浙江科技学院学报，第 28 卷第 5 期，2016 年 10 月
Journal of Zhejiang University of Science and Technology
Vol. 28 No. 5，Oct. 2016

**doi**：10.3969/j.issn.1671-8798.2016.05.006

# iOS9 平台下的 iTunes 备份文件技术研究

马洪涛[1]，陈　英[2]

（1.杭州市公安局 刑侦支队，杭州 310004；2.浙江科技学院 信息中心，杭州 310023）

**摘　要**：公安机关在对 iOS 设备进行分析取证时，为保护电子证据的完整性、真实性和原始性，通常对 iTunes 备份文件进行分析取证。为此，针对如何解析 iTunes 备份文件进行了详细的技术研究，分析了备份文件的结构和索引文件 Manifest.mbdb 中目录项结构，进而提出解析 iTunes 备份文件的技术方法，并且在此基础上开发了一款软件程序并实现了对 iTunes 备份文件的数据还原。

**关键词**：电子数据取证；iTunes 备份文件；Manifest.mbdb

**中图分类号**：TP309.3；D918.2　　**文献标志码**：A　　**文章编号**：1671-8798(2016)05-0367-06

# Technological research on iTunes backup file of iOS9

MA Hongtao[1]，CHEN Ying[2]

（1. Criminal Investigation Detachment，Hangzhou Municipal Public Security Bureau，Hangzhou 310004，China；2. Network Information Center，Zhejiang University of Science and Technology，Hangzhou 310023，China）

**Abstract**：While analyzing forensics of iOS equipment，public security organs always analyze forensics of iTunes backup files to protect integrity，authenticity and primitiveness of electronic evidences. We made detailed technical research about how to analyze iTunes backup files，analyzed structure of backup files and structure of catalogue in index file Manifest.mbdb，and proposed technical method to analyze iTunes backup file. Based on the above，we developed software and realized data recovery of iTunes backup files.

**Keywords**：digital forensics；iTunes backup files；manifest.mbdb

随着电子信息和移动互联网技术的蓬勃发展，手机基本成为人人必备的信息交流终端，依托手机和移动互联网，网络社会与实体社会高度融合，手机设备记录了大量有形、无形的有价值的信息。近年来的工作实践表明，对涉案手机的电子数据取证能为侦查破案和指控犯罪提供司法依据，是一种很有效的技术手段。为保护电子证据完整性、真实性和原始性的取证规范，公安机关在对 iOS 设备进行分析取证时，

**收稿日期**：2016-09-13

**作者简介**：马洪涛（1981—　），男，浙江省杭州人，工程师，硕士，主要从事移动通讯设备电子数据取证研究。

通常使用 iTunes 软件进行备份或第三方取证软件直接调用 iTunes 软件中的 AppleMobileBackup. exe 进行备份，再对备份文件进行分析取证[1-5]。当前，网络上公开的 iTunes 备份技术研究主要是基于 iOS4 版本，同时，苹果公司一直不公开 iTunes 备份的相关工作机制，因此，对于 iOS9 及以上版本的 iTunes 备份文件的技术研究就显得尤为重要。本研究将深入研究如何在新的 iOS 软件版本下解析 iTunes 备份文件，获取 iOS 设备中存储的文件路径和数据文件。

## 1 iTunes 备份文件概述

iTunes 软件是由苹果公司官方发布的在 MAC 和 PC 使用的免费应用程序，它除了能播放数字音乐和视频外，还提供对 iPhone、iPad 等 iOS 设备进行数据备份，以及下载安装 App 应用等设备管理功能。从电子数据取证的角度来讲，iTunes 数据备份几乎包含所有的设备信息和用户数据，包括系统自带的 App 数据和用户下载的 App 数据，并且获取 iTunes 备份相对简单，通过解析 iTunes 数据备份文件就可以获取相关的电子数据。iTunes 备份的存储文件路径由于操作系统的差异而不同，表 1 列出了 iTunes v12 版本下常见操作系统中备份文件的默认存储路径，并且 iTunes 也支持用户手动修改默认存储路径。当然，用户也可以对数据备份文件进行加密，对备份进行加密后，从加密备份文件恢复数据时需要输入密码。本研究主要讨论未进行加密的数据备份文件的相关问题。

**表 1** iTunes 数据备份文件存储路径

**Table 1** Save path of iTunes data backup files

| 操作系统 | 文件路径 |
|---|---|
| Mac OS | Users/(username)/Library/Application Support/MobileSync/Backup/ |
| Windows XP | \Documents and Settings\ (username)\Application Data\ Apple Computer\MobileSync\Backup\ |
| Windows 7/10 | \Users\ (username)\AppData\Roaming\Apple Computer\MobileSync\Backup\ |

备份文件结构：打开该 iTunes 数据备份文件夹会发现大量文件名为 40 位 16 进制字符长度且没有文件属性的数据文件和 Info. plist、Manifest. plist、Status. plist、Manifest. mbdb[6] 文件。如图 1 所示，文件名为 40 位 16 进制字符的文件是设备中存储的数据文件，而这些文件名都是通过一定的规则进行哈希编码运算得到的。3 个后缀为 plist 的文件，可以用 plistEditor 软件打开浏览，通过分析发现，其中 Info. plist文件记录了设备名称、版本、IMEI、ICCID、GUID 等在内的一些手机硬件信息；Status. Plist 文件记录了设备备份时间、UUID 及备份状态等信息；Manifest. plist 文件保存了 iOS 设备已安装的 App 信

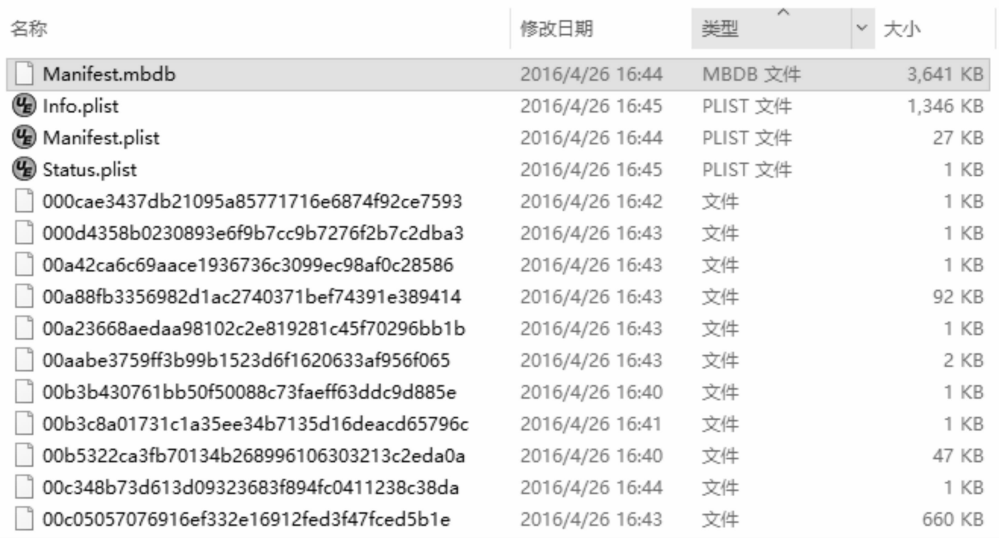


**图 1** iTunes 数据备份文件截图

**Fig. 1** Screenshots of backup files of iTunes data

息，包括 App 的名称、版本、程序和数据文件路径[6]；Mainfest. mbdb 是二进制文件，保存了所有备份文件的文件名、路径、所属域等信息，也是研究如何解析 iTunes 备份文件的技术核心。

## 2　备份索引文件 Manifest. mbdb 详解

使用二进制工具 WinHex 打开 iOS 9 平台下的备份索引文件 Manifest. mbdb，如图 2 所示，可以发现文件的前 6 个字节是固定的，其中把前 4 个字节按 char 类型处理 ASCII 码显示为字符“mbdb”，相当于文件的一种标识。

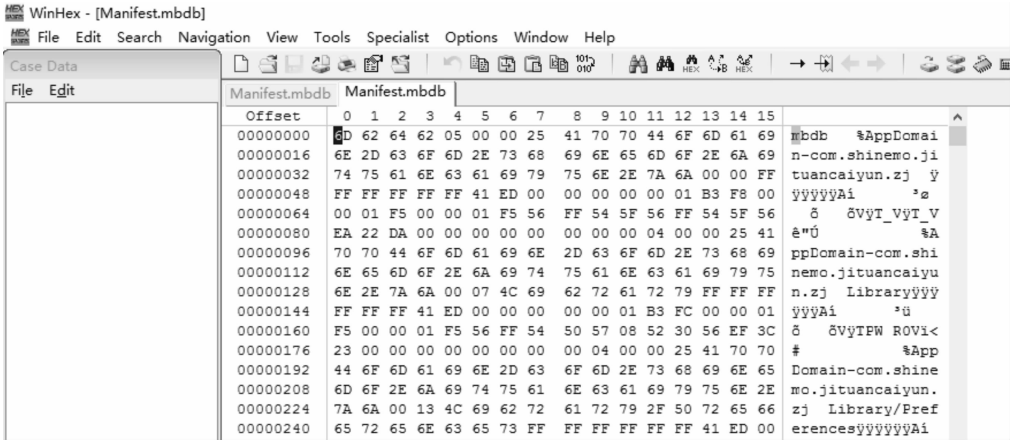


**图 2**　Manifest. mbdb 在 WinHex 中截图

**Fig. 2**　Screenshots of Manifest. mbdb in WinHex

后面的内容是一个接着一个的目录项，目录项内保存了备份域和备份路径等重要信息。整个 Manifest. mbdb 文件结构是：文件头＋目录项 1＋目录项 2＋目录项 3＋…＋目录项 $N$。其中目录项的组成结构是我们研究的重点，也是解析备份索引文件的关键。目录项的组成结构和数据类型[7]如下：

1）备份域，数据类型为字符串，前 2 个字节表示备份域的字符长度，后面为具体的内容。

2）备份路径，数据类型为字符串，前 2 个字节表示备份路径的字符长度，后面为具体的内容。

3）链接目标，数据类型为字符串，前 2 个字节表示链接目标的字符长度，后面为具体的内容。

4）文件哈希，数据类型为字符串，前 2 个字节表示数据 hash 的字符长度，后面为具体的内容。

5）保留密钥，前 2 个字节表示字符长度，对于未加密的备份文件该项内容为空。

6）定长属性，基本属性 39 个字节，最后一个字节代表附加属性的个数；其中基本属性包含了文件的创建时间、最后修改时间、最后访问时间及文件类型等基本信息；每一个附加属性都有一对属性键、属性值，属性键和属性值的头 2 个字节都表示长度，后面为具体的内容。

通过解析 Manifest. mbdb 文件，获取每个目录项中备份域和备份路径，对解析出数据文件特别重要，其中 40 位 16 进制字符的数据文件的文件名就是通过取备份域和备份路径的 SHA1 哈希值计算出来的，计算公式为：哈希值文件名 ＝ SHA1（备份域 ＋“－”＋ 备份路径）[8]。

## 3　解析 iTunes 备份文件

由于本研究主要讨论公安机关对 iOS 设备进行分析取证时针对 iTunes 备份文件的技术研究，不涉及备份文件加密和解密问题，故在解析 iTunes 备份文件时，按未加密备份文件处理。第一步，按照图 3 的方法解析出所有的哈希值和数据文件完整路径的对应关系，可以构成一个通过 hash 值查找完整路径的数据字典。

第二步，对备份文件夹中的每一个以哈希值命名的数据文件，通过数据字典查找该文件名哈希值对应的完整路径，再将以哈希值命名的文件重命名为正确的文件名和后缀格式，并移动到正确的路径位置（需创建相应的文件夹）后，就可以恢复 iOS 设备中的文件结构和数据文件，iTunes 备份就得到了解析

还原。

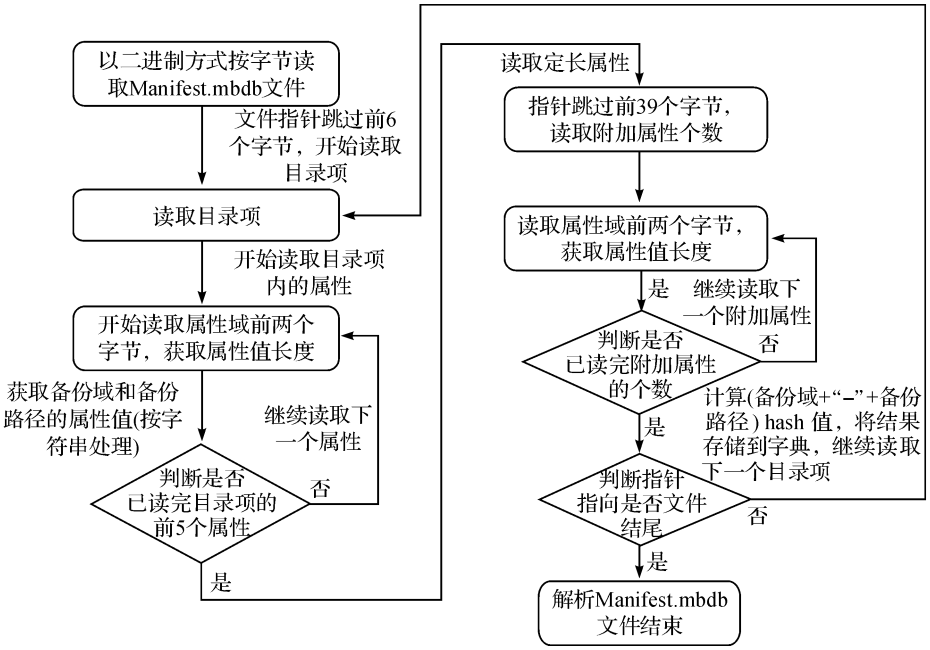


**图 3** 解析 iTunes 数据备份文件流程

**Fig. 3** Analysis of flow of iTunes data backup files

## 4 iTunes 数据备份文件解析的实例分析

针对 iTunes 数据备份文件的解析，结合前面论述的内容，根据解析流程，使用 QT5 开发了针对 iOS9 平台下备份文件的解析软件工具，生成备份文件的数据字典和导出数据文件，主要功能性测试步骤如下。

### 4.1 获取设备的 iTunes 数据备份文件

将测试的 iPhone SE(iOS v9.3)设备连接电脑进行数据备份，并将备份文件存储在本地电脑上(默认对备份不加密)，备份结果如图 4 所示。

### 4.2 运行解析软件提取 Manifest.mbdb 中目录项的数据字典

运行解析备份软件(基于 QT5 框架开发)，得到 Manifest.mbdb 的解析日志文件 Manifest_log.txt 和数据字典文件 Manifest_zd.csv，如图 5 所示。

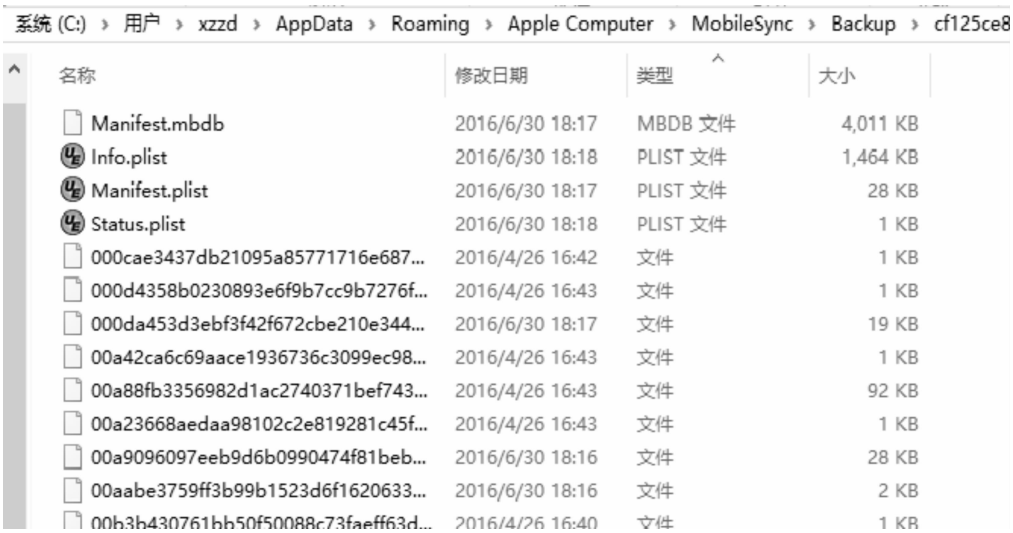


**图 4** iTunes 备份文件截图

**Fig. 4** Screenshots of backup files of iTunes


**图 5**　iTunes 备份文件数据字典和解析日志

**Fig. 5**　Data dictionary and parsing logs of backup files

### 4.3　设定输出文件夹恢复 iTunes 备份数据文件

运行解析备份软件，程序通过查询字典文件 Manifest_zd.csv，将 40 位 16 进制字符的数据文件恢复为初始文件名和文件格式，并存放在对应的文件路径中，如图 6 所示。

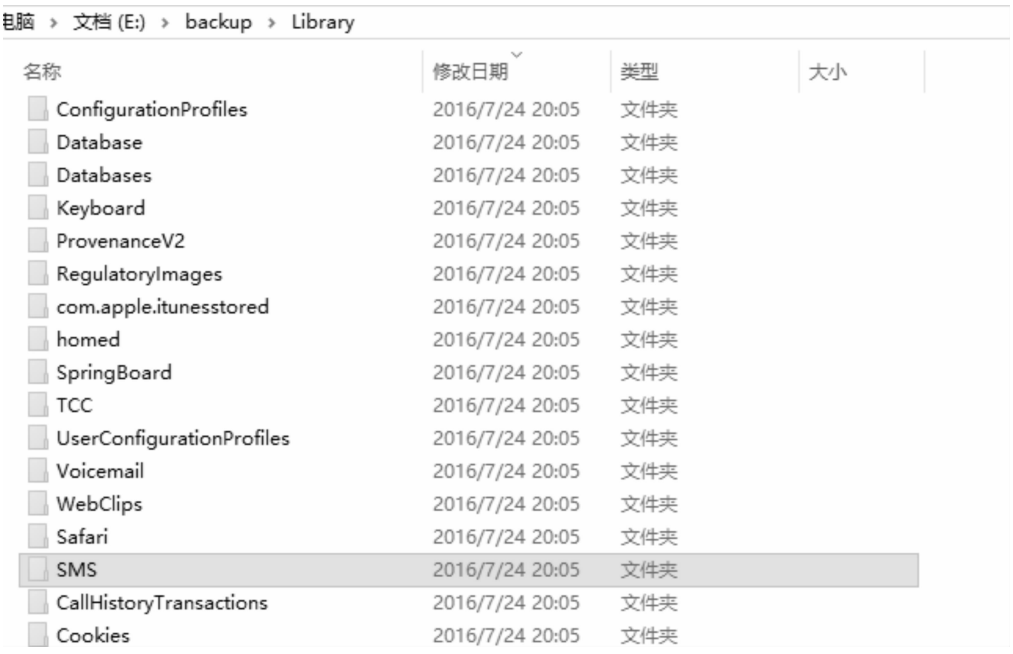


**图 6**　恢复出备份文件的结果截图

**Fig. 6**　Screenshots of results of recovered backup files

## 5 结 语

本文主要介绍了公安机关在对iOS设备进行分析取证时，针对iOS9平台下的iTunes备份文件解析的技术研究，包括对备份文件的文件组成结构和其中重要的索引文件Manifest.mbdb中目录项构成进行了深入研究，并在此基础上提出了针对iOS9平台的解析iTunes备份文件的技术方法。利用QT5开发了一款适配解析iOS9备份的软件测试程序，在iTunes v12环境下对运行iOS9.3的iPhone手机备份进行功能性测试，成功导出数字字典且恢复了手机内存储的数据文件，测试结果验证了该项技术的研究成果。此项研究为提取运行iOS9版本的iPhone手机电子数据提供了软件解决方法，可有效帮助公安部门克服在对iOS设备进行电子数据取证时过分依赖于专业厂商提供的专业手机取证硬件设备的问题，并为电子数据取证与鉴定的研究提供参考。

**参考文献：**

[1] 金波，杨涛，吴松洋，等.电子数据取证与鉴定发展概述[J].中国司法鉴定，2016(1)：68.

[2] 彭建新，周元建.iOS设备取证技术研究[J].中国人民公安大学学报(自然科学版)，2012(4)：38.

[3] 贺宇轩，孟魁，刘功申，等.iOS系统数据安全分析与加固[J].通信技术，2014(6)：668.

[4] 高建华，鲁恩铭.智能手机数据的提取与恢复研究[J].计算机安全，2014(8)：41.

[5] 金波，杨涛，吴松洋.电子数据取证与鉴定发展概述[J].中国司法鉴定，2016(1)：62.

[6] BADER M，BAGGILI I. iPhone 3GS forensics：logical analysis using apple iTunes backup utility[J]. Small Scale Digital Device Forensics Journal，2010，4(1)：7.

[7] The iPhone Wiki. iTunes Backup[EB/OL].(2016-09-26)[2016-09-10]. https：// www. theiphonewiki. com/wiki/ITunes_Backup # Record_. 28variable_size.

[8] 陈佳霖.iOS平台应用程序安全性研究[D].上海：上海交通大学，2014：37.