



Восстановление данных

«Скорая помощь» для Винчестера

Одни их уважают и буквально молятся на них, другие — ненавидят. Они могут спасти фирму от банкротства или «посодействовать» преступнику попасть за решетку. «Они» — это профессионалы в вопросах восстановления информации с «умерших» винчестеров, работу которых часто сравнивают с работой врачей.

В Британии существует авиационная служба Avimed, которая специализируется на оказании амбулаторной и неотложной помощи тяжелобольным и пострадавшим в катастрофах. Самолеты и вертолеты этой службы доставляют врачей к больным, но иногда на их борту оказываются не совсем обычные доктора и их пациенты. В экстренных случаях к помощи медицинской авиации прибегают специалисты крупнейшей британской фирмы Vagon, специализирующейся на восстановлении данных с поврежденных жестких дисков. Эти компьютерные «врачи» доставляют по воздуху своих «пациентов» в лабораторию,

чтобы незамедлительно приступить к спасению информации. Ведь в наше время, как известно, информация стоит очень дорого: потерянная база данных по клиентам или уничтоженный бухгалтерский учет могут принести серьезные убытки и даже поставить под вопрос существование фирмы. Показательный случай произошел в Германии, когда специалисты из немецкого филиала Vagon спасли массив информации одного из правительственных учреждений ФРГ объемом в 200 Гбайт. Впрочем, какие-либо подробности о своих клиентах летающие доктора не приводят, ссылаясь на «врачебную тайну».

» Клинический случай

Как правило, при восстановлении утраченной информации шансы на успех у специалистов из Vopon достаточно велики — помочь клиентам удается в 80% случаев, а если восстанавливается ленточный носитель, то вероятность повышается до 90%. Опыт сотрудников фирмы показывает, что главным виновником краха винчестера в большинстве случаев является сам пользователь. Почти половина «клинических случаев» — это по ошибке стертые или переписанные файлы, а также форматирование диска. Бывает, что и системный администратор сам перемудрит с «откатами». Около 20% приходится на брак в самом «железе» и еще 20 — на сбои в работе программного обеспечения. Остальные примерно 10% случаев утраты важных данных — это аварии, не связанные с компьютерной техникой: пожары, затопления помещений водой, механические повреждения.

Пожар, как правило, приводит к полной потере информации, имевшейся на винчестере. Теоретически можно попытаться извлечь хоть что-то из обуглившегося «винта», если только не начал плавиться магнитный слой дисков. Но это только теоретически. На практике же размагничивание и утрата данных происходит еще раньше. Однако хуже огня зачастую бывают самостоятельные попытки «юзеров» восстановить винчестер с помощью разного рода программ. После их неудавшейся «работы» шансы профессионалов близки к нулю, хотя методика их уже отработана и достаточно эффективна.



Профилактика

- ▶ Выполнять резервное копирование: крах носителя может иметь фатальные последствия, если не работает функция резервного копирования. «Профи» советуют регулярно резервировать критичную информацию на ленточных либо магнитооптических накопителях. Полагаться лишь на дискеты, винчестер и CD-диски не стоит.
- ▶ Периодически сохранять образ диска: сохранение образа диска с помощью Powerquest Drive Image или Norton Ghost может облегчить восстановление всей системы.
- ▶ Сохранять отдельно таблицу разделов: это позволит успешнее реконструировать содержимое винчестера.
- ▶ Внимательно отслеживать признаки надвигающейся катастрофы: частые «падения» системы говорят о наличии большого количества сбойных секторов и близкого краха всего винчестера.

Для того чтобы «процесс пошел», бывает достаточно запустить умерший винчестер всего один раз. Тогда «доктора» получают образ диска, переносят его на исправный винчестер, с которым и работают в дальнейшем. Рука об руку трудятся программисты, математики, электротехники.

Хирургия

Порядок дальнейших действий зависит от того, что же произошло с «пациентом». Для начала нужно заставить жесткий диск вращаться. Если дефект кроется в электронике или в электродвигателе, то перспективы работы спасателей самые благоприятные. Гораздо хуже обстоит дело, если обломившийся блок головок прочертил по всем дискам глубокую царапину. Затем доктора подступают к самим файлам: создается образ диска и информация переносится строго так, как она располагается на «умершем» винчестере, — сектор за сектором, бит за битом — вместе с вирусами, если те имеются. После этого

специалисты выносят свой вердикт о том, можно ли спасти данные или нет.

Для своей работы спасатели имеют, наверное, больше всяческих запчастей, чем все производители вместе взятые. Это нужно для того, чтобы «оживить» винчестер и не потерять то, что на нем еще осталось. В ряде случаев требуется замена всей электронной схемы винчестера или головок. Поэтому «коллекция» винчестеров и других приводов является наряду с know-how фирмы ее основным капиталом. Постоянная ускоряющаяся смена технологий, а также незначительные различия между моделями внутри одной серии не позволяют докторам иметь полную коллекцию «донорских органов» для своих «пациентов». Поэтому иногда приходится закупать необходимое там, »

▼ Тонкая работа: юстировка или замена головок электронной системы может «привести в чувство» жесткий диск

▼ «Хирург» за работой: вскрытие винчестера производится в стерильных условиях, когда отсутствует не только пыль, но и статическое электричество





▲ «Хирургический» инструмент: чтобы заставить диски вращаться, может пригодиться все — от палочки с ваткой до пассатижей



▲ Лаборатория «спасателей»: там за стеклом идет работа по спасению того, что еще можно спасти

» где оно есть, — в любой точке мира.

Свою работу с винчестером специалисты сравнивают с открытым массажем сердца, когда одно неверное движение — и случится непоправимое. Концентрированный опыт и умение «докторов» имеют свою цену. Нижняя граница стоимости работ по восстановлению данных лежит в районе \$750, а верхняя зависит от сложности работы и затраченного времени. Бывает, что гонорары выражаются шестизначными числами.

Реанимация

После того как остатки данных сохранены, производится анализ их структуры. Чтобы восстановить файл, его приходится собирать по кускам. Качество работы зависит от того, сколько фрагментов собираемого файла доступны. К сожалению, возможности даже самых высококлассных специалистов не безграничны. Совсем просто им работать, когда информация стёрта умышленно (например, преступником, заматающим

следы). По словам самих специалистов, программы, гарантирующие «безвозвратное» уничтожение файлов, часто не стоят тех денег, которые за них просят создатели. Восстанавливается стёртая информация, как правило, даже быстрее, чем «стирается». Вот почему в целом ряде случаев клиентами этих «реаниматоров» становятся прокуроры и налоговые полицейские, которым не требуется информация в полном объеме.

»



От редакции

Восстановление по-русски: надежда умирает последней

К сожалению, фирмы, подобные Vogon, — большая редкость, и если вы думаете, что винчестер, упавший со второго этажа, вам отремонтируют в соседнем офисе, то вы заблуждаетесь. Например, в Москве это сделать практически невозможно. Фактически возможно восстановление данных только на логическом уровне. Хотя такие работы, как замена контроллера и пластин, проводятся, при серьезном повреждении поверхности пластины восстановить информацию практически не удастся. Как правило, «скорая помощь» в России — это подразделение крупных поставщиков компьютерной техники, которые параллельно с основными задачами предоставляют некоторые услуги своим клиентам.

Но выход все же есть. Аналогичная фирме Vogon «скорая помощь» существует и в России: это фирма SoftJoys, расположенная в Санкт-Петербурге, опыт которой в этой области насчитывает уже 7 лет. Мы поговорили с начальником службы ремонта Михаилом Артемьевым, который работает в этом отделе со дня его основания.

Какие реальные возможности по физическому и логическому восстановлению информации вы предоставляете своим клиентам?

К нашим клиентам относятся как частные лица, так и крупные организации. Мы восстанавливаем диски и дисковые массивы с разрушенной файловой системой (самые распространенные — FAT 12, FAT 16, FAT 32, NTFS, UFS, разделы Novell). Это могут быть IDE- или SCSI-диски, RAID-массивы, диски с разрушенной служебной областью (этим страдают диски фирм Fujitsu и Quantum); информацию с дисков, у которых разрушен транслятор (при этом нарушается структура файловой системы, и никакие средства, кроме нашей методики, не позволяют восстановить информацию с них).

Мы имеем опыт восстановления дисков, залитых водой, а также из компьютеров, горевших в пожарах, со смещением пакета пластин и повреждением головок, с оборванными обмотками двигателя шпинделя, оторванными и поврежденными головками. Все варианты перечислить просто невоз-

можно — и чего только с дисками не происходит...

Какое вы используете оборудование?

Есть обычные инструменты — паяльники, фены. Есть специфические стоматологические инструменты. Есть узкоспециальные — съемники головок, например. Используется чистая зона с поддувом воздуха через фильтр.

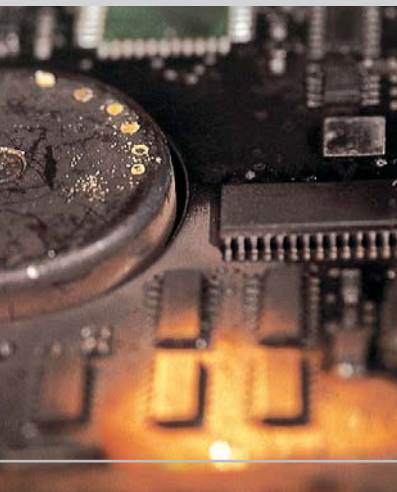
Мы имеем в коллекции несколько тысяч накопителей различной емкости от совсем древних до самых современных моделей. У нас есть специальные программы, в том числе написанные нами, которые позволяют работать как с файловыми системами, так и с накопителями в технологических режимах.

Существует ли у вас «чистая комната» и спецодежда для персонала?

Это отдельное помещение, в котором находится чистая зона, там проводятся только



Михаил Артемьев, компания SoftJoys



▲ **Жертва пожара:** если воздействие температуры не было продолжительным — есть шанс



▲ **Склад запасных частей:** самые разные дисководы (справа) и винчестеры самых различных моделей (слева) — это тоже капитал



» Одним из таких случаев стало участие фирмы Vogon в разоблачении одного врача, который после смерти своих пациентов еще длительное время использовал в своих интересах данные этих мертвых душ. Еще одна острая тема, где специалисты из Vogon помогают правосудию, — детская порнография. Метод, применяемый для выявления коллекционеров запрещенной «эротики», таков: сначала вычисляются и запоминаются контрольные суммы файлов

соответствующих изображений, курсирующих в Интернете, которые могли быть сохранены на винчестер подозреваемого. Если потом выявляется характерная контрольная сумма, то назначается «углубленное обследование», которое и позволяет определиться с окончательным «диагнозом».

Правда, в ряде случаев специалисты вынуждены констатировать, что «медицина бессильна». Так произошло с жестким дис-

ком, изъятым по делу о даче взяток и подкупе целого ряда правительственных чиновников неким Карлхайнцем Шрайбером — торговцем оружием. Так получилось, что исчезла не только информация с носителя, но и сам винчестер бесследно «испарился» по дороге в лабораторию. Впрочем, как говорится, «... это уже совсем другая история». **СНИП**



▶ работы в гермозонах дисков. Практика показывает, что для восстановления данных этого вполне достаточно. Мы перебирали там диски емкостью до 60 Гбайт с несколькими пластинами по 20 Гбайт на каждую. На самом деле плотность записи играет роль только при юстировке блина. То есть, если его сняли и переставили на другой шпиндель. Во всех остальных случаях это практически не играет никакой роли. А вот количество пластин играет большую роль.

Каков процент удачного восстановления информации и сколько стоят ваши услуги?

Смотря от чего считать... Много простых случаев, мало сложных. В этой ситуации процент довольно велик.

К нам ежедневно поступают около 20 дисков. Восстановление информации волнует около половины клиентов. Остальных интересует ремонт.

Что называть сложным восстановлением? Пример. Мне прислали диск из Израиля, до этого его возили на «Мицубиси». Там за восстановление информации с клиента попросили \$4000. При этом диск разобрали, и гермозону в том числе, то есть сняли крыш-

ку. К нам он попал именно в таком разобранном виде, в кульке. На самом деле у диска был просто неисправен контроллер, разбирать гермозону не требовалось. Мы поставили исправный контроллер и прочитали диск полностью. Клиент заплатил \$100. И то это было обусловлено таможенными заморочками и пересылкой. За такую работу мы берем обычно \$10. Я бы не назвал это сложным восстановлением, но коллеги из «Мицубиси» считали иначе.

Для нас сложность работы определяется исключительно трудоемкостью. Обычно цена восстановления не превышает \$1000. И такие деньги берутся в сложных случаях, когда это касается корпоративного сервера большого объема, выполненного в виде RAID-массива, при разрушении более чем одного диска и с нарушениями файловой системы. Даже в случае разрушения поверхности диска, когда требуется замена головок, юстировка блинов и пр., стоимость составляет \$200–700. В нее входит сама работа и стоимость диска-донора, которая составляет от \$50 до 250.

Сложными случаями я бы назвал достаточно неочевидные вещи, как-то: восстановление очень старого или малораспространенного

диска с механическими повреждениями или неисправным контроллером, некоторые нарушения логики диска, особенно когда это касается какой-нибудь экзотической файловой системы (как пример, случалось восстанавливать диски от игрового автомата «Покер», от принтер-станции Xerox, от АТС). Если говорить о времени, которое занимают восстановительные работы, то оно варьируется от нескольких минут до недели, все зависит от сложности. В среднем же 1–2 дня. Кроме того, я не буду утверждать, что мы можем восстановить любой диск с любой проблемой. Я просто могу сказать, что мы не можем. Мы не можем восстановить данные с диска, который имеет сильные механические разрушения в области хранения микропрограммы (firmware). Мы не восстановим данные с диска, который горел в огне, если была превышена точка Кюри, а также с искривленными пластинами. Хотя недавно был случай успешного восстановления 2,5-дюймового диска Fujitsu емкостью 30 Гбайт именно с искривленными пластинами, но я бы не стал говорить, что это можно сделать всегда.

Беседовал Антон Мокрецов