в результате такого перекодирования происходит пережатие видео, приводящее к модификации исходных данных и потере качества. Кроме того, при этой операции может быть утеряна метаинформация о дате и времени съемки, что во многих случаях недопустимо. Поэтому перекодирование рекомендуется выполнять только в качестве вспомогательной операции, например, для упрощения представления результатов исследования, а съем данных для анализа выполнять в исходном формате видеорегистратора.

Независимо от выбранного подхода, операции по съему и восстановлению видеозаписей на DVR должны выполняться способом, исключающим возможность случайной модификации или повреждения данных в процессе выполнения работ. При этом необходимо документировать все предпринимаемые действия.

Рекомендации по съему данных на DVR

Хотя общей для всех случаев и моделей видеорегистраторов процедуры съема данных не существует, приведенные ниже рекомендации позволяют повысить вероятность сохранения видеозаписей.

Отключать питание DVR не рекомендуется. В большинстве случаев съем данных с работающей системы более эффективен, кроме того, внезапное отключение может привести к повреждению данных или потере введенного пароля.

Извлекать жесткие диски из системы и подключать их к ПК не следует. Для большинства автономных DVR это не обеспечит непосредственного доступа к видеоданным. Такую операцию целесообразно выполнять только для создания полной посекторной копии, если есть подозрение в искажении или удалении видеозаписей, а также в случае установленного пароля, который невозможно получить альтернативными способами.

Необходимо зафиксировать основные настройки DVR (настройки записи/воспроизведения, сетевые настройки и т.п.).

Необходимо проверить соответствие системного времени DVR и официального времени.

Необходимо определить длительность цикла перезаписи видеорегистратора. Это позволит определить, насколько долго требуемые видеозаписи могут

храниться в системе. Особенно важно, если отсутствует возможность сохранить данные сразу.

Выбрать способ экспорта видеозаписей. На основании объема требуемых данных и поддерживаемых видеорегистратором интерфейсов определить возможность сохранения данных на оптический диск, Flash накопитель, внешний жесткий диск или экспорта по Ethernet. Если DVR не имеет встроенных средств экспорта, корректно отключить его и выполнить полную посекторную копию данных на всех накопителях в системе.

Определить возможность сохранения данных за требуемые интервалы времени и с требуемых камер. Это позволит минимизировать объем копируемых данных и уменьшить временные затраты.

Сохранять данные необходимо в исходном формате видеорегистратора. Не рекомендуется выполнять перекодирование видеозаписей.

В случае, если используется нестандартный формат видеопотока, необходимо совместно с видео сохранить программное обеспечение и кодеки для его воспроизведения. Некоторые системы могут делать это автоматически.

Желательно проверить возможность воспроизведения сохраненных видеозаписей непосредственно после их съема.

В случаях, когда видеозаписи удалены, повреждены или модифицированы, установлен пароль доступа, DVR имеет аппаратные или программные сбои, может потребоваться восстановление данных. Для восстановления данных обязательно необходимо создание полной посекторной копии.

Выводы

На рынке систем видеонаблюдения отсутствуют единые стандарты на способы хранения, обработки и экспорта видеозаписей. Это не позволяет разработать единую процедуру съема и восстановления данных, которая была бы применима для всех ситуаций, возникающих на рынке моделей видеорегистраторов.

Для выполнения работ по съему и восстановлению данных требуются знания о принципах хранения данных на DVR и высокая квалификация специалистов.

Разработаны практические рекомендации, которые позволяют минимизировать риск повреждения и искажения видеозаписей при съеме и восстановлении данных на видеорегистраторах.

Отримано 14.12.2011