doi: 10.3969/j.issn.1671-1122.2012.05.025

手机规范取证研究

丁红军

（天津公安警官职业学院侦查系，天津 300382）

摘 要：在司法实践中，涉及到手机的案件越来越多，手机取证的重要性日益突出，但在取证中却存在着立法滞后，移动通信技术检验机构不完善，缺少高素质的取证人员，技术落后，缺乏取证的意识和流程不规范等问题，阻碍了手机电子证据在司法实践中的应用。文章针对手机取证中存在的问题，探讨了规范手机取证的方法，为手机取证的规范化提供理论参考。

关键词：电子证据；手机取证；执法规范化

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1671-1122（2012）05-0088-04

The Study of Mobile Phone Forensics Normalization

DING Hong-jun

(Investigation Department, Tianjin Public Security Police Profession College, Tianjin 300382, China)

Abstract: In the judicial practice, more and more cases involving mobile phone, the importance of mobile phone forensics is becoming increasingly conspicuous, however, several challenges have been met in the mobile phone forensics, such as legislative lag, mobile communication technology complex, inspection body imperfect, short of high-quality forensics officers, lag in technology, lack of mobile phone forensics consciousness and process is not standard, all these have hindered the application of mobile electronic evidence in the judging practice. The article focuses on the problems of mobile phone forensics and discuss the methods of specification of electronic evidence collection, in order to provide the theoretical reference to enforcement normalization of mobile phone forensics.

Key words: electronic evidence; mobile phone forensics; enforcement normalization

0 引言

随着我国经济的高速发展，移动通讯用户不断增加，手机作为现代社会最重要的通讯工具之一，被越来越广泛地使用。手机在给人们生活带来极大便利的同时，利用手机从事诈骗、传播有害淫秽色情信息、金融犯罪、售假、造谣、煽动作案[1]等违法犯罪活动日益猖獗，作为作案工具，犯罪嫌疑人使用的手机上往往存储着大量的与犯罪有关的信息，可为侦查破案提供一定的线索或证据。

1 手机取证的特点

手机取证是指用物证鉴定的原理、方法和程序，提取和分析手机中包含的信息，用作犯罪侦查线索或法庭证据[2]。虽然在计算机取证领域的很多研究成果和实践经验可以用于手机取证，但不同于计算机取证，手机作为移动终端，取证的特点有：取证对象具有很强的移动性；取证的范围不断扩大；文件系统存在于具有非易失性的存储中，数据规范不统一；手机种类繁多，操作系统多样；产品周期非常短[3]等。

2 手机取证面临的问题

手机中的电子信息（如通话记录、短信、图片、视频等）从表现形式上属于电子证据（电子证据是以电子形式存在的、借助信息技术或信息设备形成的用作证据使用的一切数据及其派生物[4]），手机取证应由具备合法资质的侦查人员遵循法律、法规的规定，使用合法的技术手段，才能完成取证的工作，打击犯罪。但是，相对已基本成熟的计算机物证检验，手机取证尚处于起步阶段，在取证中还存在以下问题，阻碍了手机电子证据在司法实践的应用。

2.1 立法滞后

根据《刑事诉讼法》规定“证明案件真实情况的一切事实都是证据”，只要能证明案件事实，无论什么形式的依据都可以作为证据，电子证据在诉讼中可以作为证据使用。但是我国证据立法只规定了书证、物证、视听资料等七种形式的证据，电子证据

收稿时间：2012-03-12

基金项目：天津市高等职业技术教育研究会2011年度课题“信息侦查中手机取证课程设置研究”[X1501]

作者简介：丁红军（1980-），男，山东，讲师，硕士研究生，主要研究方向：电子物证、侦查、图像处理。

还不是一种独立的证据形式，因此，手机电子信息作为证据使用存在一定难度，影响了取证效率和司法的公正[5]。

2.2 移动通信现状复杂

1）手机实名制滞后。虽然手机实名制（用户办理手机入网必须持身份证进行实名登记）于2010年9月1日起正式实施，但由于机主信息实名制的落实不到位，未实行实名登记的用户超过3.2亿，导致机主信息往往存在机主资料残缺、虚假等现象，而违法犯罪人员反侦查能力的日益增强，导致侦查人员单纯依靠手机话单分析往往无法直接锁定犯罪嫌疑人[6]。

2）山寨手机的冲击。按照国际标准，每一部正规手机都有一个国际移动设备识别码（IMEI），相当于手机的“身份证”，此码具有全球唯一性。由于山寨手机（山寨手机是一些小的手机厂商，以极低的成本模仿主流手机品牌产品的外观或功能，并加以创新，最终在外观、功能、价格等方面全面超越这个产品的手机）不需要做入网检测，经常通过伪造IMEI号码进行销售，几百、上千部手机可能只用一个IMEI号码。如果几百部手机共用一个IMEI号码，通过技术手段定位一个IMEI号码，可能会发现无数个手机的位置。

3）手机上网监管难度增大。（1）WAP网站管理难度增大。随着3G网络的不断应用，为用户提供WAP网上信息服务的网站将大量出现，WAP业务的内容将更加丰富，但由于在WAP网站管理上缺乏完善的审核、备案制度和成熟的管理经验，增加了WAP网站信息安全管理的难度，犯罪嫌疑人可较为方便的开办非法的WAP网站；（2）手机无线上网多样化。在3G时代，实现了手机用户的高速上网，加速了手机与互联网的融合，手机上网方式呈现多样化，犯罪嫌疑人既可以选择通过移动运营商提供的服务上网，也可以在提供WIFI、WIMAX等公共无线网络区域上网从事违法犯罪活动，由于犯罪行为的移动性和接入互联网的开放性，导致司法机关面临着立案、定位、取证困难等问题；（3）在3G时代，手机用户主要通过将手机作内部IP地址转换成互联网能够识别的外网IP地址，掌握手机用户的基本资料对于司法机关开展社会管理和侦查工作具有重要的作用。

4）手机电子信息提取困难。手机中的电子信息包括内存和存储卡的数据，但由于手机操作系统种类繁多、手机存储卡类型众多、数据线和充电接口不统一，手机电子信息提取面临极大地困难。

（1）手机操作系统种类繁多。目前，我国手机生产厂家众多，手机种类繁多，型号不断更新，不同的生产厂家使用不同的手机操作系统，目前，应用在手机上的操作系统主要有PalmOS、Symbian、Windows mobile、Linux、Android、iPhoneOS、Blackberry等，由于不同的操作系统文件管理、数据存储原理和方式各不相同，提取手机内存中的电子信息、恢复被删除、被加密、被隐藏的文件或数据的方法也不相同。

（2）手机存储卡类型众多。目前手机储存卡有SD卡、Mini SD卡、Mirco SD卡、SDHC卡、T-Flash卡、MMC卡、RS-MMC卡、Memory Stick（记忆棒）、M2卡等多种类型，通过读卡器可提取存储卡中的数据，但不同的存储卡数据存储原理和方式也各不相同，如何恢复被删除、被加密、被隐藏的数据的方法也不相同。

（3）数据连接线标准不统一。由于手机品牌、款式和型号的众多，一些机型较老的手机无法与电脑连接，有些手机虽然能够与电脑连接，但部分手机的I/O接口与电脑不匹配，造成手机上留存的信息提取不方便。但是由于我国未统一数据连接线标准，不同的手机需要不同的连接线。

（4）充电接口不统一。由于不同型号的手机待机时间不同，难以根据手机的剩余电量情况查明判断手机的待机时间，一旦电量耗尽导致手机关机，就会破坏手机的原始状态，因此，手机取证时应确保手机电量供应，但是手机型号众多和充电接口不统一，难以确保手机的电量供应。

2.3 检验鉴定机构不完善

司法机关没有对电子证据检验机构进行明确的规定，虽然公安部物证鉴定中心从1999年就开展电子物证的鉴定工作，某些省市也设置了电子物证检验机构，但很多省市还没有建立电子物证检验机构，还没有开展电子物证检验工作，难以更为有效地打击犯罪。

2.4 取证人员自身素质不高

手机取证需要侦查人员具备法学、侦查学、计算机科学和移动通信等知识，面对日益突出的犯罪，在当前的司法机关中，缺少一定数量掌握移动通信技术的侦查人员，难以保证打击犯罪的需要。

2.5 缺乏取证的意识

1）在司法实践中，侦查人员重破案、轻办案的思想根深蒂固，侦查人员缺乏手机取证的意识，对手机上留存信息利用多局限于通话清单，作为办理案件的线索，而疏于对手机上的其他电子信息的利用，不能充分发挥手机电子信息的证据作用。

2）很多单位使用盗版软件或破解软件进行取证，而这些软件没有经过合法认证，有些功能可能不完善，存在一些缺陷，可能造成取证结果不正确。

2.6 取证技术落后

1）我国手机取证技术尚处于起步阶段，缺乏具有自主知识产权的取证软件和设备，影响了取证的效率。

2）取证工具或软件主要是引进国外，但缺少专门的机构对取证工具或软件进行强制认证，难以保证法律的尊严和取证的质量。

3）通过从国外引进技术，提高了取证效率，打击了犯罪，

但是引进的取证软件的源代码是保密的，难以保证其有效性和可靠性。

2.7 缺少取证流程的指导

手机取证的流程对取证工作起到重要的指导作用。为保证电子证据的完整性和有效性，侦查人员必须遵循必要的取证流程，才能完成取证的工作，确保手机电子证据可采、可信、可用，更好地打击犯罪。与计算机取证相比，手机取证有其自身的特点，虽然公安部在2005年制定了《计算机犯罪现场勘验与电子证据检查规则》，但只是从总体上对电子证据取证流程进行了规范，至于手机取证的流程应如何开展，还没有明确的规定，此外，侦查人员取证时，缺少必要的规则，手机取证的流程亟需规范。

3 手机规范取证的对策

3.1 加强立法

根据国际电子证据的立法趋势，积极借鉴国际电子证据立法上的成熟经验，加快我国电子证据的立法，构建符合我国国情的电子证据规则，从而为打击犯罪提供强有力的法律保障。由于我国目前尚未明确电子证据法律地位，司法机关应根据司法实践的需要，通过司法解释或规范内部工作程序等方法，规范电子证据的识别、提取、分析、鉴定与使用，初步建立电子证据的取证制度，使电子证据的取证具有更强的操作性。

3.2 加强移动通信的管理

1）全面推行手机实名制。由于我国手机实名制刚刚开始实施，未实行实名登记的用户仍超过3.2亿，相关移动运营商应加快手机实名制推行，随着手机实名制全面推行，在今后的侦查中，通过手机可以迅速确定犯罪嫌疑人的身份，降低了办案的成本。

2）规范山寨手机。一方面要加强对手机通讯市场的监督与检查，避免非法的山寨手机流入市场；另一方面要加强对山寨手机生产厂家管理，引导他们以合法的身份生产手机，避免通过伪造IMEI号码生产手机。

3）加大手机上网监管力度。（1）完善WAP网站的审核、备案制度，不给违法犯罪分子开办非法WAP网站留有可乘之机；（2）加强互联网信息监控工作，强化对WAP网站和手机上网人员在BBS、QQ群组、MSN社区等重点部位的信息监控，及时掌握手机上网人员特别是其中重点人员的网上活动情况；（3）强化管理，健全数据库，有意识地收集各类人员利用手机上网的各种虚拟身份信息；（4）在WAP网站等网上复杂场所建立网上特情，及时获取预警性情报信息。

4）统一手机技术标准。司法机关应加强与不同手机生产厂商之间的交流协作，尽量统一手机数据存储的格式、存储卡、数据连接线、充电接口等相关标准。

3.3 加快检验机构建设

为有效地打击犯罪，有条件的省市应尽快建立手机电子证据检验机构，明确机构设置，加快实验室建设、购置设备、人员培训、方法研究，形成部、省（自治区、直辖市）、市三级电子证据检验鉴定体系，依据案件管辖范围和承担的检验鉴定工作职能，分别进行相关的电子证据检验鉴定工作，为司法实践提供强有力的支持。

3.4 加强人力资源建设

1）成立培训机制，对取证人员进行培训和资质认定，使其掌握识别、提取和分析手机电子证据的方法。

2）加强宣传，提高侦查人员的取证意识，使其掌握保护手机电子证据的方法。

3）成立专家库，聘请移动通信技术专家、计算机专家和法律专家组成手机取证专家组，协助司法机关开展取证工作。

3.5 提高取证的意识

1）手机取证的对象主要是手机识别卡、内/外存储卡、移动运营网络和短信服务提供商以及相关设备中的电子信息，应加强对侦查人员的培训和宣传，使侦查人员转变重破案、轻办案的思想，提高手机全面取证的意识。

2）只有通过国家强制认证的硬件设备和软件，才能用于电子证据的取证。

3）取证中必须坚持使用合法的正版软件，严禁使用盗版软件或从互联网上下载的软件。

4）涉及国家安全和国家秘密的案件中，慎用国外的取证软件，应可能使用合法的国产软件，避免危害国家安全和泄露国家秘密。

3.6 加快取证技术的研发

1）建立和完善电子证据取证学科体系，尽快建立适合我国国情的手机取证技术国家标准体系，推行取证技术行业准入制度，统一手机电子证据取证技术规范。

2）加强具有自主知识产权的手机取证工具、软件和方法的研究，符合法律法规的要求。

3）由于手机产品更新换代的周期非常短暂，手机生产厂家众多，应收集市场各种手机的参数和功能信息，建立手机信息数据库，针对每一款手机开展相应的取证研究工作，提高手机取证的效率。

3.7 加快取证流程的研究

借鉴计算机取证的成熟经验，按照取证的顺序，将手机取证分为若干阶段，从取证的准备阶段、证据的识别、证据的获取与采集、证据分析、证据的固定，以及应采取的技术手段和使用的软硬件工具等各个方面进行研究，进一步完善手机取证的流程，严格取证程序，保证证据识别、获取和分析的可靠性和有效性，为手机取证的规范化提供参考。

随着通信技术进步，3G手机等各种新型移动通讯产品不断出现和成熟，手机自身的功能也越来越强大，手机已经从单纯的通话工具发展成为可支持多频、多卡、具备上网功能、多媒体通信和大容量可扩展内存的通信工具，犯罪嫌疑人利用手机和手机网络实施犯罪的案件越来越多，造成了极大的社会危害性，手机取证的重要性日益突出，司法机关取证的工作面临新的挑战。相比已“相对成熟”的计算机物证检验，我国的手机取证工作尚处于初期阶段，还面临着立法滞后，移动通信现状复杂、检验机构不完善、缺少高素质的取证人员、缺乏取证的意识、技术落后、流程不规范等问题，影响了手机电子证据的应用。为此，一方面要吸收和借鉴国外成功的做法和经验；另一方面应认真研究手机取证面临的问题，积极开展电子证据立法，探索手机取证的手段和方法，制定科学合理手机取证的原则和规范，提高取证的水平。当然，随着科技的进步和法律法规的日趋完善，手机取证也将更加科学和规范，手机电子证据必将更加具有客观性、关联性和合法性，在未来的司法实践中一定会发挥更大的作用。●（责编 张岩）

参考文献：

[1] 薛琴．新时期手机网络犯罪研究 [J]. 信息网络安全，2011，(05)：47-49，67.

[2] 王桂强．手机物证检验及其在刑事侦查中的应用 [J]. 刑事技术，2006，(01)：25-31.

[3] 黄芹华，欧阳为民．手机及小型手持设备数字取证研究综述 [J]. 计算机工程与应用，2009，(18)：81-84.

[4] 蒋平，杨莉莉．电子证据 [M]. 北京：清华大学出版社、中国人民公安大学出版社，2007，18.

[5] 丁红军．电子证据取证的滞后及其规范 [J]. 黑龙江省政法管理干部学院学报，2010，(09)：108-111.

[6] 斯进．手机话单分析信息碰撞技战法的应用研究 [J]. 信息网络安全，2011，(07)：63-64，68.

上接第 38 页

Guest 均成功利用本文所述的新机制获得了 Root 的 ID 身份，结果证明此机制真实有效。

在当期最新版本的 AIX 系统下进行实证，需要 Root 用户执行 dbx 分析因堆溢出产生的 core 文件，确认入侵目标进程 ttdbserver 的堆栈地址及 leftmost 分段错误时目标进程申请的内存块长度，以调整实证脚本中的相关数据设置，因此实证本身仅为提醒用户加强防范，及时检查 IBM 网站发布的安全信息，防范潜在的系统风险。

实证所用 perl 脚本基于互联网上公开的 Solaris x86 漏洞实证脚本[6]，根据 AIX 进程堆结构对其进行了调整，调整后伪造 .rec 文件的部分脚本内容如下。

```
$pkt =
"\x4E\x65\x74\x49\x53\x41\x4D\x00\x55\x6E\x6B\x6E\x6F\x77\x6E\x00".
"\x31\x2E\x31\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
"\x04\x00\x00\x00\x00\x03\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00".
"\x00\x00\x00\x03\x00\x1C\x00\x1C\x00\x00\x00\x00\x00\x03\x00\x00".
"\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x01\x00\x00\x00\x04".
"\xFF\xFF\xFF\xFF\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x20\x00\x00\x41\x41\x41\x41".
"A" x 80 . "\xff\xff\x00\x00". "\x00\x00\x00\x00". "1234".
########################################################################
# AIX 5.3 oslevel 5300-02 passed. zrlw@sina.com 2012-03-14
########################################################################
# fake root block header of sub-left-branch:
"\x20\x07\x2f\x90". #  LeftChildAddr: point to fake leftchild
"\x2f\xf2\x0c\xdc". # LeftChildLength=ShellcodeLoc+0x20(MallocLen)
"\xff\xff\xff\xff". #  RightChildAddr(unimportance)
"\xff\xff\xff\xff". # RightChildLength(unimportance)
# fake leftchild:
"\x00\x00\x00\x00". # No LeftChild
"\x00\x00\x00\x00". # LeftChildLength=0
"\x2f\xf2\x0e\x84". # RightChildAddr=_lsmalloc saved LR location - 4
"\x2f\xf2\x0c\xdc". # RightChildLength=ShellcodeLoc+0x20(MallocLen)
"\x00" x 912 .
# Shellcode:
$shellrise .
"\x00" x 4000;
```

4 结束语

本文所述的堆溢出漏洞新利用机制原理表明，从 AIX 系统内核层面加强防范堆溢出漏洞被利用的安全工作并非是一件很难做到的事情。

无论采用何种方式，攻击者总是需要在栈上做文章，以谋求控制目标进程的处理流程，因此只要在重构进程空闲内存树的过程中，对处理节点的地址进行合法性判断，即可从根源上设置一道堆溢出漏洞利用机制难以逾越的安全之门。●（责编 张岩）

参考文献：

[1] David Litchfield.An Introduction to Heap overflows on AIX 5.3L[EB/OL]. http://www.ouah.org/aix-heap.pdf, 2005-08-25/2012-03-11.

[2] Tim Shelton.Advanced IBM AIX Heap Exploitation[EB/OL]. https://media.blackhat.com/bh-us-10/whitepapers/Shelton/BlackHat-USA-2010-Shelton-IBM-AIX-Heap-Overflow-Methods-wp.pdf,2010-07-17/2012-03-11.

[3] Uma Chandolu,Gargi Srinivas. AIX 中的内存分配机制 [EB/OL]. http://www.ibm.com/developerworks/cn/aix/library/au-memoryallocation/,2011-02-14/2012-03-11.

[4] IBM SECURITY ADVISORY.UPDATED- ToolTalk rpc.ttdbserver database parser vulnerability (Doc Number=5147)[EB/OL]. http://www-01.ibm.com/support/docview.wss?uid=isg1SSRVAIX53SECUR081505_109,2010-07-16/2012-03-11.

[5] Rodrigo Rubira Branco. IBM AIX, Oracle Sun Solaris, HP HP-UX Remote Vulnerability - CVE-2010-0083[EB/OL].http://seclists.org/fulldisclosure/2010/Jul/199,2010-07-13/2012-03-11.

[6] Rodrigo Rubira Branco. rpc.ttdbserverd x86 Proof Of Concept Exploit[EB/OL]. http://packetstormsecurity.org/files/92793/rpc.ttdbserverd-x86-Proof-Of-Concept-Exploit.html,2010-08-17/2012-03-11.