NTFS文件系统下涉密文件彻底删除技术

邵炳阳 沈长达

（厦门市美亚柏科信息安全研究所有限公司 福建 厦门 361000）

[摘 要] 涉密数据的安全保存与安全销毁是涉密数据安全管理的核心，是失泄密防范工作的重中之重。NTFS文件系统是微软Windows NT操作系统上推出的新一代文件系统，以安全性高、稳定性强、高容错性等优点迅速普及，是使用最广泛的文件系统之一[1]。目前，大部分敏感数据甚至是涉密数据大多存储在NTFS文件系统格式的存储介质中。本文从NTFS文件系统底层结构存储出发，分析NTFS文件系统下文件存储技术，提出NTFS文件系统下涉密文件彻底删除技术，该技术能够彻底删除涉密文件数据，同时清除涉密文件存储痕迹，确保涉密信息的安全性，对涉密数据的安全销毁具有重要意义。

[关键词] 数据安全；涉密数据；NTFS文件系统；文件销毁

1 NTFS文件系统简介

当用户将磁盘的一个分区格式化为NTFS分区时，就建立了一个NTFS文件系统结构，NTFS分区又被称为NTFS卷[2]。总体上，一个NTFS分区总体结构示意图如下图1所示。

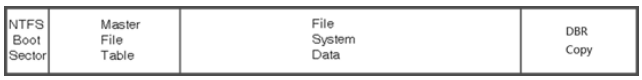

图1 NTFS分区结构示意图

NTFS文件系统使用了逻辑簇号（Logical Cluster Number，LCN）和虚拟簇号（Virtual Cluster Number，VCN）对卷进行管理[3]。逻辑簇号将整个NTFS分区从头到尾进行编号，通过LCN号以及分区的起始扇区号，就可以找到该LCN在磁盘中的具体偏移。虚拟簇号将文件从头到尾进行编号，方便文件系统对文件数据进行引用。

NTFS卷上的任何数据对象都表示为文件，通过文件记录对所有的文件进行管理，通常情况下文件记录大小固定为1KB。NTFS中所有的文件记录组成了NTFS中最重要的元数据文件为主文件表$MFT，$MFT中第一个文件记录就是对$MFT文件本身，对自身进行管理。系统通过文件记录来确定文件再磁盘上的位置一直文件的所有属性。NTFS卷中每一个文件都至少包有一个文件记录，当文件属性太多一个文件记录无法保存时，就会有多个文件记录，其中第一个文件记录称作基本文件记录，里面存储有其他关联的文件记录的信息。文件记录由文件头和一系列属性列表组成，属性由属性头和属性体组成，每一个属性完成一个单独的工作，不同的属性的结合体构成了不同种类的文件记录。属性体是构成NTFS的MFT记录的核心骨架，每一个属性完成一个单独的工作，不同的属性的结合体构成了不同种类的MFT记录。NTFS常见属性体及功能说明如下表1所示。

表1 NTFS常见属性表

类型	名称	备注
10H	标准信息属性	文件的基本属性，如文件属性、文件时间等
20H	属性列表属性	文件需要多个属性时存储其它记录的索引
30H	文件名属性	文件名属性，存储文件名和文件名时间信息
40H	对象标识符属性	文件对象ID，文件全局唯一分配的GUID描述
50H	安全性描述属性	NTFS安全对象的描述，对文件权限进行描述
60H	卷名属性	卷的名称
70H	卷信息属性	卷的版本和状态
80H	数据属性	存储文件扇区地图信息
90H	索引根目录属性	索引根节点，NTFS的B+树索引的根节点
A0H	索引分配表属性	索引分配属性，NTFS的B+树所有子节点的定位信息
B0H	位图属性	存储位图数据
C0H	重解析节点	重解析节点
100H	日志作用流属性	EFS加密属性，存储EFS解码密钥等信息

2 NTFS文件系统存储原理与可恢复性探究

NTFS文件系统底层是如何存储文件的，通过Windows系统下的常规删除手段删除的文件，其文件系统数据又是如何变化的。为了探究NTFS文件系统的底层存储机制以及Shift+Delete清除数据方式的可恢复性，笔者进行了如下试验：

1、测试环境：实验机器为WIN7 X64，Service Pack 1 Build 7601（后简称实验机）以及一块512M的VHD虚拟磁盘（后简称试验盘）；

2、用Winhex或者其它磁盘二进制数据编辑器对试验盘进行清零操作；

3、在实验机上对试验盘进行快速格式化，创建NTFS分区卷；

4、将试验盘进行备份，作为后续实验对照组使用，后续称为对照盘1；

5、往对试验盘中随机放入14张图片；

6、将试验盘进行备份，作为后续实验对照组使用，后续称为对照盘2；

7、对试验盘和对照盘1进行数据对比

在步骤7中的对比时，发现试验盘与对照盘1元数据的主要差别在于两个系统源文件：$MFT主文件表文件和$LOGFILE日志文件。其中，$MFT文件中，新增14个文件记录，而$LOGFILE日志文件新增若干修改日志。

8、采用Shift+Delete删除方式，删除其中1张图片；

9、对试验盘与对照盘2进行数据对比

在步骤7对比时，发现对于删除前后，可以发现，除了该文件的文件记录中部分数据状态值有修改以外，数据区域和其它文件属性值都没有任何变化，也就是在这种情况下，我们可以通过扫描$MFT文件里面的所有文件记录，通过识别被标记为删除状态文件记录，并将其恢复出来，这种简单的删除方式并不能真正删除掉实际的数据内容。另外，删除后，$LOGFILE日志文件也有新增若干修改日志。删除前后的文件记录对比图如下图2所示。

当文件被写入到NTFS文件系统分区时，系统需要做两件事情：其一为实际写入文件数据本身，其二为更新该文件的元数据信息。为了防止中间过程中异常断电等其他意外情况，操作系统会对这个过程中进行日志记录，及在$LOGFILE中记录相关的操作日志。通过上述简单的实验，可以证实当往NTFS文件系统分区创建或者写入新文件时，除了主文件表会新增文件记录之后，在日志文件里确实同样会有文件记录的操作日志。

3 NTFS涉密文件销毁方法

当在系统中删除一个文件时，系统只是在目录索引中将目标文件记录标记为删除可用状态，目标文件的实体数据仍然完好无损的存储在磁盘上，因此利用常见的恢复软件可以将这些被删除的文件恢复回来。针对重要敏感数据、乃至是涉密数据，这种删除方法并不安全，数据销毁技术应运而生。

软件销毁法是计算机数据销毁最常用的技术手段之一[4]。软

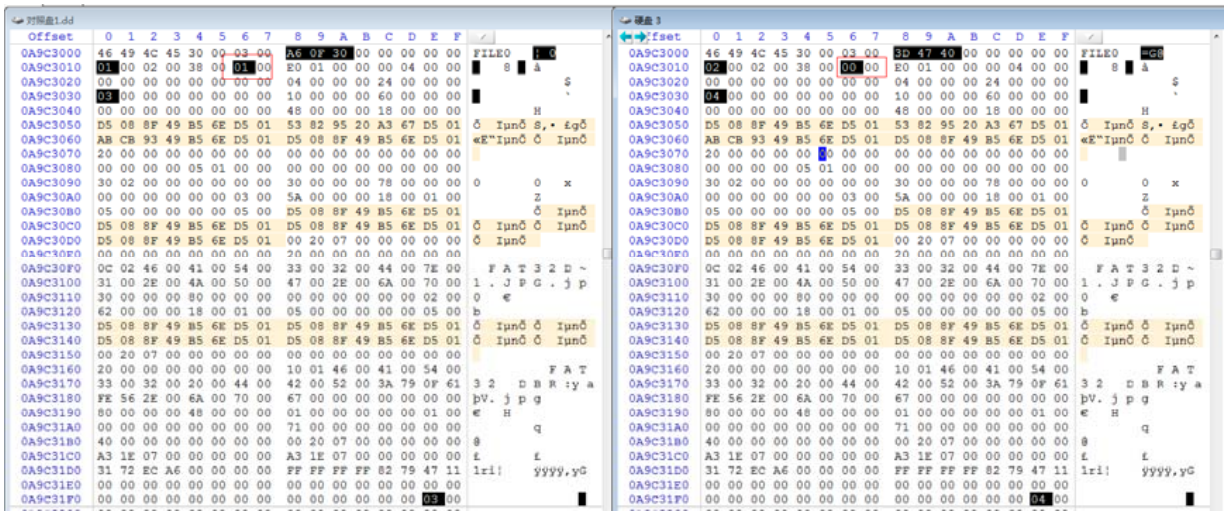

图2 Shift+Delete删除前后对比

件销毁法是基于操作系统和文件系统存储结构实现的，利用软件直接对所需要销毁的数据的存储空间进行覆盖写入以达到数据销毁的目的。软件销毁法相较于物理销毁法的主要优势在于成本低，不需要破坏存储介质，缺点在于销毁的速度慢、覆写次数少是销毁的数据依然存在被还原的风险。数据擦除标准《U.S.DOD 5220.22－M》明确要求安全擦除时磁盘数据覆写次数必须为7次以上。

目前采取的软件销毁法是采取磁盘二进制编辑器（如Winhex）等工具对整个磁盘或者分区进行擦除操作，或者采用Windows操作系统提供的磁盘格式化工具进行低级格式化以达到擦除的目的。这两种数据擦除方式的有点在于不需要依赖底层文件系统的存储格式和存储机制，直接整个磁盘数据或者分区数据全部擦除，相应的缺点在于这种操作往往耗时更长，无法单独针对特定文件进行擦除操作，灵活性不够。

因此，本文对NTFS文件系统底层文件存储进行深入研究，提出NTFS下指定文件或者目录数据销毁方法，该销毁方法分为两个模块进行：文件记录及文件内容的销毁、文件日志内容的销毁。

3.1文件记录及内容销毁

针对NTFS文件系统中的特定文件或者文件夹数据内容的销毁可以通过两种方式实现：直接通过Windows系统API进行擦除操作以及通过磁盘直接对文件数据内容占用的磁盘扇区进行擦除操作。

Windows系统API擦除方案对给定需要销毁的文件或者目录进行擦除操作，具体方案描述如下：

1、若给定需要销毁的是文件

#1 通过CreateFile以读写方式打开该文件，并获取该文件的实际大小；

#2 通过WriteFile以《U.S.DOD 5220.22－M标准》数据擦除标准对该文件进行覆写操作，并实时刷新缓存更新到磁盘中；

#3 通过CloseHandle关闭该文件；

#4 通过MoveFile重命名文件为临时文件名；

#5 通过DeleteFile删除文件。

2、若给定需要销毁的是目录

#1 通过FindFirstFile和FindNextFile查找所有子目录和子文件；

#2 对查找到的子文件以上述文件销毁方法进行销毁

#3 对于查找的子目录，若还包含子目录或者子文件，重复本目录销毁方式对该子目录进行销毁；若没有子目录或者子文件，通过MoveFile重命名为临时文件名，并通过RemoveDirectory删除该目录；

#4 直至所有文件和目录全部销毁。

通过磁盘直接对文件数据内容占用的磁盘扇区进行擦除方案对给定需要销毁的文件或者目录进行擦除操作，具体方案描述如下：

1、若给定需要销毁的是文件

#1 通过解析NTFS文件系统DBR，定位到$MFT文件的起始位置；

#2 通过解析$MFT文件记录，获取分区根目录文件夹$ROOT的文件记录；

#3 通过解析$ROOT根目录的索引属性，通过给定文件的路径名称查找第1层子目录对应的MFT号；

#4通过该MFT号从$MFT文件中读取对应的文件记录，解析该目录的索引属性，通过给定文件的路径名称查找第2层子目录对应的MFT号；以此类推，直到找到该文件对应的MFT号；

#5通过该MFT号从$MFT文件中读取目标的文件记录；

#6通过解析该目标文件的文件记录的数据属性，获取该数据内容所占据的磁盘空间扇区地图{<Start1，Length1>；<Start2，Length2>；…}；

#7采取《U.S.DOD 5220.22－M标准》数据擦除标准对DATA_MAP中记录的扇区地图进行擦除，并刷新到磁盘中；

#8 采取《U.S.DOD 5220.22－M标准》数据擦除标准对该文件的文件记录进行擦除，并刷新到磁盘中。

3.2日志记录销毁

NTFS文件系统是一个日志型的文件系统，文件记录和文件内容擦除之后，在日志文件$LOGFILE中还是会残留有该目标文件的属性信息，甚至是一些小文件的数据属性为常驻属性的情况下，还是可以通过一些日志恢复手段将该文件属性给恢复出来，还达不到一些高保密系统的要求。

NTFS的日志文件结构比较复杂，由两部分区域组成：重启动区域和无限记录区域。无限记录区域4KB大小的组成，记录头固定标志位“RCRD”。NTFS文件系统日志销毁方案描述如下：

#1 从$MFT文件中，查找NTFS日志文件的文件记录

#2 解析$LOGFILE的文件数据，获取其所有的日志区域；

#3 解析日志文件的无限记录区域，获取所有记录的文件修改记录；

（下转第88页）

浅谈美术教学中信息技术的运用

文 明
（辽宁省盘山县太平中学 辽宁 盘山 124112）

[摘 要] 信息时代的到来和不断发展，让计算机在教育领域中的应用越来越广泛。为了适应这个发展趋势，现代化信息技术介入美术课堂教学，并且在美术课堂教学和实验教学中起了不可低估的作用。因此，充分把现代信息技术融入美术教学之中，既能达到传授知识、培养能力又能实现因材施教和个别化教学的目的。

[关键词] 美术教学；信息技术；因材施教

一、恰当的运用多媒体服务于课前准备

一堂好的美术课往往是从备课开始的。现在我们要在美术教学中加入媒体教学的内容，随着对多媒体辅助教学研究的深入，美术教师应不断地把多媒体辅助教学方法和手段引入到教学课堂中。

（1）相关资料和素材的收集整理

美术是一门比较特殊的学科，尤其是在教学资料的准备上。美术的备课应该以图片、声音、视频、动画和文字为内容，它要求教师在备课时根据教材确定的教学目标和安排的教学内容，寻找较多的图片，另外配上声音、视频、动画和文字资料进行制作、整理。

（2）制作合适的美术课件

二、多媒体教学在课堂教学中实际运用

（1）图文声像并茂，激发学生的学习兴趣

多媒体教学软件必须正确表达学科的知识内容。在多媒体教学软件系统中，教学内容是用多媒体信息来表达的，各种媒体信息都必须是为了表现某一个知识点的内容，为达到某一层次的教学目标而设计、选择的。媒体能够提供有关的画面、动画、声音、活动现场、故事情节等创设的特定情境。

（2）提供生动直观的示范，展现演示过程和方法

多媒体教学软件是由文本、图形、动画、声音、视频等多种媒体信息集成在一起，经过加工和处理所形成的教学系统。如绘画和制作的步骤、过程、技能、技巧等，可供学生模仿和练习。

三、多媒体课将逐渐演变、发展成网络环境教学的新模式

1、信息技术教学与美术学科的整合

信息技术教学与美术学科的整合，形成优势互补，显示出美术学科的优势，使美术的教和学都变成了“乐事”。美术是视觉艺术，在视觉传达中向观者提供信息和传达思想是美术特点中最显著的一点。

2、丰富的网站资源和网络环境教学

由于传统的美术呈现形式需要通过各种介质来呈现，如：中国画、油画、雕塑、建筑等各种形式对传达空间和场合需要有特殊的要求，像美术馆、展览馆等。而中学生美术课上无法与这些美术作品“面对面”的机会。但信息技术、网络传播具有交互性、便捷性，这个特别“迎合”了美术视觉传达这一特有的性质。

总之，在美术教学中合理运用多媒体，有助于提高课堂教学效果。学生不会因此对传统美术的淡化，反而因为网络的优势拓宽学生的知识领域，为学生学习方式方法创设了优越的环境。

参考文献

[1]小学美术课堂教学中存在的问题及对策探究[J].朱晓磊.黑龙江科学.2018（04）

[2]VR新技术在小学美术课堂教学中的探究与思考——以人美版教材一年级的《谁的鱼最美》为例[J].王丽萍.华夏教师.2018（02）

[3]大众美术教育缺什么?[J].刘德龙.广西教育学院学报.2010（02）

（上接第114页）

#4 对于需要销毁的文件，获取其唯一文件记录号；

#5 针对所有记录的文件修改记录，若属于该销毁文件的日志记录，采用《U.S.DOD 5220.22－M标准》数据擦除标准对该日志区域进行擦除，并刷新到磁盘中。

4 结束语

数据安全删除是我们的核心关注点，即如何灵活彻底清除计算机中的涉密文件以及涉密数据。本文对NTFS文件系统结构进行深入研究，提出基于NTFS文件系统涉密文件彻底删除技术，该技术可以的对NTFS卷中的涉密文件进行擦除，可以有效防止失泄密。传统软件销毁法通过对整个磁盘或者分区进行覆写擦除，耗时时间长且不够灵活，采用本文介绍的数据擦除法，可以针对特定文件进行擦除，具备更强的灵活性。

参考文献

[1]黄步根.数据恢复与计算机取证[J].计算机安全，2006，（6）：79-81

[2]梁金千，张跃.NTFS文件系统的主要结构[J].计算机工程与应用，2003，39（8）：116-118.

[3]涂彦晖，刘胜.彻底粉碎NTFS卷中文件数据的方法[P].中国专利：200610122479.1，2007-3-14.

[4]张鹏，秦飞舟.数据销毁技术综述[J].电脑知识与技术，2015（28）.

作者简介：

邵炳阳（1990年4月）男，汉，福建厦门人，本科，厦门市美亚柏科信息安全研究所有限公司，研究方向：文件系统解析、数据恢复、计算机取证

沈长达（1989年1月）男，汉，福建泉州人，本科，厦门市美亚柏科信息安全研究所有限公司，研究方向：电子数据证据固定、取证分析