**数据恢复技术**

**摘要**

“任何技术都倾向于创造一个新的人类环境” 。在当今信息社会, 信息成为重要的战略资源,信息化的水平已成为衡量一个国家现代化综合国力的重要标志。然而,人们享受信息网络所带来的巨大利益的同时,计算机犯罪也成为一个普遍的国际性问题,计算机犯罪的案例增多,使各国计算机系统面临很大威胁, 计算机数据安全也成为一个永恒的话题。数据恢复技术被广泛应用到计算机取证中。在利用计算机取证过程中, 扩大对证据的收集和使用的相关证据的特殊性, 以保证客观,合法, 需要取证者深入了解硬盘结构与存储原理,且有责任担当精神, 实事求是。

**关键字**:取证,硬盘,数据恢复,责任担当

**一** 、**计算机取证遵循原则**

计算机通过取证得到电子证据, 必须严格按照程序, 以扩大对证据的收集和使用的相关证据的特殊性。且需遵循以下原则:

**1、客观性** 首先要有认真严谨的科学态度。证据收集人员要能够娴熟运用技术,取证过程中,得到的数据要真实客观,确保证据不被破坏,而且要删除干扰信息和伪造数据。不仅要收集证明犯罪嫌疑人的有罪证据, 也必须保存可以证明犯罪嫌疑人没有罪的证据证明。

**2、关联性** 只有与案件有关的信息和数据, 才能在收集证据的范围之内, 必须确保证据的连续性, 使所有证据形成证据链。在证据提交到法院时, 必须证明证据是最初的原始状态。所有的整个检查、收集证据的一切过程中, 必须要严格实施标准化, 以确保所有证据向法院提交不能够发生改变, 并一定要制定非常严格的保管转移, 检验系统。

**3、合法性** 必须建立法律, 法规的意识, 计算机犯罪证据收集的主体, 一定要通过合法的手段和合法措施, 提取证据的收集, 整个取证过程中, 必须依法受到适当监督和依照法定程序。分析出的证据必须确任、可靠、充分, 能够确定案件的性质, 只有这样, 才能做到正确而且有针对性地打击违法犯罪行为, 而且依法保护公民的合法权利和利益。

**二**、**硬盘结构及存储原理**

**1、硬盘结构**

硬盘一般分成主引导扇区、操作系统引导扇区、文件分配表、目录区和数据区5部分,其中只有主引导扇区是唯一的, 其它随硬盘分区的数目增加而增加。

**(1).主引导扇区**  硬盘的第一个扇区为主引导扇区，位于整个硬盘的0磁头、0柱、1扇区，包括硬盘主引导记录MBR和分区表DPT。主引导记录的作用是检查分区表是否正确以及确定哪个分区为引导分区，并在程序结束时把该分区的启动程序（即操作系统引导扇区）调入内存加以执行。分区表以80H或00H为开始标志，以55AAH为结束标志，共64字节，位于本扇区最末端。

**(2).操作系统引导扇区**

操作系统引导扇区OBR，通常位于硬盘的0磁道1柱面1扇区, (对于以多重引导方式启动的系统则位于相应的主分区/扩展分区的第一个扇区），是操作系统可直接访问的第一个扇区，包括一个引导程序和一个被称为BPB的本分区参数记录表。

**(3).文件分配表** 文件分配表FAT用来记录文件所在位置的表格。若丢失文件分配表，硬盘上的数据则因无法定位而不能使用。常见文件系统有FAT16、FAT32、NTFS。

**(4).目录区** 目录区DIR 紧跟在第二个FAT表之后, 记录着每个文件/目录的起始单元、文件的属性等。定位文件时操作系统根据DIR的起始单元,结合FAT表就可以知道文件在磁盘中的具体位置及大小。

**(5).数据区** 存放文件的实际区域。数据区占据了硬盘的绝大部分空间，整个数据区被分成若干簇，簇的大小和数据区的大小以及FAT表项的数目有关。但若无以上的各个部分,存储在硬盘上仅为是一些无用的二进制代码。

**2．硬盘数据存储原理**

向硬盘中写人文件时，操作系统首先在DIR区存储文件的相关信息，然后在数据区的空白区域写入文件具体内容，并在FAT表项中记录文件占用数据区相关簇的信息，最后将文件在数据区的起始位置写入DIR区，完成文件的写入。 Windows系统中，对文件进行删除时，并没有对数据区实际存储的文件内容进行擦除操作，只是在DIR表中做了删除标记，即将目录区中该文件的第一个字符改为E5，在FAT中将文件占用各簇表项清0，表示删除。

**三、数据恢复技术**

数据恢复指通过技术手段，将保存在硬盘、存储磁带库、U盘、数码存储卡、等设备上丢失的电子数据进行抢救和恢复。数据恢复技术不仅用于计算机取证, 也是对日常计算机使用过程中误删数据的有效弥补和中病毒后的有效抢救措施。常见数据恢复: 硬件恢复、软件恢复、备份等,以下为软件恢复方法:

删除文件存储区域在数据重新写入之前，删除的文件依然会存在之前所在的“簇”中,直到新数据的写入,覆盖原有数据。以硬盘数据恢复工具EasyRecovery Pro为例,它能够恢复丢失的数据以及重建文件系统。EasyRecovery Pro不会向原始驱动器写入任何东西，它主要是在内存中重建文件分区表使数据能够安全地传输到其他驱动器中。可以从被病毒破坏或是已经格式化的硬盘中恢复数据。被破坏的硬盘中像丢失的引导记录、BIOS参数数据块；分区表；FAT 表；引导区都可以由它来进行恢复。并且能够对 ZIP 文件以及微软的 Office系列文档进行修复。

注意: 恢复数据前尽量不要对分区进行写入操作

**四**、**课程感悟与总结** **1.课程感悟**

由于计算机犯罪大多具有专业性, 瞬时性,广域性,时空分离性等特点,通常很难留下犯罪证据,导致利用计算机技术犯罪的案例时有发生,计算机犯罪与取证这门课程的开设于打击计算机犯罪而言显得尤为重要。除此之外,由于中学教育与大学教育之间存在的跨度,很多大一学生缺乏计算机相关基础知识,计算机犯罪与取证课程中实验多与基础知识有关,易于学生理解计算机系统及网络原理,为今后的学习打下基础。同时真正的技术需要不断的深入钻研, 计算机犯罪与取证本科阶段作为一门选修课更大的作用是的是扩展学生的视野,丰富学生专业知识(例如误删数据如何解决或检查计算机无法连接到网络原因),激发学生对计算机方面学习的热情, 同时提高学生对计算机犯罪的警惕性以及被侵害后的抢救能力, 也吸引更多学生从事于计算机犯罪与取证方向。

而作为新青年的大学生,学习的目的不仅仅在于获取知识,更应该将所学应用到对社会的建设当中去,一方面我们要知法、懂法、守法,维护法律,另一方面我们要有责任担当精神,尽己所能规范计算机网络世界,使其不为法外之地。

**2.课程总结**

通过一期的计算机犯罪与取证选修课程,一共进行了计算机数据恢复、网络嗅探取证及入侵检测、DDOS攻击原理、MD5哈希算法碰撞及其在司法领域的应用、Windows 日志文件取证分析、美亚柏科FM-2008取证大师取证实验六项实践实验, 不仅提高对计算机系统的认识, 也提高了实验动手能力。通过课程学习已经能够管理好自己的计算机存储以及分区操作,并且能够独立配置虚拟机进行网络嗅探等;进一步了解了网络传输原理,知道如何检查计算机是否安全;能够知道常见计算机故障并找到解决方法。

相较于理论性的课程而言, 计算机犯罪与取证课程理论与实践相结合, 使学生能够更加深刻理解和运用学到的知识, 同时期待这门课程能够有更多的教学时长和更多学生的喜爱。

**参考资料:**

[1] 科普中国 数据恢复 2021-01-26