普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇
网络侦查与电子物证系列丛书主编：秦玉海

智能手机取证

秦玉海 孙奕 主编

Information Security

http://www.tup.com.cn

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

智能手机取证

秦玉海 孙奕 主编

Information Security

http://www.tup.com.cn

清华大学出版社
北京

内 容 简 介

全书从移动通信技术基础入手，从流程规范、基本原理和分析实践等方面系统地介绍了手机取证的相关知识，使读者能够在较短的时间内了解智能手机取证行业的情况、掌握基本的智能手机取证的理论和方法。本书结合实际案例阐述智能手机取证的工具应用，图文并茂，便于读者更好地将本书内容与实际办案工作紧密结合。

本书既可作为信息安全、电子数据取证等相关专业学生的教材，也可作为电子数据取证从业人员的培训和参考用书。

图书在版编目(CIP)数据

智能手机取证/秦玉海，孙奕主编. --北京：清华大学出版社，2014
高等院校信息安全专业系列教材
ISBN 978-7-302-35712-4

Ⅰ. ①智… Ⅱ. ①秦… ②孙… Ⅲ. ①移动电话机－证据－调查－高等学校－教材
Ⅳ. ①D915.13

中国版本图书馆 CIP 数据核字(2014)第 060820 号

责任编辑：张　民　薛　阳
封面设计：常雪影
责任校对：焦丽丽
责任印制：沈　露

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：11.5　　**字　　数**：266 千字
版　　次：2014 年 9 月第 1 版　　**印　　次**：2014 年 9 月第 1 次印刷
印　　数：1～2000
定　　价：24.50 元

产品编号：056210-01

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教

材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时5年，制定出我国第一个信息安全专业指导性专业规范，于2012年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》（由清华大学出版社正式出版）。“高等院校信息安全专业系列教材”在教育部高等学校信息安全专业教学指导委员会的指导下，根据《高等学校信息安全专业指导性专业规范》组织编写和修订，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断完善。

我们的E-mail地址：zhangm@tup.tsinghua.edu.cn；联系人：张民。

“高等院校信息安全专业系列教材”编审委员会

前言

随着社会信息化水平的不断提高，计算机、手机这些信息时代的产品已经越来越多地融入人们的生活之中，据有关机构统计，国内目前有接近 6 亿网民以及超过 12 亿的手机用户，可以说，计算机和手机已经成为人们必备的日用品，与此同时，人们对于互联网、移动通信等新技术的依赖程度也越来越大，从 10 年前的电话线拨号上网，到如今无处不在的高速移动通信网络；从浏览静态的网页，到各种新颖的多媒体互动资源；从简单的文字聊天，到现在的语音视频聊天、即时通信与社交网络……信息技术每天都在改变着我们的生活。

信息时代在为我们带来方便的同时，也展现出了双刃剑的另一面——越来越多的传统违法犯罪行为已经将主要阵地转移到了计算机和互联网上，同时，一些新的违法犯罪手段和形式也日益增多，这已成为摆在广大执法部门调查人员面前的一个难题，及时、有效地应对和打击新形势下的涉及计算机、互联网的违法犯罪已成为当务之急。

自电子数据取证调查在中国落地伊始，至今已约十年，经过近十年的发展，电子数据取证，尤其是计算机取证已经被政府执法部门、法律界从业人员和广大执法人员认可，积累了大量的经验并且取得了相当可喜的成就——在人才培养方面，国内许多公安政法类院校已开设了计算机侦查和计算机取证专业；在产品和技术方面，由最早的全部使用国外产品和技术，逐渐涌现出一批符合国内计算机取证调查实际的具备自主产权的取证产品。值得注意的是，在商业调查领域，也有越来越多的企业开始重视企业内部调查和内部 IT 审计；可以说，计算机取证在中国正像初升的朝阳，有着广阔而宏伟的发展前景。

而同样属于电子数据取证范畴内的手机取证，不仅在中国尚处于萌芽阶段，在西方发达国家的发展也不过 3～5 年；但是，伴随着信息技术，尤其是移动通信技术的迅猛发展，我们可以预见，在不久的将来，手机取证将成为电子数据取证中最为重要的部分之一，这就要求从事电子数据取证的调查人员尽早掌握和了解手机取证的相关知识，并及时掌握手机取证技术的发展，只有这样，才能更快地适应和面对日益重要的手机取证需求。

正是在这样的环境下，为了尽快填补国内计算机取证类书籍，尤其是手机取证类书籍的空白，为电子数据取证调查人员提供最新、最完善的取证技术，作者在近两年来对国内外手机取证和计算机取证研究的基础上，结合国

内电子数据取证的实际情况，编写了本书。

本书立足于手机取证技术的基础，涵盖了电子数据取证理论基础、移动通信基础、手机取证基础原理、实践技巧以及面向实战的取证方法，力图使读者能够对于手机取证，尤其是智能手机取证形成全面、完整的系统性认识，理解手机取证的基本思想和技术原理，并结合取证实践，熟悉取证实践中常见的手机取证方法以及手机取证工具的使用，从而基本具备手机取证的调查分析能力。

由于互联网及移动通信技术发展瞬息万变，加之本书篇幅有限，难免未能及时囊括各类新方法、新技术及新产品，请读者谅解。

编　者

2014 年 5 月

目录

第1章 手机取证概论

本章简要介绍目前取证行业内对于手机取证的定义，针对传统计算机取证和手机取证的关联性和差异性进行了大致分析，并通过细分类型，向读者介绍了当前在手机取证工作中通常关注的主要证据类型以及机器取证价值，最后，阐述了国际和国内取证领域中手机取证的发展现状。读者在学习完本章内容后，可以对手机取证的意义、手机取证的类型、手机取证所关注的证据信息以及当今手机取证的发展有基本的认识和了解。

1.1 手机取证的定义

手机取证目前尚没有一个准确和统一的定义，一般情况下，我们认为手机取证就是利用计算机和移动通信技术，使用专用的软硬件设备，对可能包含证据信息的移动通信设备、存储介质以及移动通信网络进行分析，并采用符合规范的程序和工具对上述信息进行收集、恢复和固定，并将所获取的信息进行分析和展现的过程。

这个定义中所指的“手机取证”，也可称之为“移动通信设备取证”，这个范围主要包含了通过移动通信技术接入无线网络，并通过网络实现各种移动通信功能和服务的设备，比如常见的手机、小灵通等。而“专用的软硬件设备”，是指进行手机取证调查过程中所使用的各类软硬件工具，必须是受到认可或进行严格测试的，以确保提取过程中不对潜在的证据信息以及证据本身造成损害。除了手机（或称移动通信设备）本身之外，手机取证的目标还包括与手机相关的存储介质，如手机存储卡、手机身份卡（如 SIM 卡、UIM 卡）以及手机通信过程中涉及的网络软硬件设备，如运营商的后台数据库、运营商的基站设备等。除此之外，“符合规范的程序和工具”是确保数据准确的重要因素，没有标准的操作流程和设备，将可能直接导致潜在证据信息的丢失。最后，是对存在的证据信息的固定和展现，主要包括证据信息的存储、报告的生成等环节。

为便于读者理解，本书将“移动通信设备取证”与“手机取证”统称为“手机取证”。

1.2 手机取证和计算机取证的相关性

从严格意义上讲，无论是针对计算机存储介质的取证、针对计算机互联网络的取证抑或是针对手机等移动通信设备的取证都属于电子数据取证的范畴之内，在西方国家，通常将此类取证工作称为 Digital Forensics，而并不仅限于 Computer Forensics 或是 Cell Phone Forensics。而在实际的调查工作中，手机取证和计算机取证工作往往具备很多共同的特点，许多方法、手段和取证工具是通用的，甚至最基本的取证规范、指导原则也是相

同或类似的(见本书第3章“手机取证的流程和规范”部分)。

举一个简单的例子,电子数据取证调查人员在进行现场调查时,面对的除了各类计算机之外,还包括相当数量的手机等移动存储设备,而通常情况下,针对手机的取证与针对计算机的取证是有很多相同或类似之处的,比如调查人员处理手机的存储卡时可以完全按照处理计算机硬盘等存储介质的方法,对其制作副本或者将其保存为证据镜像文件,并且同样可以使用取证分析软件对存储卡这类存储介质进行数据分析和文件恢复等操作。另一个例子是,针对智能手机,计算机取证调查员掌握的既有的取证知识能够继续得到沿用,比如基于 WinCE 的 Windows Mobile(或 Windows Phone)智能手机操作系统和 Windows 操作系统一样,都具有注册表结构和 Internet Explorer 浏览器——既有的取证软件可以继续在手机取证中使用;采用 Linux 内核的 Android 操作系统具有大部分 Linux 操作系统的文件结构;iOS 操作系统与苹果的 MAC OS X 很多方面都具有共性——调查人员可以方便地使用 dd 命令获取这两种手机的内部存储。

而与此同时,手机取证也有其特点,传统计算机的存储介质无外乎硬盘、U 盘等,介质接口标准化程度高,一台用于计算机取证的硬盘复制机如具备了 IDE/SATA/SCSI/USB 这些接口,便可基本支持大部分存储介质,手机则不然,在存储容量、存储结构以及硬件接口等诸多方面,不同的手机均不尽相同。如上段所提到的,现在市面上常见的手机中使用的数码存储卡可以按照传统的计算机取证方法进行取证,但实际上手机中大部分具有价值的数据一般都保存在手机的内部存储中(一些手机甚至根本不支持插入外置存储卡,如苹果公司的 iPhone),对付这些手机,证据获取是一个让人头疼的问题——手机内部存储通常采用 Flash 存储芯片,调查人员无法拆卸或直接取出,甚至无法直接访问;即使能够获取手机的内部存储,一个更大的问题摆在面前——如何进行文件系统解析和文件结构解析?这就需要手机取证调查人员学习和掌握一些计算机取证当中很少涉及的知识。

其实这样的例子不胜枚举,从很多方面都可以看出,计算机取证和手机取证是具有共性同时也有差异的。不可否认的是,一个熟练的计算机取证调查员可以通过学习很快成为一个专业的手机取证调查人员;就作者个人而言,更愿意做这样的描述:

“一个专业的手机取证调查员一定需要具备深厚的计算机取证知识积累和经验,首先应当是一个专业的计算机取证调查员。”

1.3 手机取证关注的内容

1.3.1 手机可视化取证

手机可视化取证是手机取证技术中发展最早,也较为成熟的一种取证方式,主要是采用专用台架或支架,将手机稳定放置并使用数码照相机、数码摄像机或高清数码摄像头等影像设备对手机外观和屏幕显示内容进行拍照/录像,从而达到对其内容进行固定的目的。

手机可视化取证的优点是显而易见的,那就是针对手机一般不存在不兼容的情况,手

机能够开机即可进行取证，且对于手机外形的取证较为直观和清晰，适宜展示在手机取证结果报告中；但缺点在于，由于需要调查人员在手机上进行相应操作（如切换短信、翻页等）后才能进行拍摄，所以，在进行手机大量数据提取时极其耗时、费力。

在现在的手机取证调查实践中，手机可视化取证设备仍被广泛使用，其主要作用是进行外观取证，并且在进行特殊手机取证（如其他手机取证设备不支持、手机数据接口损坏）的情况下进行辅助取证。

目前市场上常见的手机可视化取证设备主要有以下几种：

- Paraben Project-A-Phone，如图 1-1 和图 1-2 所示。

图 1-1　Paraben Project-A-Phone ICD-5200 可视化取证设备
（图片来源：Paraben 公司网站）

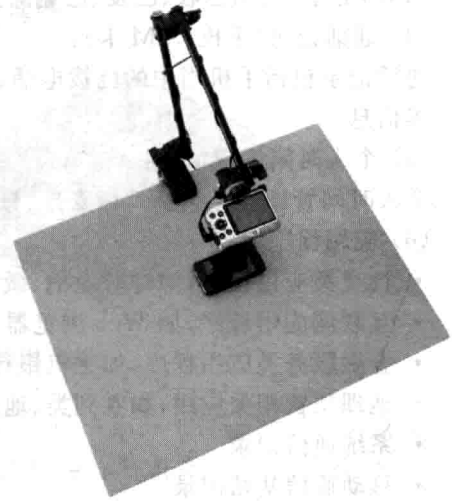

图 1-2　Paraben Project-A-Phone Flex 可视化取证设备
（图片来源：Paraben 公司网站）

- Fernico ZRT2，如图 1-3 所示。

上面所提到的诸如 Project-A-Phone 和 Fernico ZRT2 等设备，一般使用软件对数码相机、数码摄像机、高清摄像头等设备进行控制，实现自动对焦、自动图片调整，并提供报告生成功能，使用此类设备可以在一定程度上减轻手机取证调查人员的工作强度，弥补了因现有手机取证设备不支持或不兼容而无法对某些特定型号手机取证的缺陷。

图 1-3　Fernico ZRT2 可视化取证设备
（图片来源：Fernico 公司网站）

1.3.2　逻辑数据

在手机取证的调查工作中，绝大多数的调查内容是关于手机的逻辑数据的，这类数据的获取是广大手机取证调查人员最为关注的，也是手机

取证调查工作最基本的数据。

一般来说，手机的逻辑数据包括以下几个部分。

(1) 手机的基本信息：

手机的基本信息包括 IMEI、IMSI、ESN、MSN、MEID 和手机型号等。

(2) 通讯录(手机/SIM 卡)：

通讯录包括联系人姓名、号码、地址、照片、电子邮件和社交网络身份等。

(3) 信息(手机/SIM 卡)：

信息包括 SMS 短信，包括已收、已发、已删除、草稿等。

MMS 彩信，包括已收、已发、已删除、草稿和附件等。

(4) 通话记录(手机/SIM 卡)：

通话记录包括手机当中的已拨电话、已接来电、未接电话以及这些记录的时间和持续时长等信息。

(5) 个人时间管理信息：

个人时间管理信息包括日程安排、日历、备忘录等。

(6) 应用程序信息

- 社交类应用程序，如即时通信、微博、SNS 社交网络应用等。
- 互联网应用程序，如 Web 浏览器、RSS 阅读器等。
- 金融服务类应用程序，如手机银行、手机证券、手机期货和外汇等。
- 地理位置相关应用，如签到类、地理位置分享类应用等。
- 系统通信记录。
- 移动通信基站记录。
- 移动通信运营商记录。
- WLAN 连接记录。
- 蓝牙连接(或配对)记录。
- GPRS/3G 数据通信记录。

1.3.3 物理获取(内存转储)

和处理传统的计算机证据一样，物理获取(Physical Dump，或称之为内存转储)，就是使用特定的方法或软硬件工具，将手机内部存储空间(如 Flash 存储芯片)中的数据完整(在某些情况下是部分)地读取，以便进行后期调查分析，从某种意义上，可以被认为是如同对计算机硬盘进行了完整的镜像文件制作。

由于不同品牌、不同操作系统的手机软硬件架构上的不同，针对手机进行内存镜像转储的方式也不尽相同，转储的数据形式也有所差异。正常情况下，大部分手机不能通过直接获取的方式进行物理获取，原因有几点，首先，手机在运行过程中，Flash 芯片中的数据处于占用且可变状态，无法获取到相对固定和连续的数据；其次，通常情况下手机厂商提供的手机维护软硬件都不支持直接对内存较高权限的访问，这一般是出于安全方面的考虑，所以，在手机取证的调查过程中通常需要使用专用的工具进行物理获取操作。

一般意义上，手机的物理获取可以分为两大部分，首先是转储(dump)，即将手机内存中的数据完整地读取，从存储中进行位对位(Bit to Bit)的复制；随后，由于数据在手机内

部存储主要是在 Flash 芯片中(按照页、块等逻辑方式),在进行了复制之后,还需要进行重构、文件系统解析,使之成为文件形式存在以便后期使用。

对于资深的手机取证调查人员来说,物理获取是一种直接、有效的取证方式。常用是物理获取方式大致有以下几种:

(1) AT 命令获取。对于一些早期设备,如早期的摩托罗拉手机,at 命令可以有效提取手机内存当中的数据。

(2) 刷机盒[①]。刷机盒是一种特定的维修设备,如图 1-4 所示,主要被作为手机生产商和维修人员维修手机的工具,大部分刷机工具可以对手机进行参数更改、系统刷写[②]等操作,在手机取证中,刷机盒通常被用来进行内存转储。

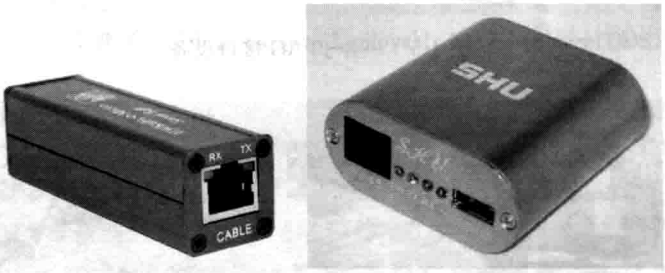

图 1-4　常见的手机刷机盒

(3) JTAG。JTAG 是联合测试工作组(Joint Test Action Group)的简称,通常代表标准测试访问端口和边界扫描结构标准,即 IEEE 1149.1 标准[③]。由于 JTAG 是一个被普遍接受的测试标准,大部分电子设备均可以采用 JTAG 方式进行测试或扫描,而绝大多数手机等设备均具备 JTAG 端口,而 JTAG 端口可以用于内存的读取,如图 1-5 所示。

(4) 恢复模式或工程模式。在某些品牌和型号的手机上,可以通过进入 Android 系统的 Recovery 模式或者使用专用的厂商工程模式工具进行内部存储镜像的提取(如三星公司的 ODIN 工具),如图 1-6 所示。

(5) 拆焊获取。拆焊获取是物理获取的最后一根稻草,一般是使用电烙铁或热风枪将 Flash 存储芯片从手机 PCB 电路板拆下,使用专门的芯片编程器进行数据读取并进行重构,这种方式的优缺点是显而易见的,优势是能够保证不改动或尽可能小地改动内存中的数据,但同时,这种方式具有不可逆的破坏性且风险较大,一般情况下不推荐非熟练的操作人员进行拆焊操作,这种方式通常也不作为物理获取的首选。如图 1-7 所示为 Flash 芯片编程器。

(6) 专用手机取证设备。随着近年来手机取证技术的不断发展,越来越多的手机取

---

① 刷机盒:一种特定的可以对手机进行编程、读写操作的软硬件设备,由于主要是对 Flash 存储芯片(或 EEPROM)进行编程操作,所以国外习惯称之为 Flasher Box,这类设备通常用于手机制造商或者维修者的维修检测;在手机取证调查中,接受过培训的手机取证调查人员可以使用刷机盒对手机内存进行转储提取。

② 系统刷写:俗称"刷 ROM"或者"写字库",主要是利用专用的软硬件维修工具对手机中的软件进行修复或更改。

③ IEEE 1149.1 标准,请见:http://standards.ieee.org/findstds/standard/1149.1-1990.html。

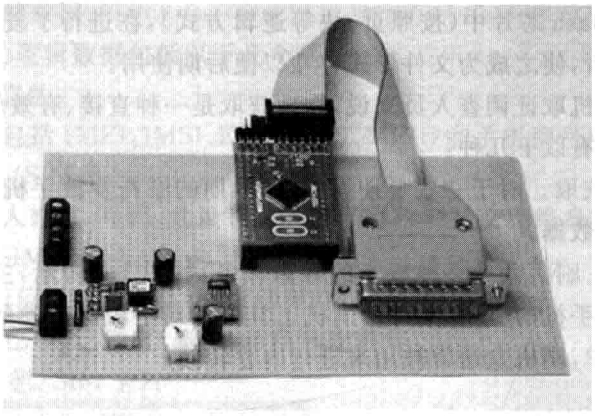

图 1-5　一种 JTAG 接口设备

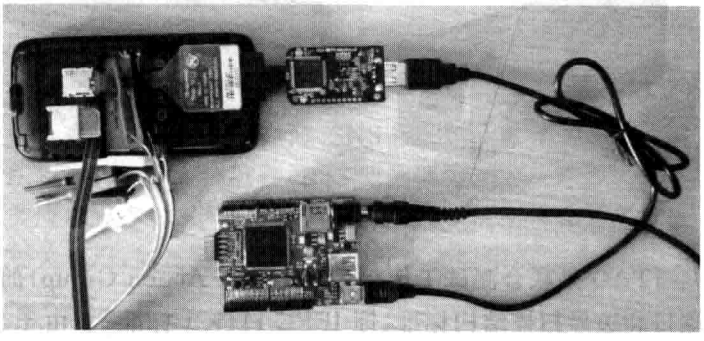

图 1-6　使用恢复模式进行获取的 HTC Android 智能手机

证工具支持直接对手机的内存进行转储，如 XACT、iXAM、Paraben Device Seizure 以及 Cellebrite UFED(见图 1-8)等，如图 1-9 所示为便携式取证设备。关于专用手机取证设备的使用，后面将进行简要介绍。

图 1-7　Flash 芯片编程器

图 1-8　可用于手机内存镜像转储的手机取证设备 Cellebrite UFED