(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103064764 A
(43)申请公布日 2013.04.24

(21)申请号 201210585940.2

(22)申请日 2012.12.28

(71)申请人 盘石软件(上海)有限公司
地址 200333 上海市普陀区中江路879号19号楼4楼

(72)发明人 李建新 李毅

(74)专利代理机构 上海天翔知识产权代理有限公司 31224
代理人 孙景宣

(51)Int.Cl.
G06F 11/14(2006.01)
H04M 1/725(2006.01)

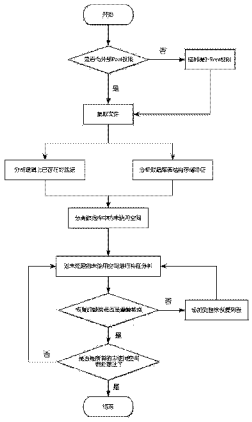
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种快速恢复安卓手机删除信息的取证方法

(57)摘要

本发明公开了一种快速恢复安卓手机删除信息的取证方法，它首先提取出手机中的用户数据文件的可直接查看信息，然后根据该可直接查看信息获取数据库表结构的存储特征，并进一步分离出数据库中的未使用空间；再在未使用空间中尝试匹配正常记录的特征，并对匹配到的数据进行验证，获取已经删除的记录，然后结合该记录的字段长度定义，将其后的数据进行分割，以还原其各主要字段的内容，最后将还原出来的数据与正常记录进行对比，通过逻辑判断后添加到记录列表中；继续匹配未使用空间中，直到所有的未使用空间都处理完毕。本发明的有益效果在于：恢复快速、使用便捷，可靠性强。



CN 103064764 A

1. 一种快速恢复安卓手机删除信息的取证方法，其特征在于，所述方法包括如下步骤：

1）首先使用安卓 SDK 中提供的调试开发工具 Android Debug Bridge 中提供的 pull 命令提取手机中的用户数据文件，并对其进行进一步分析，获取用户数据文件中的可直接查看信息；

2）通过 API 读取可直接查看信息中的数据内容，然后通过对比验证来确定数据内容中各字段的具体含义，重新组合后得到手机上的可见数据，同时也得到数据库表结构的存储特征；

3）通过数据库表结构的存储特征分离出数据库中的未使用空间；

4）通过分析安卓手机中正常记录的存储结构提取出正常记录的特征，然后通过正则表达式在未使用空间中尝试匹配该特征，并对匹配到的数据进行验证；如果其结构和正常记录相符合，则认为这是一条已经删除的记录，然后结合该记录的字段长度定义，将其后的数据进行分割，以还原其各主要字段的内容；

5）将还原出来的数据与通过 API 解析的正常记录进行对比，如果关键信息完全相同，则认为这是一条逻辑上已存在或已经有相同的记录被恢复出来的冗余数据，不添加到记录列表中；如果关键信息不相同，则添加到记录列表中；

6）继续匹配未使用空间中，直到所有的未使用空间都处理完毕。

2. 根据权利要求 1 所述的一种快速恢复安卓手机删除信息的取证方法，其特征在于，所述步骤 1）进一步包括一种获取 root 权限的方法，该方法为直接通过 adb root 提升外部的 root 权限；如果 adb root 提示无法提升到 root 权限，则通过一个临时 root 的脚本来提升到 root 用户的权限。

3. 根据权利要求 1 所述的一种快速恢复安卓手机删除信息的取证方法，其特征在于，所述步骤 5）中，将还原出来的数据添加到记录列表中的同时将该数据标记为已删除，表明这是一条被恢复出来的记录。

4. 根据权利要求 1 所述的一种快速恢复安卓手机删除信息的取证方法，其特征在于，所述用户数据文件为 SQLite3 数据库格式，通过 API 能正常的读取其中的数据内容。

5. 根据权利要求 1 所述的一种快速恢复安卓手机删除信息的取证方法，其特征在于，所述调试开发工具 Android Debug Bridge 通过应用程序调试接口连接手机。

一种快速恢复安卓手机删除信息的取证方法

技术领域

[0001] 本发明涉及移动设备信息处理及删除信息恢复领域，具体地说，特别涉及到一种快速恢复安卓手机删除信息的取证方法。

背景技术

[0002] 手机取证的方式方法目前在不断的更新和改进，最初只是对手机中的基本信息(如联系人，通话记录和短消息等)进行简单的提取和固定。后来随着智能手机的出现，手机取证也包含了对应用程序数据(如即时通讯工具，社交网络工具，定位导航工具等)进行提取、固定和关联分析等。

[0003] 司法人员在调查或取证过程中，不仅需要提取手机上当前存在的信息，还对嫌疑人已经删除的信息特别关注。现有技术中对安卓手机进行删除恢复的方法有主要是如下两种：

[0004] 1)第一种方法是通过制作手机的存储介质的镜像文件。

[0005] 如果使用简单的DD命令或其他镜像软件，由于受手机存储层使用的文件系统的结构限制，则不能获得到完整的文件系统的信息，得到的镜像文件无法重组还原成原来的文件系统。在不能重组还原文件系统的情况下，对具体删除信息的定位难度增加，对删除信息的识别及验证的难度增加，对删除信息与未删除信息进行区分的难度增加。

[0006] 如果使用复杂的外部工具虽然可以获得完整的镜像文件，但是如果镜像文件不完整或较大，再加上手机存储数据的复杂度影响，往往恢复出来的信息比较凌乱，或掺杂了很多完全无关的信息在里面，恢复的效果一般或很差。

[0007] 2)第二种方法是对信息存储文件进行定位后使用通用的方式进行处理。

[0008] 一般智能手机中的个人信息是存储在数据库文件中的，使用数据库查看工具可以查看到存储的表结构及字段信息，但是这些信息为存储而优化，所以在直接查看时，字段之间的关联等需要取证人员自己猜测和验证。而基于数据库存储结构恢复出来的字段信息，同样需要取证人员把这些信息关联起来，对取证人员的数据库专业知识要求较高，且在数据库表较多或表结构较复杂的情况下，准确性和可靠性会非常差。

[0009] 综上所述，针对现有技术的缺陷，特别需要一种快速恢复安卓手机删除信息的取证方法，以解决以上提到的不足。

发明内容

[0010] 本发明的目的在于提供一种快速恢复安卓手机删除信息的取证方法，

[0011] 克服了传统技术中的不足，从而实现本发明的目的。

[0012] 本发明所解决的技术问题可以采用以下技术方案来实现：

[0013] 一种快速恢复安卓手机删除信息的取证方法，所述方法包括如下步骤：

[0014] 1)首先使用安卓SDK中提供的调试开发工具Android Debug Bridge中提供的pull命令提取手机中的用户数据文件，并对其进行进一步分析，获取用户数据文件中的可

直接查看信息；

[0015] 2）通过 API 读取可直接查看信息中的数据内容，然后通过对比验证来确定数据内容中各字段的具体含义，重新组合后得到手机上的可见数据，同时也得到数据库表结构的存储特征；

[0016] 3）通过数据库表结构的存储特征分离出数据库中的未使用空间；

[0017] 4）通过分析安卓手机中正常记录的存储结构提取出正常记录的特征，然后通过正则表达式在未使用空间中尝试匹配该特征，并对匹配到的数据进行验证；如果其结构和正常记录相符合，则认为这是一条已经删除的记录，然后结合该记录的字段长度定义，将其后的数据进行分割，以还原其各主要字段的内容；

[0018] 5）将还原出来的数据与通过 API 解析的正常记录进行对比，如果关键信息完全相同，则认为这是一条逻辑上已存在或已经有相同的记录被恢复出来的冗余数据，不添加到记录列表中；如果关键信息不相同，则添加到记录列表中；

[0019] 6）继续匹配未使用空间中，直到所有的未使用空间都处理完毕。

[0020] 在本发明的一个实施例中，所述步骤 1）进一步包括一种获取 root 权限的方法，该方法为直接通过 adb root 提升外部的 root 权限；如果 adb root 提示无法提升到 root 权限，则通过一个临时 root 的脚本来提升到 root 用户的权限。

[0021] 在本发明的一个实施例中，所述步骤 5）中，将还原出来的数据添加到记录列表中的同时将该数据标记为已删除，表明这是一条被恢复出来的记录。

[0022] 在本发明的一个实施例中，所述用户数据文件为 SQLite3 数据库格式，通过 API 能正常的读取其中的数据内容。

[0023] 在本发明的一个实施例中，所述调试开发工具 Android Debug Bridge 通过应用程序调试接口连接手机。

[0024] 本发明的有益效果如下：

[0025] 1）快速恢复：该方法由于事先对用户数据库的表结构及存储结构进行了研究并提取了特征，所以在恢复删除信息的时候速度非常快。

[0026] 2）使用便捷：删除恢复在解析正常记录后自动进行，无需用户进行任何手动操作和分析。

[0027] 3）可靠性强：对由针对具体的特征进行扫描，针对性非常强，所以一般近期删除的数据都能恢复出来。

附图说明

[0028] 图 1 为本发明所述的快速恢复安卓手机删除信息的取证方法的流程示意图。

具体实施方式

[0029] 为使本发明实现的技术手段、创作特征、达成目的与功效易于明白了解，下面结合具体实施方式，进一步阐述本发明。

[0030] 如图 1 所示，本发明所述的一种快速恢复安卓手机删除信息的取证方法，它的工作步骤如下：

[0031] 1）首先需要确定目标手机是否已打开 USB 调试（应用程序调试接口），由于大部分

第三方手机管理软件都需要使用这个功能，所以大部分手机都已经开启。如果没有开启则需要到设置 -> 应用程序里打开。

[0032] 2）直接提取文件。使用安卓 SDK 中提供的调试开发工具 Android Debug Bridge(adb) 中提供的 pull 命令尝试提取手机中的用户数据文件(如通讯录文件 /data/data/com.android.providers.contacts/databases/contacts.db)，因为用户数据文件为私密信息，如果提示访问被拒绝，或权限不够之类的错误信息，则需要 root 权限才能访问。通过 adb root 尝试提升外部的 root 权限，继续通过上面的方法尝试提取用户数据文件。

[0033] 3）临时提升 Root 权限。如果 adb root 提示无法提升到 root 权限，则可以通过一个临时 root 的脚本(通过系统漏洞的方式)来提升到 root 用户的权限，在取得外部 root 权限的情况下，通常都能正常提取到文件。

[0034] 4）提取用户数据。提取到所需要的用户数据文件之后，首先需要提取用户已存在的数据(在手机能查看到的数据)，一般该文件是 SQLite3 数据库格式，通过其提供的 API 就能正常的读取其中的数据内容。由于没有原始设计文档，需要通过对比验证来确定各字段的具体含义，重新组合之后就能还原手机上的可见数据，同时也得到数据库表结构的存储特征。

[0035] 5)分离未使用空间。由于 SQLite 数据库是文件型数据库，其删除数据的操作只是标记该区域不再使用，所以删除之后的数据大部分还都保存在文件中，只是通过数据库查询的时候不再可见，以二进制的形式还访问到。可以通过研究数据库表结构的存储特征来分离出所有未使用的空间。

[0036] 6）恢复删除的数据。通过分析正常记录的存储结构来提取出记录的特征，然后通过正则的方式在未使用空间中尝试匹配该特征，对匹配到的数据进行验证，如果结构和正常的记录相符合，则认为这是一条已经删除的记录，然后结合记录的字段长度定义，将其后的数据进行分割，以还原其各主要字段的内容。

[0037] 7）过滤重复数据。将恢复出来的数据与通过 API 解析的正常记录进行对比，如果关键信息(如时间，内容，号码等)完全相同，刚认为这是一条冗余数据(逻辑上已存在或已经有相同的记录被恢复出来)。如果不是冗余数据则添加到记录列表中，同时标记为已删除，表明这是一条被恢复出来的记录。

[0038] 8）继续匹配未使用空间中的内容，直到所有的未使用空间都处理完毕。

[0039] 以上显示和描述了本发明的基本原理和主要特征和本发明的优点。本行业的技术人员应该了解，本发明不受上述实施例的限制，上述实施例和说明书中描述的只是说明本发明的原理，在不脱离本发明精神和范围的前提下，本发明还会有各种变化和改进，这些变化和改进都落入要求保护的本发明范围内。本发明要求保护范围由所附的权利要求书及其等效物界定。

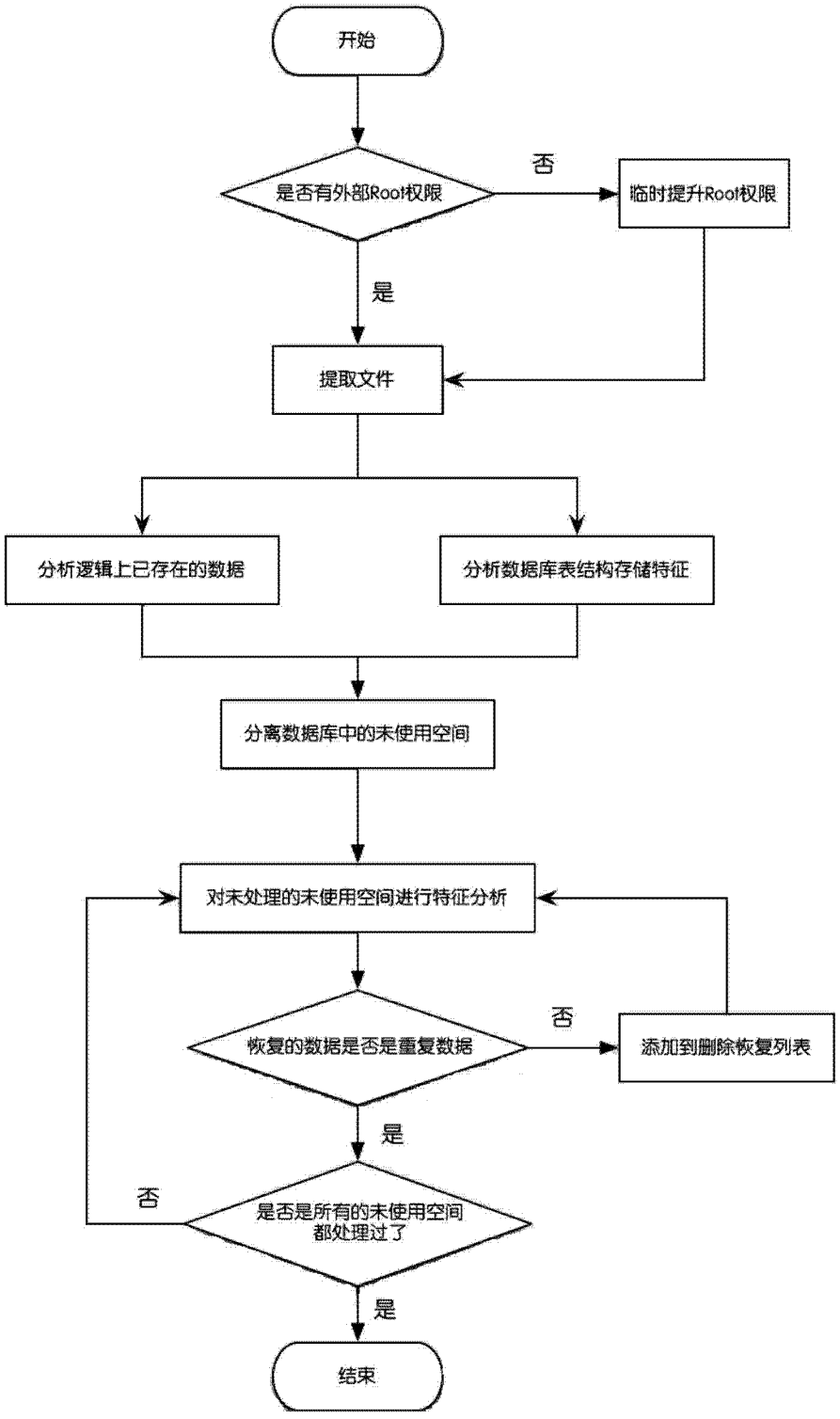

开始
是否有外部Root权限
否
临时提升Root权限
是
提取文件
分析逻辑上已存在的数据
分析数据库表结构存储特征
分离数据库中的未使用空间
对未处理的未使用空间进行特征分析
恢复的数据是否是重复数据
否
添加到删除恢复列表
是
否
是否是所有的未使用空间
都处理过了
是
结束

图 1