文章编号：2096-1472(2016)-03-06-03

一种基于备份的手机易失性数据获取方法

曹 飞[1]，胡 涛[2]
（1.重庆大学计算机学院，重庆 400044;
2.重庆市城投路桥管理有限公司，重庆 400044）

摘 要：首先介绍了智能设备进行易失性数据取证的重要性，并说明了其难点在于对易失性数据的获取上，其后介绍了几种易失性数据获取的方法。但是每种方法都有缺陷，因此提出了一种基于备份的易失性数据获取方法，没有使用环境的要求，也不会污染其他进程的易失性数据，对不同操作系统的支持也比较好，使得取证人员能够很方便获取重要的证据数据。

关键词：智能设备；易失性数据；取证；基于备份
中图分类号：TP309 **文献标识码**：A

A Method for Obtaining Mobile Phone Lost Data Based on Backup

CAO Fei[1],HU Tao[2]
(1.*College of Computer Science*,*Chongqing University*,*Chongqing* 400044,*China*;
2.*Chongqing Chengtou Road and Bridge Administration Co*.,*Ltd*.,*Chongqing* 400044,*China*)

Abstract: In this paper,we introduces the importance to carried out volatile data from smart devices and explains their difficulty lies in obtaining data on the volatile.Thereafter describes several methods to capture the volatile data.But all methods have different drawbacks,so we proposed a method based on backup of volatile data acquisition,which does not have environmental requirements,also will not contaminate other processes of volatile data,supports for different operating systems is relatively good,so that people can easily obtain evidence important evidence data.

Keywords:smart devices;volatile data;live forensics;backup

1 引言(Introduction)

随着科技进步和数字移动通信网络的普及，智能手机和平板电脑已经成为生活的必备工具。据统计，截止2015年2月，移动电话用户总数达到12.9亿，其中相当大的比例为智能手机用户。根据美国市场研究公司IDC发布的报告，2015年全球智能手机出货量增长10.4%，达到14.4亿部[1]。

与此同时，随机技术的发展，以智能手机为代表智能设备的计算能力越来越强大，使其在基本的电话和短信之外，具备了更多的功能，成为了人们工作、娱乐、交际的重要工具。甚至有人把以手机为代表的新兴传播形式称为继报纸、广播、电视、互联网之后的“第五媒体”。但是，智能设备在给人们带来遍历的背后，也常常被犯罪分子利用作为犯罪工具[2]。譬如，犯罪分子利用智能设备来诈骗、诽谤他人，甚至窥探、传播他人隐私，使其日渐成为新型犯罪工具。因此对智能设备的取证研究越来越重要，存在智能设备中的各类数据作为一种新的证据形式，也越来越多的作为诉讼证据之一，发挥了巨大的作用[3]。

当前大部分对智能设备的取证都是针对存储在内存卡和闪存上的非易失性数据取证的研究，比如。而对存储在运存上的易失性数据获取方法还比较少。然而由于手机厂商众多，并且同一个厂商的产品也具有不同的型号，使智能设备的易失性数据取证更加困难。本文既是提出一种方法来完成对不同设备的易失性数据的获取。

由于设备没有间断的运行，导致内存的数据在不断的变化中，特别是在手机在处于联网状态的时候，所以确定需要取证的时候，要首先完成对易失性数据的获取，并且不能修改设备的状态包括关闭网络连接、干扰手机信号等，因为这些操作的同时就会修改一些内部数据，从而造成数据的丢失。完成易失性数据的获取过后，在进行对非易失性数据进行取证调查[4]。

2 研究现状(Research status)

虽然现在没有一种统一方法来完成对智能设备的易失性数据获取，但是也有了很多相关的研究。由于智能设备也是电子随便的一种，因此取证方法和普通PC类似。易失性数据获取的一般方法就是断开网络，然后对当前内存数据进行镜像备份，最后通过对镜像进行分析，获取关键性证据信息。移动设备的操作系统是运行在有限资源之上的，内存的容量还是受限，因此其需要在未经用户许可的情况下移除一些优先级较低的进行，以分配内给优先级较高的进程。但是，有些重要证据就是存储在优先级较低的进程上的，因

此，在智能设备易失性数据电子取证的重点就是获取这些易失性数据[4]。

易失性数据的获取方法包括物理获取和逻辑获取。物理获取又叫硬件获取，通过独立的硬件设备完全绕过操作系统，且不在目标机上运行任何应用程序，最后完成将全部的物理内存的数据镜像拷贝到另外的存储设备之中。在普通的PC上面，物理获取的主要方法有通过PCI接口、FireWire接口等通过特殊的接口来实现。PCI接口通过预先安装特定的专用取证设备，利用DMA来获取对内存的直接访问，可以不依赖操作系统，不需要运额外的代码；缺点是不支持热拔插，需要预先安装。FireWire也是直接通过DMA访问，取证人员将一个包含适当程序并且能够向FireWire设计控制器发送特定的指令来启动设备。但是这些方法在移动智能设备上都不能使用，因为移动设备由于其小巧，不可能具有这么大的接口存在。逻辑获取也叫软件获取，通过安装特定的取证软件来访问内存数据，进而将其转储成物理镜像。在这方面，移动设备和普通PC的方法类似。

在智能移动设备的易失性数据获取上，研究人员也提出了许多不同的方法。Willassen提出了一种获取存储在易失性存储介质如RAM的物理获取方法[5]，需要拆卸手机进而从印刷版电路(PCB)获取到存储介质，然后使用JTAG芯片测试接口获取其中的易失性敏感数据。在这个过程之中，需要保持电源的持续连接，并且为了减少数据丢失的可能，需要对其进行降温处理。G.Me和A.Distefano提出了一个内部获取而不是通过USB等接口的外部获取方法，并完成了MIAT(Mobile Internal Acquisition Tool)工具，该工具需要安装在内存卡内部，使手机具有从内存获取数据能力，并在10到15分钟之内获取到内存上的所有数据。该工具存在的问题是需要手机重启一次且运行在恢复模式，然而在重启的过程中会修改一些文件和数据。但是，这些修改的数据是可以接受的，并且比一些常用的修改工具如Paraben和XRY的取证方法所修改的数据要少。

在另外一个研究上，Irwin和Hunt提供了一种使用网络连接来获取敏感数据的方法[6]，可以通过Wi-Fi或者GSM来完成，基于Windows Phone的。为了完成这项研究，他们开发出了四种工具来完成数据的获取和传输工作。第一个工具叫做CTASms(Contact、Task、Appointment和SMS)，完成从Windows Phone的PIM(个人信息管理中心)提取数据。这个工具通过复制PIM中的数据并发送到其他设备中来完成数据的获取功能。在这个工作中，需要使用到另外的两个工具：ActiveSync和DataGrabber。ActiveSync也是安装在手机上的，主要工作是使用网络连接来发送CTASms获取的数据到工作站上，完成同步工作。DataGabber设备就是安装在工作站上的工具，功能是接受ActiveSync发送的数据并分类存储。最后一个工具叫做SDCap(存储设备捕获)，通过远程连接安装有DataGrabber的工作站，获取到同步的数据并进行分析，完成最后的证据获取功能。由于需要使用移动网络，因此该研究的使用具有很大的局限性，并且在完成数据传输的过程中对易失性数据的修改也是比较多的。

此外，L.L.V.Thing和E.C.Chang提出一种自动执行易失性数据的分析方法[7]。他们通过研究易失性数据的动态行为，分析不同的应用数据的实时数据对证据呈现的重要性，找到了在不同的应用场景需要的不同参数。他们的实验表明，手机向外发送的数据比接受到的数据对取证分析上具有更大的作用，因此在数据获取的时候，应该更多的倾向于获取手机本身产生的数据。根据此原理，他们开发了一个数据获取工具MemGrab用来获取特定类型的易失性数据，并进行了后续分析。在一个实际的应用场景中，不管是连续发送还是间断发送，都能根据获取的数据分析出可信的证据信息。MemGrab跟踪系统调用的过程，控制其执行，获取对应进程的地址空间，然后在获取特定类型的数据快照，重点在于手机本身产生的数据而不是接受的数据。按照他们的观点来看，一个自动获取的系统需要及时的获取这些易失性数据。对于低持久性的数据，如果没有及时的获取则会直接丢失，这对取证工作造成了一定的困难。

3　基于备份的易失性数据获取方法(Volatile memory acquisition method based on backup)

为了克服上面的提到一些易失性数据获取方法的缺点，本文提出了一种基于备份的易失性数据获取方式，通过对特定易失性数据的备份来提高这些数据的持久能力，进而对这些数据进行分析，从而获取需要的电子证据。尽管手机型号多种多样，每种都有自己的设计和架构，但是他们具有一个相同的基于基本架构。因此，本文提出的方法可以通用大多数操作系统，包括Windows Phone、Android以及IOS等。

为了保存手机的易失性数据，提高其持久化能力，需要使用手机的部分内存作为备份存储空间来使用，重要的易失

性数据需要保存在这个备份空间里面。此备份存储在一定时间内更新的易失性数据，数据来源是其他正在该手机上运行的重要进程。根据预设的进程优先级，甚至可以做到当该进程已经被用户显示的终止，也可以在备份中找到该进程的重要易失性数据。通过这种方式，可以在调查过程中帮助取证人员获取重要的易失性数据，从而对取证过程产生积极的影响。

由于用户备份的空间有限，对于备份的数据选择就很重要。需要清楚地知道那些数据是过时的、不重要、不需要在处理的，需要在一定时间后将其从备份空间中删除。甚至是同一个进程的数据也有优先级的区分，根据上面提到的L.L.V.Thing和E.C.Chang的实验[7]表明，向外发送的数据比从外接收到的数据在取证过程中具有更高的重要性。当一个进程被终止过后，可以将其备份的数据在保存一段时间，如果一段时间过后没有其他的操作，则确定是过时的，将其自动删除。如果该进程重新运行了，则需要判断新产生的易失性数据是否具有更高的优先级，从而决定是否刷新以前备份的数据，具体流程如图1所示。

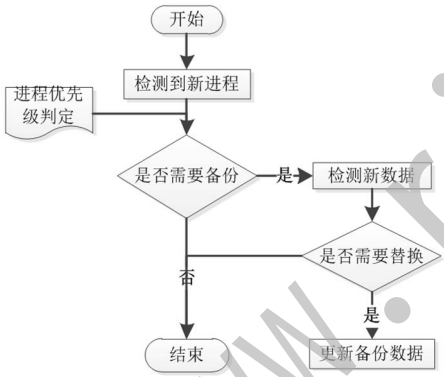

图1 数据备份流程

Fig.1 Procedures of data backup

通过这种办法，可以适当的提高一些易失性数据的持久化能力。此外为了更好的管理备份空间，需要对不同的进程进行优先级排序，这点可以通过调查人员以前的办案经验得到结果通过神经网络算法来获取不同进程的优先级。比如系统进程和日志等系统本身的数据，在调查过程中不具有比较好的证据效果，一般认为是最低的优先级的，而短信、聊天工具等具有更多的和用户行为相关的进程，其优先级应该是最高的。

以上介绍的方法不需要使用其他的额外的工具就能够获取到重要的易失性数据，并且不会修改手机中其他的数据，也不会产生额外的不必要的文件。这种方法也没有使用移动网络或Wi-Fi等网络连接，只需要通过USB数据线连接到电脑或者必要的时候直接生成一个文件就可以完成对重要易失性数据的获取，方便调查人员的调查工作。

4 结论(Conclusion)

通过备份重要进程的重要易失性数据，可以提高这些易失性数据的持久化能力，方便取证工作人员获取重要电子证据，因此本文具有一定的实用意义。但是该方法的缺陷非常明显，需要预先对待取证的手机进行操作，实现难度比较大，所以还需要一定的改进。

参考文献(References)

[1] Top Ten Smartphone Vendors Based on Market Share,http://www.dramexchange.com/ WeeklyResearch/Post/5/4272.html.

[2] 戴吉明.手机取证及其电子证据获取研究[J].计算机与现代化,2007(5):100-102.

[3] 殷联甫.计算机取证中的物理内存取证分析方法研究[J].计算机应用与软件,2010,27(12):295-298.

[4] 张瑜,等.内存取证研究与进展[J].软件学报,2015(5):1151-1172.

[5] Willassen S.Forensic Analysis of Mobile Phone Internal Memory[J].Ifip—the International Federation for Information Processing,2005,194:191-204.

[6] Irwin D,Hunt R.Forensic information acquisition in mobile networks[C]//Communications.Computers and Signal Processing,2009.PacRim 2009.IEEE Pacific Rim Conference on.IEEE,2009:163-168.

[7] Thing V,Ng K Y,Chang E C.Live memory forensics of mobile phones[J].Digital Investigation,2010,7(8):S74-S82.

作者简介：

曹 飞(1990-)，男，硕士生.研究领域：Android内存取证.

胡 涛(1963-)，男，学士，高级工程师.研究领域：桥梁结构与信息化管理.