# <<Android取证实战>>

## 图书基本信息

书名：<<Android取证实战>>

13位ISBN编号：9787111421993

10位ISBN编号：711142199X

出版时间：2013-5

出版时间：Andrew Hoog、 何泾沙 机械工业出版社 (2013-05出版)

作者：Andrew Hoog

译者：何泾沙

## 前言

【前言】从2008年10月第一部Android手机的诞生到2011年年初，Android移动平台迅速成长为全球最流行的移动操作系统。
对消费者来说，Android平台的爆炸性成长在竞争和功能方面都是一个巨大的胜利。
同时，由于缺乏用于调查相应设备和手持终端的知识以及工具，取证分析师和信息安全工程师遇到了巨大的难题。
本书试图解决这些问题，不仅详细介绍了Android的软件、硬件和文件系统，而且分享了计算机取证获取技术以及随后所需的设备分析工作。
对于缺乏计算机取证方面知识的读者，本书将提供基于免费、开放的代码库编写的实例，而且读者也可以亲身参与到这些实例的编写中。
因为免费的Android开发套件能够提供一个完整的Android仿真器，所以读者不需要实际拥有任何Android终端设备。
随着Android终端设备数量的快速增加，用户对于这些终端设备中存储着数据的意识也在相应增强。
然而遗憾的是，大多数对这些数据感兴趣的却是网络犯罪团伙，他们更清楚地知道这些终端设备中存储着大量的个人信息和商业信息，而对Android平台的成功攻击会为其带来巨大的“收益”。
如果要应对这种威胁，就需要深入地了解Android平台，不但对于Android系统开发者和制造商如此，对于Android应用开发者和企业中的信息安全管理者也是如此。
更加安全的应用将有助于防止敏感信息泄露，也会帮助信息安全管理者为系统制订更加有效的安全策略。
目前很多关于Android的统计数据都是针对智能手机以及平板电脑的，在不久的将来，Android将会在更多的终端设备中得到应用，如汽车、电视、全球定位系统（GPS）终端、游戏机、笔记本电脑以及其他电子产品。
对于取证分析师和安全工程师来说，针对Android的取证分析将会有一个很大比例的增长。
最后，Android的魅力不只绽放于某些特定的国家或地区，它将会对全球的个人、企业和机构产生巨大的影响。
下面将对本书中各章的内容进行简要介绍。
第1章该章在介绍Android平台的发展史后，还将讨论Android开放源码项目（Android Open Source Project，AOSP）、平台国际化、Android市场，同时提供有关 Linux 的一些简单辅导信息，并对Android取证进行简要说明。
本章还将逐步讲解如何创建一个基于 Ubuntu 的虚拟机，其后在全书的实例中都将会用到。
本书极力推荐 Ubuntu 虚拟机，它还可以应用到本书以外的其他Android取证实例中。
第2章该章介绍Android所支持的各种类型的硬件和终端设备。
虽然硬件的兼容性对制造商来说非常重要，最终也会使消费者受益，但是对大量硬件和终端设备的广泛支持却给取证分析师和安全工程师带来了巨大的挑战。
因此，对硬件组件、终端设备类型以及Android启动过程的清楚了解非常有助于对整个Android的了解，也对取证和安全分析具有很大帮助。
第3章该章讨论Android系统的不同版本、Android软件开发套件（Software Development Kit，SDK）、Davlik虚拟机、Android安全的核心组件以及其他与Android取证相关的重要概念，如Android程序调试桥（adb）、USB调试设置等。
本章还将提供一些详细的实例，包括如何在 Linux、OS X 和 Windows 上安装软件开发套件，以及如何创建一个Android虚拟终端用以测试取证技术。
第4章该章介绍如何在Android终端设备上存储数据，内容包括数据存储方式（共享参考、文件、SQLite及网络）以及Android终端设备所使用的内存类型，如 RAM 以及十分重要的NAND闪存。
该章也会详细介绍读者在Android终端设备中经常会遇到的各类文件系统，如 YAFFS2、EXT、FAT32/FAT16及各类底层文件系统。
第5章该章讨论Android终端设备、数据和应用的安全。

首先回顾了Android终端设备如何泄露数据及其如何被用做一个主动攻击源。
在讨论一些重要的安全概念后，该章将给个人、企业安全管理者和应用开发者这三类主要读者提供一些非常具体的建议。
随着Android持续快速增长，数据和信息的安全问题将变得日益严峻。
因此，该章对这个重要的问题进行了深入且切合实际的快速讨论。
第6章该章介绍具体且十分有用的从Android终端设备获得取证信息的一些技术。
在介绍了不同类型的获取方法以及如何对Android终端设备进行操控后，本章还讨论了规避密码的7个不同策略。
随后，本章介绍一些具体的获取 SD 卡以及任何插入的内置多媒体卡（Embedded Multi Media Card）的技术以及相对应的代码。
在此基础上，该章介绍一些逻辑获取技术，包括一些已经包含在Android和软件开发套件（SDK）里的技术以及一个称为 AFLogical 的可以供执法者和政府机构免费使用的技术，并简单描述了6个商用取证软件。
最后，本章详细介绍了获取 NAND 闪存物理映像的技术，包括6个如何获得超级用户权限的方法以及由 viaForensics 公司开发的 AFPhysical 技术。
第7章该章是最后一章，将介绍一些具体的策略以及相应的应用程序，使取证分析师和安全工程师可以对得到的Android终端设备进行分析。
虽然很多传统的取证技术仍然适用于Android取证分析，但是Android中新的文件系统以及硬件的特殊性要求更多的新技术。
没有这些新技术，从Android终端设备中实际获取的数据只能够得到极少有价值的内容和信息。
除了提供背景信息以及实用的应用软件，该章还将给出Android文件的目录（文件夹）结构，并深入分析11个可以用于获取Android终端设备中主要数据的应用程序。
具备了以上知识，取证分析师和安全工程师可以对任何可以获得的Android终端设备进行取证分析。
致谢我现在真正理解“ 举全村之力 ”（It takes a village）的深刻含义了，它不但适用于描述抚养孩子，也同样适用于撰写书籍。
因此，我要衷心感谢“ 整个村庄 ”：感谢我的家庭成员：妻子和女儿们。
感谢 Lee Haas 为本书所做的出色的文本编辑工作，并时刻督促我按照原定计划完成此书的撰写。
感谢 Ted Eull为读者提供的出色服务，时常帮助我将头脑里激荡的想法用清晰的言语和文字表达出来。
同时Ted也是我的好朋友。
衷心感谢他的妻子，为他在创业过程中长时间工作所给予的耐心和支持。
感谢 Chris Triplett 率先开始对Android的研究及其所进行的出色工作。
Chris 在将通俗的英语应用到数字取证，以弥补语言描述上的欠缺，以及提供喜剧性疏解方面十分有天分。
感谢 Katie Strzempka 负责另外一本书的撰写（“ iPhone and iOS Forensics ”）。
在此郑重地向读者推荐这本书。
感谢我的父母 Stevie 和 Al。
他们从人生的开始就为我制定了一条正确的发展道路，并且能够在我稍有偏差时及时提醒。
感谢 Harmonee 和 Hadabogee 照顾我的女儿们、准备晚餐以及提供的其他很多方面的帮助。
感谢众多在地方、州、联邦政府的法律部门及其他部门中为公共事业提供服务的勇敢的人们，感谢他们为我们的社会和国家所做的一切。
感谢 Google（谷歌）认识到 Android 的价值，并且为移动终端设备创造了一个新的开放平台。
感谢苹果公司提供了另外一个开发平台。
最后，感谢所有的读者。
我衷心希望本书可以为读者带来价值，并赞赏他们给予的任何支持。

# <<Android取证实战>>

## 内容概要

《Android取证实战:调查、分析与移动安全》是Android取证领域广受好评的经典著作，也是国内第一本关于Android取证的著作，由资深取证技术专家撰写，世界顶级取证专家审校，权威性毋庸置疑！《Android取证实战:调查、分析与移动安全》根据当前Android取证工作者的需求，首先从Android的硬件设备、应用开发环境、系统原理等多角度剖析了Android系统的安全原理，为读者打下坚实的理论基础，然后结合实用的取证分析工具和经典案例，系统而生动地讲解了Android取证的原理、技术、策略、方法和步骤，被公认为从事移动取证相关工作的从业人员必备的书籍之一。

《Android取证实战:调查、分析与移动安全》一共7章：第1章介绍了Android平台的概况和特点、Linux与Android，Android与取证，并讲解如何创建基于 Ubuntu 的虚拟机；第2章讲解了Android所支持的各种类型的硬件和终端设备，为取证和安全分析做好准备。
第3章讲解了软件开发套件、Android虚拟终端的安装，以及取证技术的一些重要概念，涵盖Davlik虚拟机、Android程序调试桥、USB调试设置等；第4章分析了Android系统的数据存储方式、涉及的内存类型，以及Android中常见的各类文件系统；第5章分析了Android终端设备成为泄漏数据以及用于作为主动攻击源的原因，并为个人、企业安全总监和应用开发者提供了一些非常具体的建议；第6章深入讲解了规避密码的几个不同策略和多种逻辑获取技术和物理获取技术（如adb pull、备份分析、AFLogical、JTAG、芯片摘取、AFPhysical等）；第7章介绍了一些具体的策略和Android文件的目录（文件夹）结构，并深入分析了11个可以用于获取Android终端设备中主要数据的应用程序。

## 作者简介

作者：（美国）Andrew Hoog 译者：何泾沙ndrew Hoog，计算机科学家，资深认证取证分析师（GCFA和CCE），计算机与移动取证研究者，viaForensics 公司（研发数字取证与信息安全技术）的创始人之一。
致力于取证分析、数字取证与信息安全等技术的研究，以及取证软件的开发，目前有两项与取证和数据恢复相关的在审专利。

# <<Android取证实战>>

## 书籍目录

## 编辑推荐

《Android取证实战:调查、分析与移动安全》编辑推荐：Andriod取证领域广受好评的经典著作，资深取证专家撰写，世界顶级取证专家审校。

## 名人推荐

如果你想学习和进行Android取证，那么本书是为你而写的，从没有一本书如此为你呈现Android操作系统与安全相关的技术细节，本书是移动取证从业人员的必备书籍。
——Jim Steele 某一级无线通信运营商（Tier 1）数字取证总监

## 版权说明