文章编号：2095-2163(2020)03-0189-03 中图分类号：TP39 文献标志码：A

基于 Android 系统的微信语音数据司法取证研究

刘继莹，谭振江
（吉林师范大学 计算机学院，吉林 四平 136000）

摘 要：当下互联网技术发展迅速，各项工作均在迈向信息化道路。2017 年年末全国各地逐步地展开了监察体制改革工作，改革以来，通过对手机信息的提取、分析、整理，对案件的审查调查有着十分重要的作用。本文通过对 Android 手机中微信语音取证的研究探讨来推进案件的审查调查进度，提高案件办理效率。

关键词：Android 系统；微信语音取证；司法取证

Research on judicial forensics of WeChat voice data based on Android system

LIU Jiying, TAN Zhenjiang
(College of Computer Science, Jilin Normal University, Siping Jilin 136000, China)

【Abstract】 The current Internet technology is developing rapidly, and all work is on the road to informatization. At the end of 2017, the supervision system reform work was gradually carried out across the country. Since the reform, through the extraction, analysis and sorting of mobile phone information, it has played a very important role in the investigation and investigation of cases. This article promotes the progress of the case investigation and investigation through the research and discussion of WeChat voice forensics in Android phones, and improves the efficiency of the case inspection and supervision.

【Key words】 Android system; WeChat voice forensics; judicial forensics

0 引 言

2019 年 8 月 30 日，CNNIC 发布了第 44 次《中国互联网络发展状况统计报告》。报告中指出，截至到 2019 年 6 月，中国通过手机上网的民众数量已经达到 8.47 亿，占比高达 99.1%，较去年年底上升 0.5 个百分点[1]。2019 年上半年，手机上网用户使用的 App 中，即时通信类 App 的使用时间最长，其中微信则已成为备受大众青睐的最常用的通讯工具。因此，对于手机取证来说，微信取证具有极大的现实意义。微信可以实现文字、语音通信、文件传输、资金支付等功能，现已成为人们生活中不可缺少的通信工具。多数情况下，手机中存储了包括微信记录在内的大量信息[2-3]，在案件审查调查中手机微信取证工作起着不可或缺的作用。其一通过手机取证获取的信息可以直接作为证据；其二通过获取到的信息，特别是微信交互信息，可以提高案件破获效率。

1 手机数据取证基本理论

1.1 手机数据取证定义

Android 手机数据取证就是通过对被调查人使用过的手机中存储的数据进行技术提取，再将提取出的数据进行整合分析，既可为案件提供证据支持[4]，也可通过在手机中获取的信息找到案件的突破点。

1.2 手机数据取证内容

手机取证包含 2 部分内容，分别是：基本的数据信息；使用者在各类 App 程序中产生的数据记录信息，如微信语音记录、通话记录、浏览器搜索及浏览网页内容、各类支付软件中的资金交易信息等[5]。

1.3 手机数据取证步骤

步骤 1 获取到被调查人的手机是整个取证工作的基础，这个过程要严格履行相应的程序手续，同时要申请对被调查人手机取证的权限[6]。

步骤 2 保证电量，同时在开机后要将手机的网络断开或者将手机调至飞行模式，防止新数据的写入破坏原有记录[7]。

步骤 3 准备工作做好后，要按照规定的步骤对手机进行数据提取。

步骤 4 对提取出的数据进行分析研判，在其中寻找与案件相关的线索，最终形成取证报告[8]。

基金项目：赛尔网络下一代互联网技术创新项目(NGII20180408)；吉林省教研课题(高等学校学生实习、就业、创业人才共享服务平台建设和 2017ZCZ045、2019ZCY361)。

作者简介：刘继莹(1995-)，女，硕士研究生，主要研究方向：计算机应用技术；谭振江(1965-)，男，博士，教授，主要研究方向：计算机网络、信息安全。

收稿日期：2019-11-26

具体流程如图 1 所示。

图 1 手机数据取证步骤

Fig. 1 Mobile data forensics steps

2 Android 系统数据存储

研究可知,考虑到 Android 系统的开源性,即使得 Android 系统现已广泛应用于便携设备中。Android 系统有 5 种存储方式来存储不同类型的数据,具体阐述如下。

(1)SharedPreferences:存储应用程序的配置信息。

(2)Files:存储大容量数据。

(3)SQLite DataBase:存储用户的所有个人数据。

(4)ContenеProvider:实现各程序间的数据共享。

(5)网络:通过连接网络来获取应用程序所需要的数据。

3 微信语音取证工作

3.1 微信语音数据的存放路径

在内部存储下有一个 Tencent 目录[9],Tencent 是腾讯手机 App 数据存放目录。Tencent 下的 MicroMsg 目录中存储着微信用户的多媒体文件,如图 2 所示,包括接收的图片、语音、视频等信息。有时候,会用手机登录不同的微信账号,每登录一个账号,"/Tencent/MicroMsg/"路径下就会创建一个登录账号对应的文件[10]。文件下有一个 voice2 目录,目录中就存储着人们要找的微信语音记录。找到其下第三层中的.amr 文件,这就是微信语音存储文件,如图 3 所示。

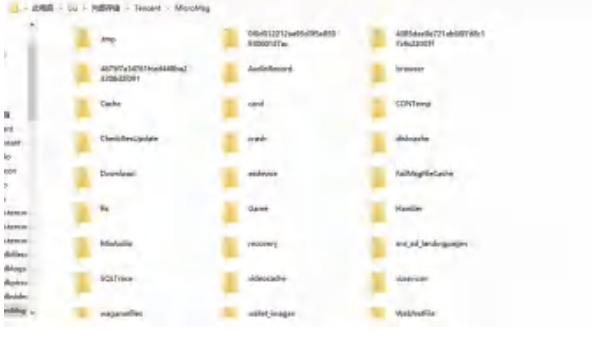

图 2 MicroMsg 目录

Fig. 2 MicroMsg directory

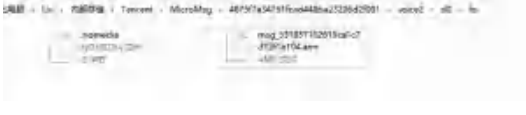

图 3 微信语音文件

Fig. 3 WeChat voice file

3.2 微信语音文件播放

通过存储路径,很容易就找到了微信语音文件,将其拷贝后,但却会发现并不能直接将拷贝得到的.amr 文件顺利播放出来。在语音聊天信息存储时,微信对其文件格式做了特别的处理,此时如果想要播放语音文件,就要对获取到的.amr 文件进行还原解码。大部分.amr 文件以 SILK_V3 开头,若要还原成可正常播放的文件,就要将微信做出的处理加以还原。总地来说,就是要跳过.amr 文件的前 10 个字节,再把第 11、12 字节的值组成的十进制整数记作 N, 真正的 Silk 数据是从第 13 字节数 N 个字节后开始的,而此前的字节在将其删除后,获取到 Silk 数据,通过调用 Skype 公开算法对数据进行解码,将其转成 MP3 格式,就可以正常播放了。

操作过程如下:用 WinHex 工具来修改.amr 文件的文件头信息,如图 4 所示。首先删掉开头的前 10 个字节"0x02 0x23 0x21 0x53 0x49 0x4C 0x4B 0x5F 0x56 0x33"。找到第 11、12 字节,从图 4 中看即为"0x0C"和"0x00",组成十进制整数 13,13 就是数据偏移量,因此从"0xA7"开始的 13 个字节"0xA7 0x2B 0x74 0xF7 0xA8 0xEE 0x49 0xE5 0xE0 0x23 0x70 0x43 0x0B"后才是音频文件真正的开始位置。经修改文件头信息后,再通过音频转换算法将文件转换成 MP3 格式。

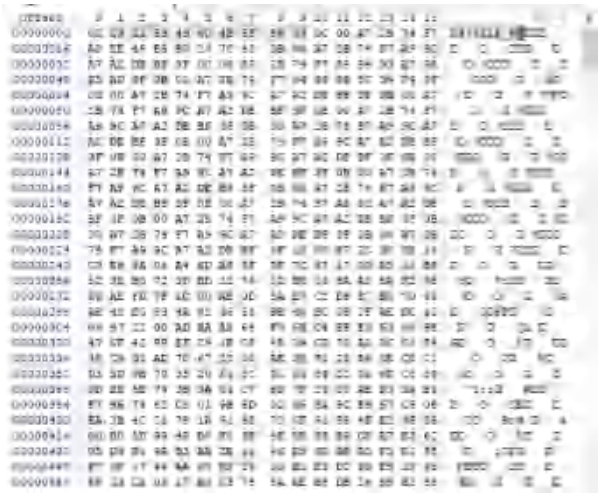

图 4 .amr 文件信息

Fig. 4 .amr file information

3.3 .amr 文件与微信语音关联

voice2 目录下的每一个.amr 文件都是一条微信语音记录[11],但为了将.amr 文件同聊天消息关联上,通过研究发现在每个.amr 文件上有 2 层目录,如图 5 所示。"d0"、"fe",是十六进制字符,这两个字符是与语音消息相关联的重要标识,通过此标识就

可以将.amr 文件与对应聊天消息关联上[12]。

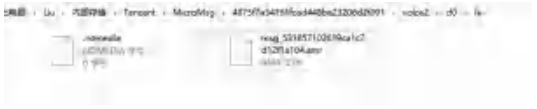

图 5　微信语音文件上两层目录

Fig. 5　Two-layer directory on WeChat voice file

在微信数据库文件中，找到名为 message 的数据表，这个数据表中就记录了语音消息的相应信息。在 message 数据表中有 type 字段和 imgPath 字段。当 type 字段的值为 34 时，此条记录为语音记录；imgPath 中的内容的 MD5 值是 16 字节编码，该编码前 2 个字节就是上述路径中的标识，以此实现.amr 文件同消息的关联[13]。

3.4　EnMicroMsg.db 数据库文件

3.4.1　微信数据库文件

Android 手机中的数据库文件存放在/data/data/com.tencent.mm 中，名为 EnMicroMsg.db。要想找到并拷贝出 EnMicroMsg.db 文件，就要将手机 ROOT 得到最高权限[14]。在 ROOT 过的手机中将 EnMicroMsg.db 文件拷贝出来，该文件是经过严格加密保存的，要将其打开还需要得到 EnMicroMsg.db 数据库文件密码[15]，获得密码的前提是先获取 IMEI 和 UIN。

3.4.2　获取 IMEI

IMEI 是识别码。IMEI 获取方式有 2 种方式。第一种，通过系统的配置文件 Compatible.cfg 中获取 IMEI 码。第二种，手机开机后跳转至拨号页面，键入”＊ # 06 #”后，就可以查看到 IMEI 码。

3.4.3　获取 UIN

UIN 是 user information。在”/data/data/com.tencent.mm”下的 shared_prefs 目录中存储着 system_config_prefs.xml、app_brand_global_sp.xml 文件，从中就可以获取到 UIN。

UIN 码是计算密钥的关键元素，而多个微信账号登录同一个 Android 手机时，在配置文件 system_config_ prefs.xml 中只保存最后一个登录的 UIN 码。获取其他账户的信息，必须利用保留在手机中的每个账号的 32 位缓存文件名，udir_name =MD5(mm+uin)。依据已知的 32 位文件名得到对应的 UIN。

3.4.4　EnMicroMsg.db 文件密码

要想破解EnMicroMsg.db文件的密码，就要知道其密码的算法，算法为把 IMEI 与 UIN 拼接后计算 32 位 MD5 值，在此基础上选取前 7 位，如图 6 所示。

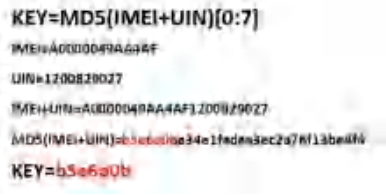

图 6　EnMicroMsg.db 文件密码获取过程

Fig. 6　EnMicroMsg.db file password acquisition process

4　结束语

本文通过对 Android 手机中的微信语音数据文件进行提取、并与微信聊天消息相关联、最后对.amr 文件还原解码播放，来达到微信语音数据成功取证，以此实现通过对微信语音数据取证工作来推进案件的审查调查进度，提高办案效率。本文研究具有重要的现实意义。

参考文献

[1] 于朝晖. CNNIC 发布第 44 次《中国互联网络发展状况统计报告》[J]. 网情军民融合，2019(9)：30.

[2] 潘其凡. 现行监察体制下职务犯罪调查权问题研究[D]. 上海：华东政法大学，2018.

[3] 黄鑫. 国家监察体制改革法治化构建之维—兼论“社会中心主义”与反腐“理性构建”[J]. 时代法学，2018，16(5)：64.

[4] 李佳. 微信语音鉴定意见的审查[J]. 人民检察，2018(2)：12.

[5] 罗建利. Android 手机数据取证在案件侦破中的应用研究[D]. 广州：华南理工大学，2016.

[6] 王弈. 手机取证规范化研究[J]. 电信科学，2010，26(S2)：65.

[7] 杨雪. Android 手机取证技术研究综述[J]. 计算机时代，2015(6)：7.

[8] 孙波，孙玉芳，张相锋，等. 电子数据取证研究概述[J]. 计算机科学，2005，32(2)：13.

[9] PEREIRA M T. Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records[J]. Digital Investigation，2009，5(3-4)：93.

[10] 张艳姣，曾光裕，冯培均，等. 一种基于 Android 平台的微信取证分析方法[J]. 信息工程大学学报，2018，19(6)：719.

[11] 王伟兵，文伯聪，吴琪. 复杂条件下的 Android 版微信取证方法研究[J]. 网络安全技术与应用，2017(8)：170.

[12] SANGJUN J，JEWAN B，KEUNDUCK B，et al. A recovery method of deleted record for SQLite database[J]. Personal and Ubiquitous Computing，2012，16(6)：707.

[13] 黄平，周俊峰，陶远辉. Android 手机微信语音聊天数据提取研究[J]. 警察技术，2017(2)：64.

[14] 陈丹. 基于 Android 平台的手机取证技术[J]. 信息与电脑(理论版)，2019(5)：186.

[15] 金波，吴松洋，熊雄，等. 新型智能终端取证技术研究[J]. 信息安全学报，2016，1(3)：37.