

# 数据恢复的基本知识

丢失的数据可以恢复吗?在没有得知数据丢失的原因和数据丢失之后所做的操作之前,答案是不确定的。但在绝大多数的情况下,数据丢失之后都是可以恢复的。数据恢复可以看作是一种技术,也可以看作是抢救受损数据的一个过程,甚至可以看作一个 IT 技术行业。在今天的计算机世界中,数据恢复举足轻重。

## 1、数据恢复的定义

简单地说,数据恢复就是把因各种原因丢失的数据还原。一般来说,只要介质没有严重受损,或数据没有被完全覆盖,数据就有可能被完好无损地恢复。逻辑故障造成的数据丢失,其恢复的成功率比较高;硬盘因物理损坏而无法访问时,更换发生故障的零件,即可能恢复其中的数据。但在介质严重受损或数据被覆盖情况,数据将无法恢复。

应该说,数据恢复不是一种目的,而是在万不得已的情况下的一种急救措施。数据恢复工作因专业性、数据的重要性与保密性而使其具有较大的难度,而一些特殊要求又使数据恢复工作难上加难。如遇到固件区或磁头损坏故障时,需要花大量的时间去寻找匹配的固件和磁头;在处理由于硬盘内部的磁头或电机故障而引起的数据丢失时,需要进行开盘操作,这既要有严格符合标准的无尘室,又要求操作人员的技术过硬;对于盘片严重划伤,有大量物理坏道的硬盘进行数据恢复时成功率极低等,都是比较棘手的问题。

数据恢复是出现问题之后的一种补救措施,既不是预防措施也不同于备份。所以在一些特殊情况下数据将很难被恢复,如数据被覆盖、硬盘被低格清零、磁盘盘片严重划伤等。

## 2、数据恢复的一般原则

在对硬盘中的数据进行恢复时,需要遵循一定的原则使数据恢复过程更加安全,避免造成对数据的二次伤害。

首先,需要准确判断硬盘故障,可以依据硬盘使用者在硬盘出现故障前的使用描述,再结合硬盘的故障表现以及丰富的经验综合判断;之后对故障进行分析,了解其产

生的原因,并选择解决故障的手段。采用最合理的手段来处理故障。对于硬盘相对正常的软故障,能够镜像的尽量采取镜像技术先镜像一份,镜像工具也尽可能选择 DOS 下的工具,或者先进行相应的处理后再使用 Windows 下的工具来进行处理,镜像工具必须达到 S TO S(扇区到扇区)方式来进行,当然对某些特殊的个案,还需要使用校验方式进行。

对于没有任何数据恢复操作经验的人来说,在硬盘数据出现丢失后,应立即关机,不要再对硬盘进行任何写操作,否则会增大修复的难度,也影响到修复的成功率。修复的每一步操作都应该是可逆的或者对故障硬盘是只读的,这也是很多数据恢复软件的工作原理。

另外在数据恢复之前,可以首先完成以下几个步骤:

备份当前能工作的驱动器上的所有数据。如果 C 盘损坏,那么,在开始任何工作之前首先备份 D 盘及其他盘上的数据到其他可靠的地方。

调查使用者。询问在数据丢失之前发生的事情,是否有其他的应用程序对硬盘进行过操作。

如果可能,备份所有扇区是一个不错的方法。

手头要有一个好的扇区编辑工具,如 WinNex 就是一款不错的基于扇区的编辑工具。

尽可能多地得到最后使用者的关键文件的信息。

了解完这些信息后,就该对数据恢复有一个基本的认识,如为什么会出现这个问题,破坏程度如何,什么工具能达到最好的恢复效果,其主要步骤有哪些等。

另外要记住的是:先恢复最有把握的数据,恢复一点,备份一点。

### **3、数据恢复的分类**

根据数据丢失的原因不同,对应的数据恢复方法一般分成两类,即逻辑恢复和物理恢复。

在数据存储设备能正常工作的情况下进行的数据恢复工作,称逻辑恢复。也就是说数据遭受的破坏是逻辑破坏,例如格式化、删除、重新分区等情况。逻辑恢复是数据恢复中比较常见的操作。

在数据存储设备不能正常工作的情况下进行的数据恢复工作,称物理恢复。物理恢复往往要先进行设备的修复,硬盘开盘操作就属于数据恢复中的物理恢复。物理恢复是数据恢复中非常难的一类,并且往往需要特殊的环境和辅助设备来进行操作。

### **4、数据恢复的原理**

造成数据丢失的原因多种多样,在对丢失的数据进行恢复时,相应地也要针对不同的数据丢失原因,遵循其工作原理进行数据恢复。下面对几种典型数据丢失原因进行数据恢复时的原理进行介绍。

#### 4.1、分区被格式化

造成分区被格式化的原因一般是误操作，如想格式化 C 盘，却错误地将 D 盘格式化了，或者说格式化以后才想起硬盘有重要的数据没有备份等。解决的方法一般通过网上的数据恢复工具软件等即可将数据恢复。因为格式化只不过是对分区头按照相应操作系统的需求进行逻辑簇的组织，并没有将数据真正地清除掉。所以软件可以重构此分区头，以支持数据的访问。达到恢复数据的目的。

#### 4.2、主引导扇区的分区丢失

如果主引导扇区的分区丢失，那所有分区的信息都将丢失，其原因可能是软件误操作，如一键恢复等软件将恢复特定的分区误扩展到所有分区；安装 Linux 时自动安装到全盘，将把其余分区删除；Partition Magic 也容易导致分区问题。此情况下可以采用 Active Partition Recovery 自动修复，因为尽管分区丢失，但是每一个分区的引导扇区数据还在，通过对全盘所有扇区的扫描，可以发现所有的引导扇区，以此为界定。就可将分区都找出来。

#### 4.3、数据文件删除

若数据文件被删除，可以通过 Undelete 工具恢复。因为文件是通过目录结构维护的，在目录中占用一项，而这一项有个标识为是否删除。进行数据恢复时，只要将此标识改为正常就可以了。所以，要想真正彻底破坏数据文件，只删除是不行的，需要用专门工具将此文件所占用的块字节清 0。

#### 4.4、不能启动操作系统

操作系统启动过程失败，有多种可能性。但若这时需要将硬盘中的数据读出来，可通过将此硬盘以从盘形式挂到另一系统中进行读取来解决。若是 Windows 操作系统可直接读到此盘，而对于 Linux 或 UNIX 操作系统则需要 Mount。如果

不将故障硬盘挂到另一个系统，对于 Windows 操作系统可以直接重装一个系统到另一目录，而对于 Linux 或 UNIX 操作系统可用启动光盘来启动系统，进而读取其中的数据。这是因为不能够启动系统只是操作系统的引导分区损坏或者启动关键进程错误或丢失，而存在数据区中的数据并没有丢失，只要想办法引导系统启动就可以完成数据恢复。

#### **4.5、0 柱面 0 磁道 1 扇区损坏**

若硬盘的 0 柱面 0 磁道 1 扇区损坏，则坏磁道会致使磁道外缘更容易损坏。0 柱面 0 磁道 1 扇区中存放的是主引导分区，控制着操作系统的启动，极为重要。使用 DiskGen 可以将主引导分区改为 0 柱面 1 磁道 1 扇区，借此启动硬盘，再试图做分区搜索。如果分区搜索未能成功，可以参照恢复数据文件的方法进行数据恢复。这是因为系统在启动时，先在 BIOS 中读取硬盘保留区定位主引导区。系统保留区一般位于硬盘 0 磁道前面的几十个物理磁道。写入的程序模块一般用于硬盘内部管理，如低级格式化程序、加密解密程序、自监控程序、自动修复程序等等。写入的参数近百项，如型号、系列号、容量、口令、生产厂家与生产日期、配件类型、区域分配表、缺陷表、出错记录、使用时间记录、SMART 表等，数据量从几百 KB 到几 MB 不等。

#### **4.6、硬盘高级格式化错误**

若硬盘存在严重坏道，在对其进行高级格式化时，会出现速度很慢，快结束时出现“Windows 无法完成格式化”等提示信息。

对于此类问题，可以分两种情况进行解决。如果硬盘用的数据需要保留，只能通过相关的数据恢复工具进行复制，如 data Compass 等；如果是修复硬盘，

可以用相关的专修工具进行处理，此类软件能够将硬盘中的坏道找出，并做自动修复，从而使格式化成功。

#### 4.7、硬盘磁头损坏

若硬盘受到剧烈撞击等情况，就有可能导致硬盘磁头损坏，其表现为可以听到明显的磁头抖动的声音，磁头接触到硬盘或者磨损敲盘的声音等。这是最严重的情况，只能做物理处理。通常情况下是将硬盘交给专业的数据处理公司，进行数据恢复。这些专业的数据处理公司在无尘工作室内拆开硬盘，更换损坏的对应配件，从而使得硬盘可以读写，恢复出其中的数据。



#### 4.8、固件损坏

硬盘的固件区在经过长时间的读写之后，也可能会造成数据丢失，模块损坏等问题，进而导致不能读写数据区中的数据。这类故障的恢复原理通常情况是找到同类型的硬盘固件，通过效率源、PC3000 等专业工具将其损坏的固件部分进行回写修复，启动硬盘后读取数据区的数据，达到恢复数据的目的。

注意:进行数据恢复最重要的一点是确保需要恢复的数据没有被覆盖，存储数据的介质没有被损坏，没有被人为二次破坏过；如果数据被覆盖或者存储介质损坏，则无法进行恢复。