восстановление данных на NTFS разделах

крис касперски

эта статья открывает цикл публикаций, посвященный ручному восстановлению данных на NTFS-дисках без использования автоматизированных "докторов", зачастую только добивающих "пациента" вместо его лечения. мы коснемся всех аспектов проблемы – логические и физические дефекты, жесткие диски и съемные носители (CD-ROM, ZIP, магнитооптика, FLASH…), программные и аппаратные RAID-массивы и т. д. сегодня мы рассмотрим основные концепции хранения и организации данных на жестких дисках и соберем необходимый инструментарий.

введение

Долгое время главным козырем противников NTFS был следующий аргумент – чем вы будете ее восстанавливать, если она умрет? А мрет она, как показывает практика, достаточно часто. При всей своей надежности, NTFS не застрахована от потрясений. Ошибки оператора, вирусы, сбои питания, зависания ОС, дефекты поверхности, отказ электроники… С каждым днем человечество все сильнее и сильнее становится зависимо от компьютеров, объемы жестких дисков стремительно растут, а вместе с тем растет и ценность содержащихся на них данных, потеря которых зачастую невосполнима.

Спрос рождает предложение и на рынке как грибы после дождя вылупляются фирмы, специализирующиеся на восстановлении данных, однако, по-настоящему хороших специалистов можно встретить только в двух, ну от силы в трех из них, а все остальные лишь создают видимость кипучей деятельности, выставляя астрономические счета при довольно посредственном качестве восстановления. Но время кустарей уже ушло. Рабочая атмосфера изменилась. Хакеры разобрались со строением NTFS и документировали ее ключевые структуры. Начал формироваться достойный инструментарий для ручного восстановления. Наконец, за минувшее время накопился огромный опыт по борьбе за спасение данных, частью которого автор и хочет поделиться с читателями.

если вдруг случился сбой и данные оказались утеряны…

Прежде всего – не паникуйте! Заниматься восстановлением можно только на трезвую голову. Непродуманные, лихорадочные действия только усугубляют ваше и без того незавидное положение!

Не используйте никаких автоматизированных "лечилок", если полностью в них не уверенны. Последствия такого лечения могут быть катастрофическими, а результаты "восстановления" – необратимыми. То же самое относится и к "специалистам", обитающим в фирмах непонятного происхождения и орудующих все теми же автоматизированными утилитами, которыми вы можете воспользоваться и без них. Некоторые пытаются создавать необходимый инструментарий самостоятельно. Чаще всего он оказывается неработоспособным еще с рождения, но зато какая гордость для фирмы! Какое впечатляющее средство демонстрации собственной крутизны! Поверьте, утилиты типа Easy Recovery и Get Data Back далеко не дураки писали (да еще и при участии непосредственных разработчиков оригинального драйвера NTFS, хорошо знающих все его тонкости и особенности поведения). Это лучшее из того, что есть на рынке и пока еще никому не удалось их превзойти! (разумеется, речь идет лишь об автоматизированном восстановлении).

Ничего не записывайте на восстанавливаемый диск и не позволяйте этого делать остальным приложениям! Если вы случайно удалили файл с системного диска, ни в коем случае не выходите из Windows "культурным" способом. Лучше нажмите RESET (при штатом завершении сеанса, система сохраняет на диске текущую конфигурацию, существенно увеличивая риск необратимого затирания удаленного файла).

Не пытайтесь "насиловать" сбойные сектора многократными чтениями – это лишь расширяет дефектную область на соседние сектора и здорово уродует магнитную головку, после чего здоровые сектора не смогут читаться тоже. Лучше выполните длинное (long) чтение с диска с отключенными контролирующими кодами, тогда контроллер возвратит все, что осталось от сектора (зачастую сбой затрагивает только несколько байт).

Если винчестер издает подозрительные звуки типа постукивания или скрежета, немедленно выключите питание компьютера (опять-таки, не позволяя системе ничего писать на

диск), поскольку в любой момент винчестер может доломаться окончательно и тогда ему уже никакой электронщик не поможет.

Восстанавливайте SCSI (и, в особенности, RAID!) диски только на "родном" контроллере (различные контроллеры используют различные схемы трансляции адресов). Если же контроллер сдох, то либо ремонтируйте его, либо ищите точно такой же. С IDE-дисками в этом плане намного проще, – их контроллеры более или менее стандартизованы, однако, с дисками большого объема (свыше 528 Мбайт) уже начинается неразбериха и путаница, ставящая их в зависимость от конкретной BIOS и выбранного режима работы (NORMAL, LBA или LARGE). Если восстанавливаемый диск работает под управлением нестандартных драйверов типа Rocket, OnDisk и т.д., они должны присутствовать и на загрузочной диске (загрузочном CD), с которого производится восстановление.

Наконец, если данные восстановить так и не удалось – не расстраивайтесь. Во всем в жизни надо видеть и хорошие стороны, даже когда ничего хорошего нет.

структура диска – базовые концепции

Физически жесткий диск представляет собой запечатанную банку с одной или несколькими одно или двухсторонними пластинами, насажанными на шпиндель. Чтение/запись данных осуществляется блоком магнитных головок, каждая их которых обслуживает одну из поверхностей пластины. Информация хранится в форме концентрических колец, называемых ***треками*** (***track***) или дорожками. Треки, расположенные на равном расстоянии от центра всех пластин, образуют ***цилиндр*** (***cylinder***). Фрагмент трека, образованный радиальным делением, называется ***сектором*** (***sector***). В современных винчестерах количество секторов на трек не остается постоянным и дискретно растет по мере удаления от центра пластины, поддерживая более или менее постоянные линейные размеры сектора. Треки и головки нумеруются начиная с нуля, сектора – начиная с единицы. Размер сектора для жестких дисков – 512 байт.

Первой схемой адресации секторов, доставшейся жестким дискам в наследство от дискет, стала так называемая ***CHS-адресация***, представляющая собой сокращение от Cylinder/Head/Sector (Цилиндр/Головка/Сектор) и возникшая под давлением экономических причин. Когда-то, координаты адресуемого сектора напрямую соответствовали физической действительности, что упрощало (а, значит, и удешевляло!) дисковый контроллер, не требуя от него никакой интеллектуальности. Помимо того, что такая схема адресации чудовищна неудобна для программистов (последовательное чтение диска растягивается на три вложенных цикла!), она еще и до неприличия косна! Количество секторов в треке должно быть постоянным для всего диска, а в новых винчестерах это не так. Поэтому, для сохранения совместимости с существующим программным обеспечением, дисковый контроллер виртуализует геометрию винчестера, что ставит нас в зависимость от выбранной схемы трансляции (а схема трансляции – дело сугубо внутреннее и потому не стандартизированное). Параметры диска, сообщаемые устройством и напечатанные на этикетке, ***всегда*** виртуальные и никакой возможности узнать реальное положение дел у нас нет.

IDE-диски благодаря наличию интегрированного контроллером внутри, в наименьшей степени зависимы от внешнего мира и могут свободно мигрировать от одной машины к другой (при условии корректного поведения BIOS'а, но об этом чуть позже). Некоторые винчестеры поддерживают специальную ATA-команду "Initialize device parameters", устанавливающую текущую виртуальную геометрию диска, а точнее выбранное количество головок и число секторов на дорожку. Количество цилиндров вычисляется контроллером самостоятельно, на основании общего объема диска, который кстати говоря, также можно изменять программными средствами (за это отвечает ATA-команда SET MAX ADDRESS). Некоторые драйвера (и BIOS'ы) изменяют геометрию диска, привязывая винчестер к себе прочными брачными узами и в другом окружении такой диск работать уже не будет, ну во всяком случае до установки правильной геометрии.

Со SCSI-устройствами ситуация обстоит гораздо хуже и диск соглашается работать только с тем контроллером, под которым он был отформатирован. Различные контроллеры используют различные схемы трансляции и потому подключение диска к несовместимому контроллеру произвольным образом "перемешивает" сектора. Редактор диска с таким винчестером работать еще будет, а вот штатные средства операционной системы (и большинство "докторов") нет.

Продвинутые контроллеры автоматически замещают плохие сектора, либо сохраняя эту информацию в свой энергонезависимой памяти, либо в записывая ее в инженерные сектора самого диска. Это еще сильнее привязывает накопитель к его контроллеру (правда, некоторые

SCSI-диски выполняют переназначение секторов собственными средствами). Таким образом, выход SCSI-контроллера из строя фактически приравнивается к отказу самого диска. Никогда не приобретайте SCSI-контроллеры no-name производителей – в любой момент они могут кануть в лету и тогда поставки новых контроллеров прекратятся. Контроллеры, интегрированные в материнские платы, это вообще песня. Ненадежные, ни с чем не совместимые… а что вы еще хотели за такую цену?

Сложнее всего приходится RAID-массивам, схема трансляции адресов которых полностью определяется контроллером. Массивы уровня 1 (mirroring или зеркала) чаще всего транслируются всквозную и без особых проблем могут быть перенесены на любой другой контроллер или даже подключены в обход него. Массивы остальных уровней (и в особенностей RAID 3/RAID 5) на других типах контроллеров по обыкновению неработоспособны. Программные RAID'ы, монтируемые Windows NT, содержат информацию о своей геометрии в системном реестре и не могут быть непосредственно перенесены на другие системы. Переустановка Windows NT (равно как и крах оной) уничтожает программный RAID. К счастью, эта потеря обратима и в следующих статьях этого цикла мы раскроем секреты техники восстановления.

Несмотря на то, что CHS-трансляция в настоящее время признана устаревшей (устройства, придерживающиеся спецификации ATA/ATAPI-6, принятой в июне 2001 года, уже не обязаны ее поддерживать), она до сих пор встречается во многих служебных структурах операционной системы (в частности в таблице разделов и загрузочном секторе), поэтому имеет смысл остановиться на этом вопросе поподробнее, тем более, что здесь есть о чем поговорить.

На интерфейсном уровне, адрес сектора передается следующим образом (см. листинг 1)

порт	значение
0172/01F2	кол-во секторов
0173/01F3	номер сектора (биты 0-7)
0174/01F4	номер цилиндра (биты 0-7)
0175/01F5	номер цилиндра (биты 8-15)
0176/01F6	номер головки (биты 0-3), привод на шине (бит 4), режим CHS/LBA (бит 6)

Листинг 1 интерфейс с IDE-диском в режиме CHS

Сервисные функции BIOS'а, напротив, адресуют диск слегка по своему:

регистр	значение
AL	кол-во секторов для обработки
CH	номер цилиндра (биты 0-7)
CL	номер цилиндра (биты 6-7), номер сектора (биты 0-5)
DH	номер головки
DL	привод на шине | 80h

Листинг 2 интерфейс с прерыванием INT13h BIOS

Таким образом, на адресацию цилиндров BIOS отводит всего 10 бит и потому максимальное количество цилиндров на диске ограничено всего 1024, что при четырех битной адресации головок, дает предельно достижимый объем диска в $512 * 2^{10} * 2^6 * 2^4 == 536870912$ байт или 512 Мб. Ха! Производители винчестеров перешагнули этот барьер уже много лет назад и с той поры, кстати говоря, очень многое изменилось. MS-DOS ушла небытие, а пришедшая ей на смену Windows работает с диском через собственный драйвер и ограничения BIOS ее никак не касаются. Ну почти не касаются… Ведь первичную загрузку операционной системы осуществляет никто иной как BIOS и если системные компоненты расположены в секторах, находящихся за пределами 1024 сектора, операционная система попросту не будет загружена! Причем, это относиться ко всем операционным системам, а не только к критикуемой Windows!

Для преодоления этого ограничения BIOS вводит дополнительный уровень трансляции (режим LARGE), увеличивая количество головок (благо, BIOS выделяет для их адресации аж 8 бит, против 4 бит, выделяемых контроллером диска). К следствие, предельно допустимый объем диска теперь составляет $512\ 2^{10}\ 2^6 * 2^8 == 8.589.934.592$ байт или 8 Гбайт. Это в теории. На практике же большинство BIOS'ов содержали грубые ошибки и при работе с дисками свыше 2 Гб они либо банально зависали, либо теряли старшие разряды цилиндра, обращаясь к началу

диска и необратимо гробя все служебные структуры. До сих пор многие вполне современные BIOS'ы не позволяют адресовать более 64 головок (виртуальных), что ограничивает предельно допустимый объем диска все тем же 2 Гбайтами. Поэтому, при переустановке Windows поверх старой версии на логический диск емкостью свыше 2 Гбайт, она может перестать загружаться. Все очень просто! Когда система ставится на только что отформатированный диск, она располагает все свои файлы в самом начале, но по мере же заполнения диска, область свободного пространства отодвигается все дальше к концу… Кстати говоря, отодвинуть файлы первичной загрузки может и дефрагментатор (или установка пакета обновления). Короче говоря, владельцем больших винчестеров настоятельно рекомендуется разбить свое хозяйство на несколько дисков, установив размер первого (загрузочного) раздела не более, чем в 8 Гбайт, а лучше даже в 2 Гбайта.

SCSI-устройства от рождения поддерживают прозрачный механизм логической адресации, или сокращенно ***LBA*** (*Linear Block Address*), последовательно нумерующий все сектора от 0 до последнего сектора диска. В IDE-накопителях LBA-адресация появилась только начиная с ATA-3, но быстро завоевала всеобщее признание. Разрядность адресации определяется устройством. В SCSI она от рождения 32-битная, а IDE-устройства вплоть до принятия спецификации ATA-6 были ограничены 28 битами, которые распределялись следующим образом:

порт	значение
0172/01F2	кол-во секторов
0173/01F3	номер сектора (биты 0-7)
0174/01F4	номер сектора (биты 8-15)
0175/01F5	номер сектора (биты 16-24)
0176/01F6	номер сектора (биты 24-28), привод на шине (бит 4), режим CHS/LBA (бит 6)

Листинг 3 интерфейс с IDE-диском в режиме LBA

Как можно видеть, 28 битная адресация обеспечивает поддержку дисков с объемом вплоть до 128 Гбайт, однако, включение в BIOS поддержки LBA еще не отменяет 8 Гбайтного ограничения и номер последнего адресуемого цилиндра по прежнему остается равным 1024 со всеми вытекающими отсюда последствиями. SCSI-дискам с их подлинно 32 битной адресацией несколько проще и они поддерживают законные 2 Тбайта, а все потому что управляются своим собственным BIOS'ом, на которых не наложено никаких дурацких пережитков старины.

Утвержденная ATA-6 48 битная адресация расширяет предельно допустимые размеры IDE-дисков до астрономических величин (конкретно – до 131.072 Тбайт), по крайней мере в теории. На практике же, в Windows 2000 с пакетом обновления SP2 или более ранним, отсутствует поддержка 48 разрядной LBA и для работы с большими дисками необходимо обновить драйвер Atapi.sys и добавить к следующему ключу реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\atapi\Parameters параметр EnableBigLba типа DWORD со значением 1. (за подробностями обращайтесь к Microsoft Knowledge Base: 260910).

Один физический диск может быть разбит на несколько ***логических***, каждый из которых последовательно нумеруется от первого до последнего сектора либо "сквозной" адресацией, либо по CHS-схеме. В одних случаях Windows требует задания абсолютного номера сектора (который на самом деле никакой не абсолютный, а относительный, отсчитывающийся от стартового сектора раздела), в других – ожидает увидеть "святую троицу" (цилиндр, головку, сектор), опять-таки, отсчитывающихся от стартового сектора. Так, если раздел начинается с адреса 123/15/62, то первой его головкой все равно будет головка 0!

На уровне файловой системы операционная система адресует диск ***кластерами*** (***cluster***). Каждый кластер образован непрерывной последовательностью секторов, количество которых равно степени двойки (1, 2, 4, 8…). Размер кластера задается на этапе форматирования диска и в дальнейшем уже не меняется. Основное назначение кластеров – уменьшение фрагментации файлов и уменьшение разрядности служебных файловых структур. В частности, FAT16 нумеруют кластеры двойными словами и потому может адресовать не более 10000h*sizeof(cluster) дискового пространства. Легко видеть, что уже на 80 Гбайтовом диске размер кластера составляет 1 Мбайт и десяток файлов по одному байту каждый сожрут 10 Мбайт! Впечатляет, не правда ли? NTFS, оперирующая 64 битными величинами, не страдает подобными ограничениями и типичная величина кластера, выбираемая по умолчанию, составляет всего 4 сектора. В отличии от секторов, кластеры нумеруются начиная с нуля.

>>>> врезка первичная диагностика аварии

симптом		диагноз	лекарство
жесткий диск не опознается BIOS'ом		отказ электроники жесткого диска	–
операционная система не загружается, BIOS выдает надпись "non system disk", missing operation system или что-то в этом роде	при загрузки с дискеты логические диски не видны (команда C: дает ошибку)	повреждена таблица разделов или сигнатура 55h AAh	восстановите MBR вручную или при помощи GetDataBack
	логические разделы видны и исправны (команды C: и dir C: работают)	слетел boot и/или MBR загрузчик	запустите консоль восстановления и дайте команды FIXBMR и FIXBOOT
	логические разделы видны, но команда dir C: дает ошибку	поврежден boot-сектор или MTF	восстановите boot-сектор вручную или резервной копии, восстановите MFT из MFTMirr
операционная система начинает закружатся, но затем виснет или прерывается с сообщением об ошибке	команда dir C: выполняется нормально, chkdsk не находит ошибок	навернулась сама операционная система	переустановите операционную систему, предварительно скопировав все ценные файлы на другой носитель
	команда dir в одном или нескольких подкаталогах выводит мусор или показывает не все файлы	повреждена MTF или одна из ее дочерних структур	запустите Disk Explorer и прочитайте файлы из MFT напрямую в обход индексов
	некоторые файлы не читаются, при этом винчестер издает ритмичные скребущие звуи	физические повреждения поверхности диска	запустите утилиту восстановления жесткого диска от его производителя
	некоторые файлы содержат в себе фрагменты других файлов	на диске образовались пересекающиеся кластеры	запустите chkdsk
	свободное место на диске планомерно уменьшается без видимых причин	некоторые кластеры оказались потерянными	запустите chkdsk

Таблица 1 симптомы основных заболеваний жестких дисков

инструменты

Даже если у вас золотые руки и светлая голова, при восстановлении данных ни за что не обойтись без инструментов. В идеале вы должны быть готовыми разработать все необходимое для работы самостоятельно. Восстановление данных – довольно кропотливая и рутинная работа и при реанимации 80 – 120 Гбайтного диска без автоматизации никуда. Недостаток всех известных дисковых докторов – отсутствие встроенного языка или хотя бы развитой системы макрокоманд. Естественно, прежде чем что-то автоматизировать необходимо разобраться в ситуации и выполнить эту работу может только человек. Компьютеру доверять ее ни в коем случае нельзя – для этого он недостаточно интеллектуален. Только человек может надежно отличать где лежат актуальные данные, а где мусор.

Однако, не стоит впадать и в другую крайность, в очередной раз изобретая велосипед. Среди представленных на рынке утилит, есть практически все необходимое. Естественно,

большинство распространяются по коммерческой схеме и за них приходится платить. К сожалению, многие из дорогостоящих инструментов не оправдывают своих ожиданий и к выброшенным на ветер деньгам примешивается горечь утраты по безвозвратно потерянным данным. Автор протестировал большое количество разнообразных программных продуктов и ниже описывает наиболее предпочтительные из них, проверенные энтропией и временем.

загрузочная дискета

Средства восстановления и диагностики, расположенные на основном жестком диске, годятся разве что для обучения, а для реальной работы они бесполезны. Даже если сбой окажется не настолько серьезным, чтобы воспрепятствовать загрузке Windows, попытка "лечения" диска в многозадачной среде носит весьма непредсказуемый характер. Записывая что-либо на диск в обход драйвера файловой системы вы здорово рискуете. Допустим, вы восстанавливаете удаленный файл, обновляя MFT (Master File Table – святая святых файловой системы NTFS), а в это время система создает/удаляет другой файл, обращаясь к тому же самому сектору, что и вы. Ну и что произойдет в результате? Правильно – файл, а, возможно, и весь дисковый том, умрет окончательно. К тому же система блокирует активные исполняемые файлы и файлы данных, что делает невозможным их восстановление даже при наличии архивной копии. Про борьбу с вирусами лучше вообще не говорить. Многие вирусы, обосновавшись в системе, блокируют запуск антивирусных программ или умело скрываются от них, не давая себя удалить или обнаружить. Если же в результате сбоя перестала загружаться Windows, вы вообще остаетесь ни с чем…

Главное преимущество FAT16/32 по сравнению с NTFS это, бесспорно, возможность загрузки с системной дискеты. MS-DOS 7.0 поддерживает длинные имена, позволяя скопировать с восстанавливаемого диска все файлы, которые только доступны штатному драйверу операционной системы. Но с NTFS такой номер уже не пройдет! Однако, никто не запрещает нам подключить восстанавливаемый диск "вторым" к системе с работоспособной NT. Для этого даже не обязательно иметь два компьютера. Просто подключите к своему компьютеру еще один винчестер, установите на него NT и наслаждайтесь жизнью. При этом следует учитывать, что информация о программных RAID'ax, созданных Windows NT 4.0 или более ранними версиями, содержится в реестре и потому при переносе диска на другую систему оказывается недоступна. Динамические диски, появившиеся в Windows 2000, хранят свою атрибуты в фиксированных местах диска и потому не привязаны к своей родной системе. С шифрованными файлами дела обстоят не в пример хуже. Ключ шифровки хранится в недрах пользовательского профиля и на другой системе извлечение файлов оказывается невозможным. Причем, создание пользователя с таким же именем/паролем не решает проблемы, т. к. ключ генерируется системой случайным образом и не может быть воспроизведен. Ничего не остается, как действовать тупым перебором.

Некоторые типы разрушений файловой системы способы завешивать оригинальный NTFS-драйвер или выбрасывать синий экран смерти, что создает серьезные проблемы (чтобы восстановить диск, мы должны запустить определенный инструментарий, а чтобы запустить инструментарий, нам надо загрузить Windows, а вот это мы как раз сделать и не можем!). Попробуйте подключить такой диск к системе, не поддерживающий NTFS (например, Windows 98 или MS-DOS), естественно выбранные вами утилиты восстановления должны быть совместимы с ней. Или – как вариант – натравите на такой диск LINUIX. Драйвер LINIX'a игнорирует вспомогательные структуры файловой системы (такие, например, как файл транзакций) и потому успешно монтирует диск даже когда в них содержится сплошной мусор.

Благодаря усилиям Марка Руссиновича, создавшего замечательную утилиту **NTFSDOS Professional**, мы может работать с NTFS-разделами в среде Windows 9x/MS-DOS. Однако, это отнюдь не самостоятельный драйвер, а всего лишь обертка вокруг штатного NTFS.SYS, эмулирующая необходимое окружение и диспетчеризующая файловые запросы. С одной стороны это хорошо тем, что мы имеем полноценную поддержку NTFS, на 100% совместимую с нашей версией операционной системы (NTFS.SYS извлекается как раз оттуда), в то время как драйвера сторонних производителей (и в частности драйвер LINIX'a) реально работают лишь на чтение, да и то кое-как (потоки и прочие "вкусности" NTFS начисто игнорируются). С другой стороны, если порушенный диск завешивает NTFS.SYS, он завесит и Руссиновича! Однако, с такими проблемами приходится сталкиваться не так уж и часто, поэтому полезность этой утилиты воистину неоценима. Демонстрационная копия NTFSDOS Profrssional, доступная для бесплатного скачивания (http://www.sysinternals.com/files/NTFSProR.exe), поддерживает лишь чтение NTFS-дисков, а за

возможность записи приходится платить (несите свои денежки на http://www.winternals.com – платный вариант www.sysitnernals.com).. Впрочем, поскольку NTSFDOS Professional всего лишь обертка, после небольшой доработки напильником она с готовностью соглашается и читать, и писать. (Внимание! Никто не говорит о взломе! Мы ничего не ломаем! Напротив, мы создаем, наращивая функциональность программы!). Кратко об установке и сопутствующих проблемах. Для начала вам потребуется создать системную дискету, что легче всего осуществить средствами Windows 98. Русская версия MS-DOS даже в минимальном комплекте поставки (io.sys + command.com) занимает намного больше места, чем рассчитывал Руссинович и NTFSDOS Professional на стандартную 3" дискету уже не вмещается. Поэтому, приходится устанавливать NTFSDOS Professional на чистую диску (точнее говоря, инсталлятор создает таких дисков два – на первый помещает NTFS-драйвер, а на второй – chkdsk.exe). Загрузившись с системной дискеты, выньте ее из дисковода (естественно, command.com должен быть предварительно скопирован на виртуальный диск), вставьте первый диск, сформированный инсталлятором и наберите в командной строке NTFSPRO.EXE.

Как вариант можно воспользоваться загрузочным диском от компании **Active@Data Recovery Software** (http://download2.lsoft.net/NtfsFloppySetup.exe) или загрузочным CD-ROM диском от нее же (http://download2.lsoft.net/boot-cd-iso.zip). Центральным звеном каждого из них является независимый NTFS-драйвер, работающий из под MS-DOS и монтирующий NTFS тома даже при полном разрушении вспомогательных файловых структур и серьезном повреждении таблицы MFT и полном разрушении корневого каталога. Драйвер самостоятельно сканирует диск в поисках уцелевших записей в MFT, показывая в том числе и удаленные файлы, предлагая их восстановить. Естественно, возможность записи на диск реализована только в коммерческой версии, а демонстрационная позволяет лишь скопировать файлы на внешний носитель (жесткий диск, размеченный под FAT, или дискету). Динамические диски, к сожалению, не поддерживаются. Помимо этого в комплект входит утилита для создания/восстановления образом диска, средство избавления диска от данных (полезно когда вы сдаете диск с конфиденциальными данными назад продавцу), программу для работы с патрициями[1] (восстановление разрушенных таблиц разделов и их заблаговременная архивация), и автономный энурез – утилиту unerase для NTFS.

Если приобретение второго жесткого диска вам не по карману, а возможности MS-DOS загрузчиков вас не устаивают, воспользуйтесь другой утилитой Марка Руссиновичка – **ERD Commander'ом**, позволяющим запускать усеченную версию Windows с дискет (5 штук) или CD-диска. В настоящее время ERD Commander распространяется только на коммерческом основании, хотя в сети до сих пор можно найти предыдущие, бесплатные версии, хотя их функциональные возможности весьма ограничены. В частности, опробованный мной EDR Commander 2000 вызывал смесь разочарования с удивлением. Во-первых, он забросил на дискету многопроцессорное ядро (а у меня однопроцессорная машина!). Как следствие, при загрузке с дискеты Windows не нашла нужного ядра и умерла еще в зачатье. Пришлось менять ядро вручную. Затем всплыли и другие ошибки инсталлятора и пришлось немало попотеть, прежде чем Windows все-таки загрузилась. Подготовленный инсталлятором образ CD-ROM'а так же был в сильно разобранном стоянии – просто папка с файлами и bootsector.bin, который еще не каждой утилитой прожжешь (я пользовался CDRTOOLS, так же подходит и CDRWIN, а вот популярный Нерон, сжигающий Рим, для этой цели увы, не пригоден). Тем не менее, ERD Commander стоит всех мучений! С его помощью вы можете: менять администраторский пароль в системе, редактировать реестр упавшей системы, управлять сервисами и драйверами, восстанавливать удаленные файлы, копировать и модифицировать любые системные и пользовательские файлы (в том числе и по сети), редактировать таблицу разделов и управлять динамическими дисками, сравнивать файлы упавшей и рабочей системы, производить откат системы в рабочее состояние и многое-многое другое. К сожалению, непосредственными средствами для восстановления разрушенного диска ERD Commander не располагает и в основном он применим для реанимации операционной системы (правда, из под ERD Commander'а вы можете вызвать дискового доктора или любую другую Windows-утилиту, в таком случае никакого смысла в его приобретении нет – второй винчестер будет дешевле).

Начиная с Windows 2000, Microsoft наконец-то включила в операционную систему некоторую пародию на загрузчик, способную стартовать с CD-ROM и поддерживающую NTFS. Называется эта штука ***Консоль Восстановления*** или по-английски ***Recovery Console***. Это

[1] английское partition (раздел) в русской транскрипции, изначально произносилось как "партитио" и "патриция", но затем язык это переварил в более благозвучную и легко выговариваемую "патрицию".

действительно консоль, ничего не знающая о GUI и способная запускать только консольные приложения (типа chkdsk.exe и подобных им). Для ее активации загрузитесь с дистрибутивного CD-ROM и сделайте вид, что хотите переустановить систему, но на определенном этапе установки нажмите <R> для вызова консоли восстановления. Вас запросят пароль администратора (если вы его забыли или системный реестр поврежден войти в консоль не удастся!), при успешной регистрации запуститься командный интерпретатор, позволяющий (теоретически!) скопировать уцелевшие файлы на другой диск. Практически же по умолчанию доступа только папка WINNT, причем копирование на съемные носители запрещено. Хорошенькое начало! Вам нужна WINNT? Личные документы намного нужнее! К счастью, доступ можно разблокировать. Для этого необходимо присвоить системным переменным AllowAllPaths и AllowRemovableMedia значение true ("SET AllowAllPaths = true", "SET AllowRemovableMedia = true"), или локальных параметрах безопасности" (папка Администрирование в Панели Управления) заблаговременно найти пункт "Консоль восстановления: разрешить копирование дискет и доступ ко всем папкам" и перевести рубильник во включенное состояние. Смысл этой защиты не совсем понятен. Простые пользователи до консоли восстановления все равно не дотянуться, а профессионалов подобные манипуляции ужасно раздражают. Находясь в консоли восстановления вы можете: запускать chkdsk[2], создавать и удалять разделы на жестком диске, перезаписывать главную запись и boot-record, форматировать логические диски, управлять службами и драйверами, удалять/копировать/переименовывать/изменять атрибуты файлов (включая те, что блокируются при запуске системы), а так же выполнять другие сервисные операции. При желании вы можете запускать и свои собственные консольные приложения, при условии, что они не используют никаких динамических библиотек за исключением NTDLL.DLL, однако, технику их создания мы обсудим как ни будь в другой раз, т. к. это очень обширный вопрос.

В Windows XP идея консоли восстановления получила дальнейшее развитие, в конце концов вылившееся в **Windows PE**. Это – слегка усеченная версия Windows XP, способная грузиться с CD-ROM и запускать GUI-приложения. Фактически она полностью заменят собой "второй" жесткий диск и для восстановления системы теперь не требуется никакого дополнительного оборудования! Несмотря на то, что легальная версия Windows PE в широкую продажу так и не поступала (Microsoft предоставляет ее только разработчикам оборудования, сервисным специалистам и прочим своим корешам), в России копию оригинального диска Windows PE можно найти в каждом ларьке. Пиратство пиратством, но то, что спрос рождает предложение – факт, а загружать Windows с диска требуется многим. Если же вы связаны лицензионными ограничениями, диктуемыми уставом вашей фирмы, воспользуйтесь **Bart's PE Builder'ом**. Эта бесплатно распространяемая утилита (http://www.danilpremgi.com/nu2/pebuilder3032.zip) вытащит с дистрьбютивного диска обыкновенной Windows все необходимые файлы и автоматически сформирует iso-образ загрузочного CD. Прожигаете его на болванку и все! При желании вы можете помещать на CD и свои собственные утилиты, формируя приличную аптечку для восстановления умерших дисков и размещающуюся на 3" CR-R/RW, свободно умещающимся в нагрудном кармане. И не зачем таскать эти жуткие стопки дискет или страшно сказать – отдельный винчестер. К слову сказать, к Bart's PE Builder'у выпущено множество плагинов, представляющих собой программы, адоптированные для запуска с CD. Среди них есть и утилиты восстановления данных, и дисковые редакторы, и даже Nero Brining Rom. Большую коллекцию плагинов можно найти на домашней страничке Bart'a – http://www.nu2.nu/pebuilder/ здесь же вы найдете и краткое руководство по работе с PE Builder'ом. Официально PE Builder поддерживает Windows 2000, Windows XP и Windows 2003, однако, при ближайшем рассмотрении выясняется что ему как минимум нужен Windows 2000 с интегрированным SP1, зато создание диска на базе Windows 2003 прошло успешно (использовался CD-ROM с 180-дневной версией Windows 200 Server, бесплатно распространяемый компаний Microsoft).

Рисунок 1 логотип диска Bart's PE

выбор носителей для копирования

Времена, когда восстанавливаемый винчестер было можно скопировать на пару пачек дискет, давно прошли и теперь процедура спасения данных значительно усложнилась. Пишущие приводы (особенно DVD) – хороший выбор и пара пачек болванок вмещает в себя

[2] полезность которого, кстати говоря, весьма сомнительна, т. к. он зачастую лишь усугубляет разрушения

жесткий диск любой разумной емкости, однако достойных программ прожига под MS-DOS нет и по-видимому уже и не будет. Существующие утилиты (включая их консольные разновидности!) требуют для своего запуска Windows PE/Bart PE, который не в состоянии монтировать разрушенные NTFS-диски (на некоторых из них NTFS-драйвер просто виснет или уходит в голубой экран).

Штатная же консоль восстановления, NTFSDOS Proffessional и Active@ Data Recovery Boot Disk поддерживают только дискеты и IDE-накопители, причем демонстрационные версии двух последних требуют, чтобы диск-приемник был размечены под FAT16/32, а его максимальный объем не превышал 8 Гбайт. Если же вам необходимо восстановить диск большего объема – последовательно копируйте его на несколько жестких дисков. Согласен, это достаточно дорогое удовольствие, но дешевых решений в деле восстановления данных не бывает.

редактор диска

Настоящие профессионалы восстанавливают разрушенные логические структуры непосредственно в дисковом редакторе, не доверяя никаким автоматизированным утилитам (кроме своих собственных), поскольку никогда не известно наперед, какой подлости от них следует ждать. Так будем поступать и мы, делая основной упор именно на ручном восстановлении. Коль скоро дисковый редактор станет нашим главным инструментом, это должен быть хороший и комфортный редактор, в противном случае, восстановление из увлекательной работы превратится в пытку.

Лучшим, и кстати говоря до сих пор никем не превзойденным, дисковым редактором, когда-либо созданным за всю историю существования IBM PC, был и остается знаменитый **Norton DiskEditor** от компании Symantec. Удобная навигация по диску, просмотр большинства служебных структур в естественном виде, мощный контекстный поиск до предела упростили процедуру восстановления, взяв всю рутинную работу на себя. Старичок и поныне остается в строю. Естественно, под Windows NT он не запускается, однако, работает под MS-DOS и Windows 9x, наследуя все ограничения, накладываемые BIOS'ом на предельно допустимый объем диска в 8 Гбайт (правда, попытка восстановление диска из многозадачной среды, коей и является Winnows 9x, могут носить диаметрально противоположный характер, впрочем, на NTFS-разделы это условие не распространяется. Windows 9x не поддерживает NTFS и ничего не пишет на ее разделы). К сожалению, DiskEdit ничего не знает об NTFS и потому разбирать все структуры приходится вручную. Но еще пол-беды. DiskEdit'or не умеет работать с UNICODE, а это уже хуже. Поэтому, лучше выбрать другой редактор.

Рисунок 2 Disk Editor отображает FAT

Рисунок 3 Disk Editor отображает корневую директорию

Microsoft DiskProbe, входящий в состав бесплатно распространяемого пакета Support Tools, это незатейливый и довольно неудобный в использовании дисковый редактор. Если все, что вам нужно – это подправить пару байт в нужных секторах, Disk Probe вполне подойдет, но для восстановления серьезных разрушений он непригоден. Тем менее, базовые функции редактирования им поддерживаются – чтение (запись) логических/физических секторов и групп, просмотр Partition Table, FAT16 и NTFS boot-секторов в естественном виде, поддержка UNICODE, глобальный поиск по фиксированному/произвольному смещению строки от начала сектора, запись/восстановление секторов в/из файла и т. д. Основная претензия – отсутствие горячих клавиш и невозможность перехода к следующему сектору по PagePown (для каждого сектора приходится лезть в меню, что ужасно напрягает).

Рисунок 4 Disk Probe за поиском сектора

Рисунок 5 Disk Probe отображает Partition Table

Acronis DiskEditor – слегка улучшенный клон Disk Probe. Разукрашен интерфейс, существенно упрощена процедура выбора дисков, по PageDown/PageUp переходит к следующему/предыдущему сектору. В поиске появилась поддержка большого количества различных кодировок (DiskProbe понимает только Cyrillic Windows-1251), и HEX-поиск. Но есть и упущения. При масштабировании окна меняется и количество байт в строке, что делает навигацию по сектору весьма противоречивой и затруднительной, к тому же текущая позиция

курсора отображается только в десятичном виде (у DiskProbe – в шестнадцатеричном), что так же не добавляет восторга.

Рисунок 6 Acronis DiskEditor за поиском строки

Рисунок 7 Acronis DiskEditor отображает NTFS boot-сектор

DiskExplorer от Runtime Software – великолепный дисковый редактор, самый лучший из всех с которыми мне только доводилось работать. Фактически это клон Norton DiskEditor под Windows NT/9x с полной поддержкой NTFS. Вы можете просматривать все основные NTFS-структуры в естественном виде, монтировать виртуальные диски, работать с образами лазерных и жестких дисков, перемещаться по директориям, восстанавливать удаленные файлы из любой записи MFT, копировать файлы (и даже целые директории!) с предварительным предпросмотром в текстовом или шестнадцатеричном формате и это еще далеко не все! Удобная система forward/backward навигации (приблизительно такая же как в браузере или IDA PRO, даже гиперссылки поддерживаются), изобилие горячих клавиш, история переходов, мощный поиск с поддержкой основных структур (INDEX, MFT, Partition), поиск ссылок на текущий сектор, возможность удаленного восстановления диска с подключением по TCP/IP, локальной сети или прямому кабельному подсоединению. Все числа выводятся в двух системах исчисления – шестнадцатеричной и десятичной.

Короче говоря, это мой основной (и при том горячо любимый!) инструмент для исследования файловой системы и восстановления данных. Первое же знакомство с ним вызывает эйфорию, граничащую со щенячьим восторгом. Наконец-то мы получили то, о чем так долго мечтали. Естественно, за все хорошее надо платить. Disk Explorer это коммерческий продукт, а доступная для скачивания демонстрационная версия лишена возможности записи на диск. Причем, имеются две различные версии редактора: одна поддерживает NTFS (http://www.runtime.org/gdbnt.zip), другая – FAT. Так же доступны плагины под Bart's PE, которые можно скачать с сайта Runtime Software.

Рисунок 8 DiskExplorer отображает MFT в сокращенном виде

Рисунок 9 DiskExplorer отображает MFT в расширенном виде

Sector Inspector, входящий в бесплатно распространяемый фирмой Microsoft пакет "Windows Resource Kits", представляет собой не интерактивный утилиту для чтения/записи отдельных секторов в файл. Поддерживает LBA и CHS адресацию. При запуске без параметров выводит декодированную partition table вместе с расширенными разделами и boot-секторами. Редактирование диска осуществляется правкой секторного дампа в любом подходящем HEX-редакторе с последующей записью исправленной версии на диск. Естественно, это непроизводительно и неудобно, однако, Sector Inspector единственный известный мне редактор, поддерживающий работу из Recovery Console, так что в некоторых случаях он бывает просто незаменим!

Рисунок 10 SectorInspector за работой

автоматизированные доктора

Более убогой утилиты, чем **ChkDsk** – стандартный дисковый "доктор", входящий в штатный комплект поставки Windows, – по-видимому не придумать даже сценаристам из Голливуда. Система диагностики ошибок упрощена до минимума – доктор лишь информирует о факте их наличия, но отказывается говорить, что именно по его мнению повреждено и что он собирается лечить, поэтому последствия такого "врачевания" могут носить фатальный характер.

Известно много случаев, когда ChkDsk залечивал до смерти полностью исправные разделы. С другой стороны, успешно проведенных операций восстановления на его счету намного больше. Обычно он используется неквалифицированными пользователями (и администраторами) для периодической проверки разделов и исправления мелких искажений файловой системы.

Рисунок 11 ChkDsk за работой

GetDataBack от создателя Disk Explorer'a. Полная автоматизация и никакой ручной работы. Сканирует MFT и выводит все файлы, которые только удалось найти (включая удаленные), рассовывая их по директориям (при условии, что соответствующие индексы не

повреждены). Если споткнется о BAD-сектор – вылетит не прощаясь. Зато поддерживает удаленное восстановление, создание образов дисков, и мощную систему поиска по файлам (дата/размер), но почему-то нет поиска по содержимому, что не есть хорошо. Допустим, вы хотите восстановить файл со своей диссертацией ключевые слова которой вам известны, а вот в каких секторах они располагаются – не ведомо. Тоже самое относится и к поиску файла записной книжки с телефоном приятеля. Тем не менее, для большинства рядовых задач по восстановлению, возможностей GetDataBack'a хватает с лихвой. Демонстрационную версию программы под NTFS можно раздобыть по адресу (http://www.runtime.org/gdbnt.zip). Она все показывает, но восстанавливать ничего не дает. Однако, позволяет открывать файлы ассоциированным с ними приложениями. Важно отметить, GetDataBack не является доктором, таким как NDD или ChkDsk. Она не лечит разделы, а всего лишь позволяет скопировать из них уцелевшие файлы.

Рисунок 12 внешний вид GetDataBack

DIY Recover от нидерландской фирмы с неоригинальным названием Data Recovery – замечательный полуавтоматический доктор с кучей настроек. Поддерживает динамические диски, позволяет задавать все параметры сканирования вручную. Надежен. Не зависает даже на сильно поврежденных томах. Правда, навигация по восстанавливаемому диску выполнена крайне неудобно (если не сказать – небрежно), что особенно хорошо заметно на больших дисках, содержащих миллионы файлов. Как и его соперник – GetDataBack – он ничего не лечит, а лишь вытягивает уцелевшие данные из небытия. Тем не менее, я отношу DIY Recover к лучшим автоматизированным средствам восстановления из всех имеющихся в моем арсенале (не считая своих собственных утилит, которые пишутся на скорую руку для восстановления конкретного диска, после чего уходят в /dev/null, как и всякий фаст фуд). Демонстрационную копию программы можно найти по следующему адресу http://www.diydatarecovery.nl/~tkuurstra/downloads/Demo/iRecoverSetup.exe.

Рисунок 13 ползущая змейка DIY Recover'a

Easy Recovery Professional от OnTrack Data Recovery (www.ontrack.com) – симпатичный, но на проверку довольно бестолковый инструмент, к тому же работающий полностью в автоматическом режиме, интеллектуальность которого находится на зачаточном уровне. Не рекомендуется для использования (ну разве что вы хотите восстановить только что отформатированный том на который еще ничего существенного не писалось).

Рисунок 14 EasyRecovery и полтораста мегабайт косметики

заключение

В шутку говорят, что всякий обладатель не зарезервированных данных ошибается лишь дважды – первый раз, когда теряет их и второй – когда запускает DiskEditor. Действительно, восстановления данных – чрезвычайно ответственная операция и одно неверное движение мыши способно отправить ваш дисковый том к праотцам. Редактор диска – это не та программа, которую можно осваивать на лету. Подключите к компьютеру жесткий диск, не содержащий ничего интересного, и тренируйтесь! Как раз успеете к следующему номеру оторвать у мыши хвост и стучать по горячим клавишам вслепую, после чего будет не грех поговорить о восстановлении загрузочных областей (таблиц разделов, boot-секторов) на обычных и динамических дисках, так же называемых программными RAID массивами.