doi 10.3969/j.issn.1671-1122.2016.01.008

# 一种 Android 系统下的 QQ 取证模型分析

李强[1,2]，刘宝旭[1]，姜政伟[1]，严坚[1]
（1. 中国科学院信息工程研究所，北京 100093；2. 中国科学院大学，北京 100049）

摘 要：作为 Android 智能终端上一款装机量较大的社交类即时通信应用程序，手机 QQ 上保存着各类丰富的用户数据，甚至可作为证据的信息，对其的取证分析研究有着重要的意义。文章首先介绍了 Android 系统和手机 QQ 的基本情况，并对国内外取证模型和移动终端即时通信应用的取证研究现状进行介绍，随后参考传统的数字取证分析模型，结合 Android 移动智能设备和 QQ 的特点，提出了一种 Android 系统下的 QQ 取证分析模型，并对模型的 9 个阶段工作内容和输出进行说明。最后，按照数据获取能力、数据可信性评价能力、取证结果机器可读能力 3 个评价指标，将基于分析模型开发的原型系统与典型的商用数字取证分析软件进行测试对比，结果表明本文模型在 Android 系统下的 QQ 取证分析具有明显优势。

关键词：Android；手机 QQ；取证；分析模型
中图分类号：TP309 文献标识码：A 文章编号：1671-1122（2016）01-0040-05

中文引用格式：李强，刘宝旭，姜政伟，等 . 一种 Android 系统下的 QQ 取证分析模型分析 [J]. 信息网络安全，2016（1）：40-44.

英文引用格式：LI Qiang, LIU Baoxu, JIANG Zhengwei, et al. Analysis of Model of QQ Forensic in Android System[J]. Netinfo Security, 2016 (1) : 40-44.

## Analysis of Model of QQ Forensic in Android System

LI Qiang[1,2], LIU Baoxu[1], JIANG Zhengwei[1], YAN Jian[1]
(1. *Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*; 2.*University of Chinese Academy of Sciences, Beijing* 100049, *China*)

**Abstract:** As one of popular instant messaging applications on smart phone, mobile QQ contains many kinds of user data which even includes the information of evidence, so forensic analysis for mobile QQ is significant. Firstly, this paper introduces the basic information of Android and mobile QQ, and the research status of forensic model and social network instant messaging application on smart phone. Then, referring to traditional digital forensic models and features of Android mobile intelligent device and mobile QQ, this paper comes up with an analysis model of QQ forensic in Android system, and introduces the detail and output at nine phases. Finally, according to three evaluation parameters as follows: ability of data acquisition, ability of data trustworthiness evaluation and ability of machine readable analysis result, the paper compares the prototype based on analysis model with two typical commercial digital forensic software, and the comparative result shows that the analysis model has a couple of advantages in QQ forensic analysis in Android system.

**Key words:** Android; mobile QQ; forensic; analysis model

收稿日期：2015-09-15
基金项目：国家高技术研究发展计划（国家 863 计划）[2015AA017204]
作者简介：李强（1992—），男，江西，博士研究生，主要研究方向为高级威胁检测、攻击溯源取证等；刘宝旭（1972—），男，山东，研究员，博士，主要研究方向为网络与信息安全、攻防对抗、网络安全评测技术等；姜政伟（1985—），男，湖南，助理研究员，博士，主要研究方向为态势感知、网络安全评测技术；严坚（1985—），男，广西，工程师，本科，主要研究方向为数字取证。
通信作者：李强 liqiang@ihep.ac.cn

## 0 引言

Android 系统作为一个开源的移动设备操作系统，其装机量已达 20 亿部，已经超越 Windows，成为全球使用最多最广泛的操作系统。我国作为全球最大的智能手机消费市场，有着数量庞大的安装了 Android 系统的移动设备，市场调研公司 Kantar 最新发布的智能手机市场份额报告 [1] 显示，截止到 2015 年 8 月，在中国市场 Android 操作系统的份额达到 78.1%。即时通信应用作为 Android 系统上普遍安装的应用程序，有着较大规模的用户群体，《第 36 次中国互联网络发展状况统计报告》[2] 显示，截止到 2015 年 6 月，网民中即时通信用户的规模达到 6.06 亿，其中手机即时通信用户 5.40 亿，占手机网民的 91%，腾讯旗下即时通信产品 QQ 和微信在该领域维持优势地位。

手机 QQ 作为 QQ 即时通信体系中重要的一员，依靠传统电脑版 QQ 多年对用户的积累，培养了用户在日常生活中使用 QQ 沟通的习惯，手机 QQ 已成为智能手机中装机量庞大的一款社交类即时通信软件。手机 QQ 有着丰富多样的功能 ：支持发送语音短信、视频、图片和文字 ；支持账号关联 ；支持群聊、群相册、群文件等群组功能 ；支持讨论组功能 ；支持查看所在位置附近的人 ；支持与电脑互传文件、QQ 邮箱、QQ 钱包 - 红包、银行卡 IC 支付、QQ 空间、游戏、购物等功能。另外，QQ 还支持消息记录保存在云端，并可以实现电脑版 QQ 和手机 QQ 同步。

手机 QQ 丰富的功能，在给人们生活带来便利的同时，也为不法分子实施网络诈骗和网络攻击提供了便利。手机 QQ 中不仅可以保存与电脑版 QQ 相同的消息记录，还保存着更多的手机用户数据信息。用户可能会在手机 QQ 中收到诈骗信息，甚至会被黑客利用手机 QQ 植入木马程序，而犯罪分子的手机 QQ 中则可能存储着与犯罪活动相关的信息。因此，针对 Android 系统下的 QQ 取证分析，对于维护网民权益，打击网络犯罪，有着重要作用。

## 1 研究现状

随着智能手机的广泛应用，移动智能终端取证逐步成为许多学者和企业的研究热点，即时通讯应用取证是移动智能终端取证的重要组成部分，主要包括取证模型、即时通讯应用中数据分析等研究内容。

针对移动智能终端取证模型的研究主要集中在取证流程模型上，PERUMALT[3] 通过分析现有的取证流程模型，包括 Kruse&Heiser 电子取证调查模型、Lee 的科技犯罪案件调查模型、Casey 的电子取证框架模型、DFRWS 调查模型等，基于马来西亚案件调查流程，提出了针对完整调查流程的取证模型。该模型将电子取证调查分为计划、鉴定、侦查、分析、结果、证据和辩护、信息扩散 7 个阶段，并对每个阶段具体的工作内容进行介绍和说明 ；RAMABHADRAN[4] 通过分析 Windows 手机设备的硬件结构，提出了 Windows 手机设备取证阶段模型，该模型将取证分为准备、保护现场、调查和识别、记录现场、通信屏蔽、易失性证据收集、非易失性证据收集、保存、检查、分析、展示、评审共 12 个阶段，并对各个阶段的具体工作内容进行介绍。目前各类电子取证模型多数都是基于传统 PC 电子取证的流程规范，针对移动智能终端的电子取证模型的研究还比较少，对于移动智能终端电子取证的思考和分析也不够全面和深入。

针对即时通信应用的数据分析主要集中在对提取的 SQLite 文件结构和数据内容的分析上，MAHAJAN[5] 等以 WhatsAPP 和 Viber 为例，对 Android 设备上的即时通信应用取证进行研究，并对这两款应用的功能特点、数据目录结构、SQLite 文件结构和内容进行比较和分析 ；THAKUR[6] 针对 Android 系统下的 WhatAPP 应用的用户文件目录结构和 SQLite 文件结构进行分析 ；FENG GAO[7] 等人使用多种电子取证分析软件针对 iPhone 中 WeChat 数据进行分析，包括 SQLite 文件、音频文件、视频文件等 ；吴熙曦 [8] 等人针对 Android 智能手机中微信会话消息的相似度特点，提出了利用 KNN 聚类分析算法来找到相似主题的会话消息，以此来找出与犯罪案件相关的数据信息。当前针对即时通信应用的分析主要还是侧重在针对特定版本应用的文件目录和数据内容的基础分析，针对 Android 系统下的 QQ 取证分析还比较少，特别是缺乏对手机 QQ 数据的全面深度分析和可信性评估的研究。

此外，知名的国际数字取证公司研发的数字取证软件对 Android 系统下的 QQ 取证分析支持度一般，而国内前沿的电子取证厂商美亚柏科研发的 DC-4500 和盘石软件 SafeMobile 支持部分手机 QQ 数据的导出和分析，但支持

提取的数据内容有限，对提取数据的可信性也没有验证。

## 2 关键技术

Android 系统下的 QQ 取证分析的基础是 Android 系统取证。本文通过参考传统的数字取证分析模型 [9]，结合 Android 移动智能设备和 QQ 的特点，提出了一种 Android 系统下的 QQ 取证分析模型，如图 1 所示。


图1 Android系统下QQ取证分析模型

图 1 左侧介绍的是该模型针对 Android 系统下 QQ 取证分析的主要分析阶段，包括意识、准备、保护现场、记录现场、数据收集、保存、检查、分析、评审 9 个活动阶段。活动阶段具体的工作内容以及输出在图的右侧。此外，该模型允许取证分析人员根据案件调查的实际情况返回到上一个阶段，便于取证分析人员获取更多的证据信息，或者重新确定后续得出的分析结果。各分析阶段的含义如下：

1）意识

鉴于 Android 取证分析对时间要求比较高，取证分析人员需要有较强的取证意识以保证能够及时取证。意识作为分析模型中的第一个阶段贯穿整个取证流程。

2）准备

在该阶段，取证分析人员需要在得到机构授权和相关法律法规下开展，通过了解数字取证案件的外延背景、案件环境、智能手机设备等相关信息，取证分析人员制定出详细的取证方案。

3）保护现场

Android 智能手机设备可以通过无线网络与外界连接，由于无线信号隐蔽性较强，在对 Android 智能手机实施数据取证之前，需要针对手机实施通信屏蔽措施，以确保手机中的数据不受无线信号的干扰。具体方法有通信屏蔽设备或者专用的信号屏蔽室等。

4）记录现场

该阶段取证人员的主要工作是从 Android 智能手机设备中提取原始的数据信息，技术手段包括手机芯片直读、手机镜像提取或者直接读出关键位置的数据目录信息。可以根据案件实际情况采取相应的数据提取方法，以上 3 种方式均可以获取到 Android 系统上的 QQ 数据信息。

5）数据收集

本阶段的重点在于从 Android 手机镜像、文件目录中提取出与手机 QQ 及案件相关的数据信息，根据手机 QQ 的数据存储特征，可以将关联数据分为易失性数据、非易失性数据和离线 / 云数据。另外，基站信息对于数字取证案件可能也会有帮助。

6）保存

提取出的手机 QQ 关联的原始数据信息需要刻盘备份保存，对数字证据做好备案。

7）检查

传统 PC 取证的重点是磁盘，以磁盘挂载的方式进行取证操作，不会破坏原始数据。而针对移动智能设备的取证则不同，除非在特殊情况下需要对手机芯片进行拆解外，正常情况下都是在 Android 智能手机开机状态下进行数字取证操作。同时，为完整提取 QQ 相关数据，在操作之前还需要获取 Root 权限。每次 Android 智能手机重启操作和 Root 权限获取操作均会不同程度地改变 Android 智能手机上的数据，这些操作是否改变了

Android 智能手机上 QQ 相关数据，改变的这些数据对于案件是否有影响，都需要进行检查和分析，以确保提取数字证据的可信性。

8) 分析

本阶段的工作内容有：针对基础数据和新功能数据进行分析，形成分析报告和可交换证据。基础数据分析针对 QQ 用户的通信相关信息，包括个人信息、好友信息、群组信息、会话信息等。新功能数据分析针对 Android 系统下的 QQ 软件不断推出的新功能应用产生的数据，包括 QQ 钱包、QQ 红包、银行卡 IC 支付等新功能应用信息。由于 Android 系统下不同版本的 QQ 文件存储结构和数据存储特点不同，在提取和分析手机 QQ 数据信息时，需要根据 QQ 的版本信息，采取对应数据分析方法。例如，在分析 Android 系统下 QQ 的 V5.7.1.2485 版本时，可以从目录文件 /data/data/com.tencent.mobileqq/databases/QQ 号 .db 中找到保存该 QQ 号聊天记录的 SQLite 文件，查看聊天记录文件数据是否已被加密，如图 2 所示。通过查找资料和对加密数据的深入分析，发现加密数据为原信息与手机 IMEI 号进行异或加密生成，IMEI 号存储在 /data/data/com.tencent.mobileqq/files/imei 文件中，通过编写相应的解密程序，可以对原会话记录进行提取和分析。

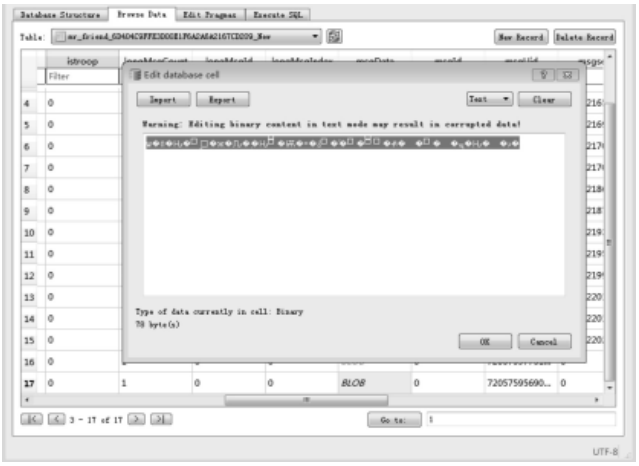

图2 使用Browser for SQLite查看聊天记录显示为乱码

分析完成后，整理并输出 QQ 数字取证分析报告。此外，模型还充分考虑了可能的证据交换需求，支持手机 QQ 取证分析结果以规范的 JSON 和 XML 格式导出，满足机器可读的需求。

9) 评审

该阶段主要是对手机 QQ 取证分析整体流程和分析报告进行评审，评审内容包括：取证流程是否合规合法、取证手段是否合理科学、取证报告是否规范准确等，最终根据评审结果判断此次手机 QQ 取证分析及分析结果是否具有证据效力。

## 3 评价及比较

Android 系统下的 QQ 取证是移动智能终端数字取证调查中的重要内容，对于取证分析的评价必须结合实际的取证调查问题和移动智能终端设备的特点 [10]，如 Android 移动智能终端中 QQ 应用软件的数据获取、鉴别和分析等。结合传统数字取证技术评价指标以及在实际取证业务中数据关联性分析和深度挖掘的需求，Android 系统下的 QQ 取证分析的评价指标如下：

1) 数据获取能力。数据收集和获取是 Android 系统 QQ 取证分析的核心环节，获取完整、准确的 QQ 数据，对于数据分析以及案件证据获取都有着重要的意义。从数据存储方面考虑，可以从 Android 智能终端提取易失性 QQ 数据、非易失性 QQ 数据，还可以通过其他方法获取 QQ 的云数据等信息。数据获取能力是评价取证分析的基本指标。

2) 数据可信性评价能力。如何保证从 Android 智能终端获取的 QQ 数据是真实的、有证据效力的数据，数据的可信性如何，如何对提取的数据的可信性进行评价，评价的过程和结果是否可以校验，是 Android 系统下的 QQ 取证分析需要考虑的重要内容。

3) 取证结果机器可读能力。在真实的取证调查案件中，取证数据获取来源和渠道是多元的，将获取的结果数据按照规定的格式进行存储和导出，为后续的关联分析做准备。支持 Android 系统下 QQ 取证数据的机器可读能力，是移动互联网时代背景下，对数字取证以及情报交换提出的新的要求。

综合上述评价指标，将基于本文提出的取证分析模型研发的原型系统与典型的商用数字取证分析软件进行测试比较，商用数字取证软件选用美亚 DC-4500 和盘石 SafeMobile，测试 Android 手机为 Nexus4，测试手机 QQ 版本为从 V1.0 到最新 V5.9.5 的多个版本，比较结果如表 1 所示。

表1 手机QQ取证分析效果对比分析表

| | | 美亚 DC-4500 | 盘石 SafeMobile | 基于模型的原型系统 |
|---|---|---|---|---|
| 数据获取能力 | 支持版本 | 从V1.0到V5.9.5 | 从V1.0到V5.9.5 | 从V1.0到V5.9.5 |
| | 支持获取数据类型 | 非易失性数据 | 非易失性数据 | 易失性数据<br>非易失性数据<br>离线/云数据 |
| | 支持获取数据内容 | 基础数据 | 基础数据 | 基础数据<br>新功能数据 |
| 可信性评价能力 | | 不支持 | 不支持 | 支持 |
| 机器可读能力 | | 支持 HTML 格式<br>CSV 格式（取证列表）<br>XML 格式（面向取证云） | 支持 HTML 格式 | 支持 JSON/XML 格式 |

从实际对比测试中发现，三者对 Android 系统下的加密 QQ 数据均可解密，并能支持到最新的 V5.9.5 版本。美亚 DC-4500 和盘石 SafeMobile 提取的数据内容为以 SQLite 数据库为主的基础数据，包括账号信息、好友列表、群信息列表、群列表、讨论组列表、讨论组、聊天记录等，而原型系统还支持获取易失性数据和离线 / 云数据以及 QQ 钱包、QQ 红包等新功能数据信息。同时原型系统还支持对提取数字证据的可信性评价。另外，在取证结果数据机器可读能力方面，美亚 DC-4500 和盘石 SafeMobile 均支持 HTML 格式导出结果报告，美亚 DC-4500 还支持 CSV 格式导出取证列表，支持 XML 格式导出报告到加密压缩包中，以用于上传到最高检察院和美亚柏科合建的“ 取证云 ” 中，原型系统支持取证结果以 JSON 和 XML 格式导出。对比可以发现，相较于商用数字取证软件，原型系统在针对特定机型的 QQ 取证分析中有一定的优势。

## 4 结束语

传统的移动智能终端即时通信应用的取证研究主要集中在取证流程和基础数据的提取上，这类取证分析存在流程规范不严谨、提取数据不完整等问题。本文根据 Android 系统下的 QQ 取证分析的特点，提出了一种 Android 系统下的 QQ 取证分析模型，模型具有较规范的取证流程和较完整的 QQ 数据提取方法，并支持对取证分析结果进行格式化处理，便于后续深度关联分析。最后，本文还将基于分析模型研发的原型系统与两款商用数字取证软件做比较测试，对比结果显示，本文提出的 Android 系统下的 QQ 取证分析模型在规范 QQ 取证流程和数据获取方面有一定的优势。（责编 程斌）

参考文献：
[1] 刘浩阳 . Android 设备取证研究 [J]. 信息网络安全，2015（9）：29-32.
[2] 第 36 次中国互联网络发展状况统计报告 [R]. 北京 ：中国互联网络信息中心，2015.
[3]PERUMAL S. Digital Forensic Model Mased on Malaysian Investigation Process[J]. International Journal of Computer Science and Network Security, 2009, 9(8): 38-44.
[4]RAMABHADRAN A. Forensic Investigation Process Model for Windows Mobile devices[J]. Tata Elxsi Security Group, 2007: 1-16.
[5]MAHAJAN A, Dahiya M S, Sanghvi H P. Forensic Analysis of Instant Messenger Applications on Android Devices[J]. International Journal of Computer Applications, 2013, 68(8):38-44.
[6]THAKUR N S. Forensic Analysis of WhatsApp on Android Smartphones[D]. Lovisiana: University of New Orleans. 2013.
[7]GAO Feng, ZHANG Ying. Analysis of WeChat on iPhone[C]// 3CA 2013.2nd International Symposium on Computer, Communication, Control and Automation，December 1-2 2013，Singapore. Paris Atlantis Press，2013 ：278-281.
[8] 吴熙曦，李炳龙，张天琪 . 基于 KNN 的 Android 智能手机微信取证方法 [J]. 山东大学学报（理学版），2014，49（9）：150-153.
[9] 李炳龙，贾俊峰，王清贤，等 . 文档碎片取证分析模型 [J]. 郑州大学学报 ：理学版，2008（3）：64-68.
[10] 尚士泽，孔祥维，尤新刚 . 伪造变造文件数字被动无损取证技术综述 [J]. 信息网络安全，2015（4）：62-67.