数据恢复技术在涉案计算机侦查取证中的应用研究

王翰尧　张晟源
沈阳铁路公安局　网络安全保卫处

[摘　要]科技不断发展让人们的生活更加便利，但是与此同时也为犯罪提供了更加科技化和复杂化的手段，现实中很多刑事案件都涉及到计算机以及相关的数据。犯罪嫌疑人在犯罪过程中常常会将犯罪相关的数据损坏或者删除，数据恢复技术就会将删除和被破坏的数据进行还原和修复，以此来取证。当前数据恢复技术已经成为公安勘查取证的一种必不可少的手段，本文就数据恢复技术在涉案计算机勘查取证中的应用进行探析。

[关键词]数据恢复技术；计算机；侦查取证

引言

计算机当前在各个领域都得到了广泛的应用，甚至很多犯罪嫌疑人的犯罪活动也使用了计算机，对于这一类的犯罪活动就要加强对涉案计算机的勘查，掌握有效的电子证据。犯罪嫌疑人在犯罪完成之后为了将证据消灭，常常会删除或者格式化计算机以及计算机附属设备的数据，甚至损坏计算机。这时，公安技侦工作人员就要采取有效的手段和技术来复原和提取受到破坏的数据，掌握线索，提供有力的证据。

一、数据恢复的原理

犯罪嫌疑人为了能够毁灭证据往往会在犯罪之后将和案件相关的电子数据删除，或者直接损坏计算机设备。将相关的电子数据删除或者格式化之后，并没有将相关的电子证据永久消除，而是被新的电子数据覆盖了，所以要想将数据恢复，可以灵活应用数据恢复技术，采用相关的硬件工具或者软件工具就可以将相关的数据恢复。

（一）数据存储原理

硬盘能够存储数据需要经过一定的处理，硬盘被制作出来出厂时没有经过各种处理是无法存储数据的，而要想让硬盘能够储存数据就需要进行低级格式化，将扇区和磁道划分出来，并进行磁盘分区，也就是把硬盘的存储空间分成多个区域，各个区域相互独立。最后，硬盘还需要进行高级格式化才能存储数据，将硬盘分区之后，还要建立多个逻辑驱动器，并且各个逻辑驱动器是相互独立的，每一个逻辑驱动器分区能够指引代码的地址，这样驱动器中就可以正常引入系统，搭建文件系统就能够实现数据存储[1]。对于 Windows 操作系统来说，高级格式化会按照特定的顺序来将分区进行划分，划分为文件数据区和文件分配区，其中目录文件分配区记录了文件相关的重要属性，包括文件的大小、文件的命名以及数据所在的物理位置等，都在目录文件分配区中有所体现。硬盘实现存储功能时，整个系统会在目录文件分配区将文件的大小、文件的名字以及文件内容等记录到数据区的起始位置，并将文件的真正内容写入到数据区，从而完成数据的存储。

（二）数据删除和恢复

人们将文件删除时，往往是被删除文件对应的目录以及 FAT 项被系统修改了，文件数据区中还存有文件的相关数据，数据区占用的簇还可以存储新的数据，只要新的数据没有将该文件的数据覆盖，那么采用数据恢复硬件或者软件工具就可以恢复被删除的数据。如果操作的人员将硬盘分区格式化，那么只是文件分配表被系统删除了，而数据区中的相关数据和内容还在，采用数据恢复工具和技术就能够通过一定的途径来将已经被删除的文件扫描出来。通过文件签名能够将文件的类型检测出来，通过数据恢复技术就可以恢复数据整体或者是恢复一些零散的文件。此时分析文件系统中的文件物理删除前后的结构数据的变化，就能够得到数据删除和数据恢复的原理。

二、数据恢复的方法

（一）软件恢复：

当硬盘没有出现物理损坏时，数据被删除或者通过病毒破坏文件导致数据丢失，此时就可以通过文件恢复来扫描恢复已经删除或者丢失的数据。软件修复的过程比较简便，操作简单。

（二）硬件恢复：

硬件恢复就是指磁盘出现机械硬盘的磁盘主控制芯片损坏以及坏道等情况时，可以将替换磁盘主控制芯片或者磁道修复好，购买对应的专业设备，并结合一定的电路知识就可以获取存储的数据。

（三）其他方法：

除了硬件修复和软件修复之外，还可以通过软件自动备份的功能恢复以及云恢复来将数据恢复，其中前者通过备份文件来修复，后者是依赖于云技术，例如微软公司有一款办公软件能够将用户的文档等相关的信息上传到云端，如果本地文件被删除，只要活得用户的入口就能够下载云存储空间的数据。

三、数据恢复技术在涉案计算机侦查取证中的应用

（一）利用文件签名恢复数据

利用数据恢复软件来恢复数据时，要完全扫描数据区，并对比每一个簇的起始字节，这样就能够掌握存储数据的文件类型。无论是哪一种类型的文件签名值都是固定的十六进制，数据恢复软件中的文件特征库中存储了各种类型的签名值，在对数据区进行扫描时就可以将扫描的文件签名值和特征库中相应的数值进行对比，并最终确定文件具体的类型，例如常见的 .mp4、.xlsx 和 .docx 等，通过 Win Hex 软件都可以查找得到文件的签名值。

（二）搜索文件关键词恢复数据

犯罪分子在犯罪活动之后一般都会将和案件相关的电子数据删除，通过数据存储和删除的原理可知，存储设备相应的扇区中还存有被删除的数据，如果存入新的数据，那么这部分的数据就会被新的数据所覆盖，这样就导致电子证据变得不完整，是通过碎片的形式存在的，在存储设备的不同位置分布[2]。正是因为数据是零散的，所以通过数据恢复软件也很难得到完整的原始数据，这时就可以通过搜索文件关键词来从数据碎片中得到一些和案件相关的重要的证据和线索。在磁盘数据区中采用 Win Hex 软件搜索关键词，并提取搜索得到数据，就能够得到比较完整的数据。在涉案计算机的侦查取证中，只有得到案件相关的关键词就可以采用文件关键词搜索法来恢复数据，得到比较完整的信息。

四、结语

在当前信息化的大背景下，涉及到计算机的犯罪案件越来越常见，如果犯罪分子将案件相关的数据删除或者破坏，公安技侦工作人员就可以灵活应用数据恢复技术来将被删除的数据恢复，结合各种数据恢复软件和数据恢复技术来对文件系统结构和案件的性质进行深入分析，得到对应的数据来为案件提供线索和证据。

参考文献

[1]吴汉勇，陆克思佳，田一粟，等．涉案计算机的数据恢复与侦查取证[J]．湖北警官学院学报，2015，028(009):41-44.

[2]张远桂．计算机犯罪取证中数据恢复的应用分析[J]．数字化用户，2018，024(041):124.