第 36 卷 第 2 期 计 算 机 工 程 2010 年 1 月
Vol.36 No.2 Computer Engineering January 2010
·开发研究与设计技术· 文章编号：1000—3428(2010)02—0275—02 文献标识码：A 中图分类号：TP309.2

# NTFS 文件系统中的视频数据恢复方法

黄步根[1]，刘建军[2]，张晓南[2]
(1. 江苏警官学院公安科技系，南京 210012；2. 南京市公安局网警支队，南京 210005)

**摘 要：**在 NTFS 文件系统中，视频监控文件在形成过程中被分割成大量非常小的块进行存储，通过多个索引表形成整个文件，删除该文件后，主索引表被丢弃，但扩展属性中的索引表还存在。针对该问题，提出根据文件的扩展属性恢复数据的方法，通过整合大量分散存储的碎片，能够恢复被删除的视频文件的大部分内容。

**关键词：**数据恢复；视频监控；NTFS 文件系统

# Recovery Method of Video Data in NTFS File System

HUANG Bu-gen[1], LIU Jian-jun[2], ZHANG Xiao-nan[2]
(1. Department of Forensic Science, Jiangsu Police Institute, Nanjing 210012;
2. Department of Network Police, Nanjing Municipal Public Security Bureau, Nanjing 210005)

**【Abstract】** In the NTFS file system, video monitor file is divided into a large number of very small block for storage, the entire file is formed by the index tables, the main index table is missing when the file is deleted, but other index tables exist in the extended attributes. This paper proposes a method for recovering data by the extended property according to file. This method can effectively combine many scattered fragments together and recover most of video monitor data which has already been deleted.

**【Key words】** data recovery; video monitor; NTFS file system

视频监控已经广泛应用于各行各业，在案件处理过程中经常需要用到监控录像，但它们常被人为删除，一般的数据恢复软件不能对其进行恢复。本文研究 NTFS 文件系统下监控录像的存储结构，提出数据恢复的方法。

## 1 NTFS 文件系统的文件存储方式

视频监控，由于其数据量较大，一般使用大的硬盘，如 320 GB, 500 GB，划分成 2 个~3 个逻辑分区，大的分区比较适合使用 NTFS 文件系统。

NTFS[1]文件系统以簇为单位分配和回收存储空间，从 0 扇区开始划分簇，通常每簇 8 个扇区(4 KB)，文件存储时，操作系统根据应用程序提出的申请分配存储空间，由于文件的增加、删除等操作，不能保证文件存储到连续存储空间，因此操作系统必须记录每个文件存储的位置，在 NTFS 文件系统中使用索引表来记录。索引表的形式是“簇号(簇数)”，假设文件占用 8 簇，分别在 400, 401, 420, 421, 422, 423, 500, 501，则索引表的形式为 400(2), 420(4), 500(2)，由于操作系统为了节省索引表的存储空间，因此只有第 1 项的簇号是绝对数，其他簇号是相对前 1 项给出的，如上形式的索引表存储形式是 400(2), 20(4), 80(2)。由此可以看出，索引表是存储分配的关键，如果索引表中某一项被破坏了，那么其后的位置就无法确定。

操作系统以文件为单位管理系统数据和用户数据，文件通过主文件表(Master File Table, MFT)来管理，MFT 是一个与文件相对应的数据库，由一系列文件记录(称为 FILE 项)组成，每一个文件(夹)至少有一个 FILE 项，长度一般固定为 2 个扇区，即 1 024 Byte，FILE 项记录了文件的所有数据，每类数据以一个属性来表示，如文件名、文件长度、文件的时间等，文件内容也是一个属性。属性数据较小时能够存放在 FILE 项中，称为驻留的属性，否则为非驻留的属性，通过索引表来保存其存储位置，如果索引表很大，在一个 FILE 项中存储不下，那么可以有扩展属性以增加 FILE 项来保存。每个 FILE 项由一个整数文件号来标识，从 0 开始编号，每个属性也用一个整数值来标识，如日期属性是 0x10，扩展属性是 0x20，文件名属性是 0x30，文件内容属性是 0x80。不用扩展属性的文件存储 MFT 603 如表 1 所示。

**表 1 MFT 603**

| 偏移 | 属性 | 值 | 含义 |
|---|---|---|---|
| 0x38 | 0x10 | 2008.10.13 23:24:10 | 时间 |
| 0x98 | 0x30 | 4-0-20081013232409.MPG | 文件名 |
| 0x198 | 0x80 | *Length*=110400 115967361(10) 115967409(6) 115967549(8) 115967677(3) | 文件长度及索引表 |
| 0x1f0 | 0xffffffff | - | 结束标记 |

视频监控系统用于小区、商场、银行等处，往往有多个探头，24 h 监控，有的固定半小时生成 1 个文件，有的根据现场目标的变化情况来采集和存储数据、分割文件，在多探头录像形成过程中，各文件不是一次形成的，而是不断追加数据，使文件被分割成许多块存储在硬盘上。以一个 5 探头监控系统为例，5 个文件的存储索引如下：

(1)0-0-20081110163817.MPG: 27306963(6) 27306991(18) 27307187(8) 27307211(16) 27307243(16) 27307363(16) 27307411(16)…；

(2)1-0-20081110163817.MPG: 27306987(4) 27307159(28)

**作者简介：**黄步根(1958－)，男，教授、硕士，主研方向：信息安全，计算机取证；刘建军、张晓南，技术员

**收稿日期：**2009-06-17 **E-mail：**bghuang@sina.com

27307195(16) 27307259(16) 27307347(16)…；

(3)2-0-20081110163817.MPG: 27306977(6) 27307081(50) 27307291(24) 27307427(16) 27307523(16)…；

(4)3-0-20081110163817.MPG: 27306983(4) 27307131(28) 27307227(16) 27307275(16) 27307379(32)…；

(5)4-0-20081110163817.MPG: 27306969(8) 27307009(72) 27307315(32) 27307491(32) 27307619(16)…。

由此可以看出，连续的硬盘空间被依次分割分配给 5 个文件：27306963(6)~(1), 27306969(8)~(5), 27306977(6)~(3), 27306983(4)~(4), 27306987(4)~(2), 27306991(18)~(1), 27307009(72)~(5), 27307081(50)~(3), 27307131(28)~(4), 27307159(28)~(2), 27307187(8)~(1), …。

视频文件长度一般有 100 MB，索引表需要占用多个 FILE 项，通过扩展属性关联。以文件(1)为例，MFT 834 主要属性数据见表 2。

**表 2　MFT 834**

| 偏移 | 属性 | 值 | 含义 |
|---|---|---|---|
| 0x38 | 0x10 | 2008.11.10 17:08:17 | 时间 |
| 0x98 | 0x20 | (0x80 840) (0x80 845) (0x80 850) (0x80 855) (0x80 858) (0x80 863) (0x80 867) (0x80 872) (0x80 877) (0x80 882) | 扩展属性 |
| 0x2c8 | 0x30 | 0-0-20081110163817.MPG | 文件名 |
| 0x340 | 0xffffffff | - | 结束标记 |

扩展属性记录了每个扩展属性的文件号。可见，文件内容属性(0x80)存储的文件号有 10 个，依次为 840,845, 850,…,882。MFT840, MFT845 主要属性数据见表 3、表 4。

**表 3　MFT 840**

| 偏移 | 属性 | 值 | 含义 |
|---|---|---|---|
| 0x38 | 0x80 | *Length*=220506304 27306963(6) 27306991(18) 27307187(8) 27307211(16) 27307243(16) 27307363(16) 27307411(16)… | 文件长度及索引表 |
| 0x3f0 | 0xffffffff | - | 结束标记 |

**表 4　MFT 845**

| 偏移 | 属性 | 值 | 含义 |
|---|---|---|---|
| 0x38 | 0x80 | *Length*=0 27335219(32) 27335363(64) 27335619(16) 27335699(32) 27335875(16) 27335939(16) 27336035(16) 27336227(16) 27336291(16)… | 文件长度及索引表 |
| 0x3f0 | 0xffffffff | - | 结束标记 |

其余扩展属性形式与上相同。在第 1 个扩展的 FILE 项是真实的文件长度，在其他扩展的 FILE 项中，文件长度记为 0，无效。

## 2　NTFS 中文件的删除

删除文件后，系统回收存储空间，并在 FILE 项中做相应处理。在每个 FILE 项中，有 1 个删除标记，文件删除后，标记为 TRUE。如果文件的存储索引不够大，那么不需要扩展属性，在文件删除后，除删除标记和时间属性外，其他属性不变，存储索引没有被破坏；如果有扩展属性，则较复杂，以上文的监控录像文件(1)为例，删除文件 0-0-20081-110163817.MPG 后的情况见表 5。

**表 5　MFT 834**

| 偏移 | 属性 | 值 | 含义 |
|---|---|---|---|
| 0x38 | 0x10 | 2008.11.10 17:08:17 | 时间 |
| 0x98 | 0x20 | (0x80 840) | 扩展属性 |
| 0x1a8 | 0x30 | 0-0-20081110163817.MPG | 文件名 |
| 0x230 | 0xffffffff | - | 结束标记 |

在扩展属性中，存储索引只保留了 1 个，其后的属性位置提前，覆盖原来的其他扩展属性。

删除文件 0-0-20081110163817.MPG 后的情况见表 6。

**表 6　MFT 840**

| 偏移 | 属性 | 值 | 含义 |
|---|---|---|---|
| 0x38 | 0x80 | *Length*=0 | 文件长度 0 |
| 0x80 | 0xffffffff | - | 结束标记 |

可见，文件内容属性(0x80)中没有了索引表。索引数据大多数还在，但由于属性结束标记 0xffffffff 的提前，覆盖了索引结构的开头部分。由上文可知，相对于前一项簇号，索引数据中的簇号，存储时除了第 1 个使用绝对数外，其余均使用相对数，因此，只要一项被破坏，其后的所有索引均无法还原，即文件删除后，第 1 个索引表失效就无法再还原。

删除文件 0-0-20081110163817.MPG 后的情况见表 7。

**表 7　MFT 845**

| 偏移 | 属性 | 值 | 含义 |
|---|---|---|---|
| 0x38 | 0xffffffff | - | 结束标记 |

可见，表 7 只是将表 4 0x38 处的 0x80 用结束标记 0xffffffff 替代，索引结构没有受到破坏，可以还原。

## 3　NTFS 中文件监控录像的数据恢复

从上文的分析可以知道，多探头监控录像数据被分割成长度不等的(如 16 簇、24 簇)许多小块存放在数据区，仅从数据区难以辨别出不同文件。如果文件的存储索引不够大，那么不需要扩展属性，在文件被删除后，FILE 项中仅添加删除标记，文件内容属性(0x80)的存储索引没有被破坏，可以根据它进行数据的完全恢复(见表 4)。如果文件有扩展属性，第 1 个扩展属性中的索引表被破坏，那么文件无法恢复。多探头监控录像往往是带有扩展属性的，在文件被删除后，即使立即被发现，一般的数据恢复工具也得不到录像数据。比较表 3 与表 6、表 4 与表 7 可以发现，除了第 1 个扩展的 FILE 项外，其他扩展的 FILE 项中数据索引没有被破坏，可以还原。可见，一个视频录像文件可以根据扩展属性的 FILE 项还原出几个较大块的数据文件，但不包括第 1 个扩展项对应的数据块。在上文的例子中 1 个 200 MB 文件包含 10 个扩展 FILE 项，平均 1 个扩展项对应文件大小为 20 MB，为显现其视频内容提供了较好的基础。

具体实现方法为：在 NTFS 分区中搜索 MFT[2]，对于删除的 FILE 项，如果第 1 个属性就是结束标记 0xffffffff，那么将其改为 0x80，恢复索引表，命名文件，根据索引表存储数据得到一个较长的视频监控录象数据块。

## 4　结束语

本文提出的恢复方法可以恢复被删除视频文件的大部分内容，但是有一定的局限性，要求 MFT 中文件 FILE 项存在。由于根据扩展属性恢复出来的视频数据文件没有标准的头部信息，因此下一步的研究工作是如何对该视频数据文件进行播放[3]。

### 参考文献


[1] 黄步根. NTFS 系统存储介质上文件操作痕迹分析[J]. 计算机工程, 2007, 33(23): 281-283.

[2] 黄步根. 存储介质上电子证据的发现和提取技术[J]. 计算机应用与软件, 2008, 25(1): 88-90.

[3] 黄本雄, 昌玉芳. 基于 MPEG-4 的视频监控系统中视频流的存储算法[J]. 电视技术, 2005, 28(8): 150-152.


编辑　陆燕菲