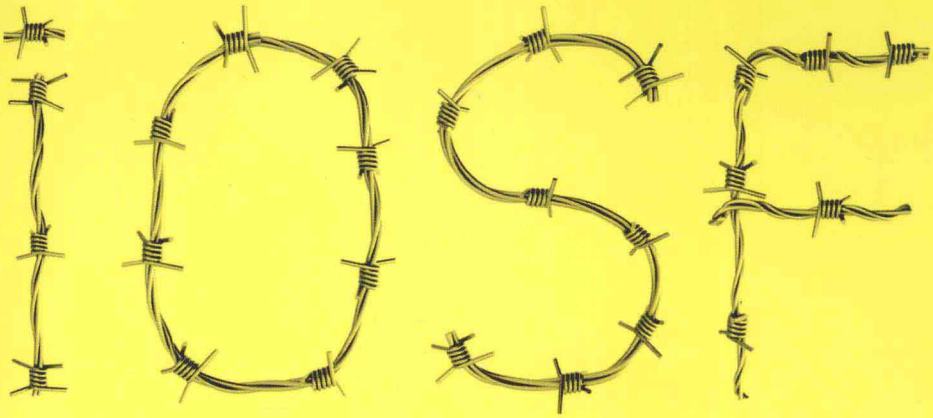
HZ BOOKS
华章科技

iPhone和iOS取证领域广受好评的经典著作，资深取证技术专家撰写，理论指导与实用性兼备！

从iPhone和其他iOS设备的硬件设备、应用开发环境、系统原理多角度剖析iOS系统的安全原理，结合实用开源工具和案例系统讲解取证的技术、策略、方法和步骤。

安全技术大系
SECURITY

ELSEVIER
爱思唯尔



iPhone and iOS Forensics

Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices

iOS取证实战

调查、分析与移动安全

（美）Andrew Hoog　Katie Strzempka　著

彭莉娟　刘琛梅　赵剑　译

机械工业出版社
China Machine Press

iPhone and iOS Forensics

Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices

iOS取证实战

调查、分析与移动安全

（美）Andrew Hoog　Katie Strzempka　著

彭莉娟　刘琛梅　赵剑　译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

iOS 取证实战：调查、分析与移动安全 /（美）胡格（Hoog, A.），（美）史特山普卡（Strzempka, K.）著；彭莉娟，刘琛梅，赵剑译 . —北京：机械工业出版社，2013.7
书名原文：iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices

ISBN 978-7-111-42862-6

Ⅰ. i… Ⅱ. ① 胡… ② 史… ③ 彭… ④ 刘… ⑤ 赵… Ⅲ. 移动电话机 – 应用程序 – 程序设计
Ⅳ. TN929.53

中国版本图书馆 CIP 数据核字（2013）第 127721 号

iPhone 和 iOS 取证领域广受好评的经典著作，资深取证技术专家撰写，理论指导与实用性兼备！从 iPhone 和其他 iOS 设备的硬件设备、应用开发环境、系统原理多角度剖析 iOS 系统的安全原理，结合实用的工具和案例系统讲解取证的技术、策略、方法和步骤。

第 1 章是对 iPhone 的概述，介绍 iPhone 型号、硬件组件、iPhone 设备的取证采集，以及一些功能强大的 Linux 命令行。第 2 章介绍运行 iOS 的主流设备及其独有特性，涵盖操作系统的操作、设备安全和启动至不同操作模式的方法，以及 iTunes 和 iOS 设备之间的交互。第 3 章讨论存储在 iPhone 上的可恢复数据类型、存储的格式和常规位置，概述 iPhone 设备的存储器类型、操作系统、文件系统以及磁盘分区。第 4 章通过 Apple 设备测试的过程来确定能从这些设备中恢复哪些敏感数据类型，并涵盖安全移动应用程序的沿革，以及对设备和应用程序安全的一些常规建议。第 5 章涵盖可在 iOS 设备上执行的各种逻辑获取和物理获取方法，并概述其他可映像的 iOS 设备。第 6 章介绍 iPhone 上的数据分析技术，涵盖基础技术（如挂载磁盘映像）以及用十六进制编辑器分析映像的高级技术，并全部提供实用的脚本供审查者实践，随后论及分析技术、文件系统的设计和各数据类型的存储位置。第 7 章介绍各种移动取证工具的使用方法及其差异对比，包括 iPhone 测试数据构造、测试方法论，尤为重要的是，该章介绍 12 个取证工具的安装、取证和分析，并给出测试步骤和调查报告。

机械工业出版社（北京市西城区百万庄大街 22 号　　邮政编码　100037）
责任编辑：高婧雅
藁城市京瑞印刷有限公司印刷
2013 年 7 月第 1 版第 1 次印刷
186mm × 240mm • 16.25 印张
标准书号：ISBN 978-7-111-42862-6
定　　价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

译 者 序

近几年，信息技术处于高速发展时期，智能手机和平板电脑普及率逐渐增高，尤其是2011年以来，iPhone和iPad在中国的销售额更是其领域中的佼佼者。我们看到，使用智能终端的人越来越多，各个企业、学校、机关都在开始如火如荼地进行无线网络的建设，移动设备正渗透到我们生活和工作的方方面面。很多学校开始购买iPad进行辅助授课，许多企业甚至考虑允许员工通过自带智能设备使用企业的内部应用（携带iPad平板电脑辅助办公），以提高沟通和工作效率，同时降低企业在移动终端上的成本和投入。

然而我们需要关注的是，这种方案在带来效率的同时也带来了安全的隐患，比如员工获取了企业的信息后却丢失了移动设备，如果不对移动设备上的数据进行处理，则会导致企业或个人信息泄露；或者员工自带设备从企业获取机密信息后，将信息用于侵权交易，企业如果没有获取证据的方法，没有追溯的手段，就只能白白蒙受损失。另一方面，社会上越来越多的不法分子在利用手机进行犯罪，比如在犯罪行为的实施过程中使用手机来充当联络工具，用手机存储犯罪证据，或者用手机进行短信诈骗、短信骚扰，或者将其作为病毒软件传播的实施工具。移动设备取证将是应对这些安全、违法事件的一个手段。

本书是iOS设备取证领域比较经典的著作，专注于研究苹果公司的iOS设备的取证技术和工具，深入浅出地向我们介绍了iOS设备的发展历史，设备上存储的数据类型和文件系统结构，以及各种可用的取证技术和取证工具。非常系统而全面地向我们展示了iOS设备取证分析的原理和实践。如果你是名企业网络安全管理员，你可以在本书中了解到如何对企业中的设备实施安全保护；如果你是一名合法的取证审查工作者，你可以系统掌握如何利用各种工具在iOS设备上获取证据，用于法律诉讼。虽然各种技术的发展非常快，本书的一些实践并不是采用近年最新版本的iOS设备或最新版本的工具，但是不妨碍我们去理解这些取证的原理、技术和方法。在第7章，作者还对各种移动取证工具做了详细的试用和介绍，这对取证审查工作而言是非常有用的，学习本章后就可以从作者推荐的取证工具中选出适合自己的，而不需要再花时间自己下载安装逐一比较。

译者也是从事信息安全工作的，通过阅读本书给我们的工作带来了很多帮助。我们很荣幸能够将本书的中文版带给大家！希望本书也能为你的工作带来新的思路。如果你才接触移动设备取证，可以通读这本书来了解iOS设备取证技术；如果你是一名企业安全管理员，企业中要管理许多iPhone和iPad设备，你可以重点关注第4章，这里会对设备和应用程序安全给出一些常规建议，帮助你做好安全防御工作；如果你已经有了移动设备取证的相关经验，建议重点关注第6、7章，这里的高级分析技术或许能够为你的工作带来新的突破。

参与本书翻译和校对工作的有彭莉娟、刘琛梅、赵剑，同时杨人权等也对本书的部分文字进行了优化。此外，也非常感谢机械工业出版社华章公司为本书的出版所做的努力。

由于时间以及译者水平所限，尽管我们尽了最大努力，但书中难免有不尽人意之处，敬请读者不吝指正！你可以发邮件到：echopenglijuan@126.com，我们将尽快答复提出的疑问。在此对你的谅解和支持表示真诚的感谢。

彭莉娟

前　言

本书适用于对 iPhone 和其他 iOS 设备感兴趣的读者，尤其适合那些对设备中能恢复的存储数据类型感兴趣的读者阅读。移动取证的需求随着智能手机的发布在惊人地增长。随着手机的应用不再局限于通话功能，使得通过手机进行的交流互动逐渐被数据化了。当用户用 iOS 设备发送短信、查收个人或工作邮件、上网、管理财务，甚至照相和摄影时，他们并没有意识到，这些数据正在被存储到他们的设备上。当删除一条信息时，他们会认为这些数据永远消失了。但事实上并非如此，本书不仅解释为什么这些被删除的数据能够恢复，还向取证审查者提供了用于从 iOS 设备中提取信息的一些具体方法。

本书的结构使得读者可以单独专注于每一章。如果你是一名企业安全主管，仅对存储在 iPhone 或 iPad 上的数据是否安全感兴趣，你可以直接阅读第 4 章。如果你是有经验的移动取证审查者，了解存储在 iPhone 文件系统中的所有文件，但是还想学习更多的高级分析技术，那么可以跳过前面几章，直接阅读第 6 章。

下面对各章内容进行简要介绍。

第 1 章是对 iPhone 的概述，包括 iPhone 发展过程中的关键事件时间表。详细介绍不同的经典 iPhone 型号，包括设备中的多种硬件组件。通过阐述数据采集的各种方法来介绍 iPhone 设备的取证获取。这一章的结尾部分对 Linux 系统进行了介绍，展示了在移动设备审查中，这些命令行工具是多么强大。

第 2 章介绍了多种主流 iOS 设备以及这些设备独有的特性。这一章涵盖了软件升级、设备安全和各种操作模式的介绍、系统升级 / 降级的执行，以及将设备启动至不同操作模式的方法。还将讨论 iTunes 和 iOS 设备之间的交互，包括 iTunes 中支持 iOS 设备的功能。

第 3 章讨论了存储在 iPhone 上的数据类型，以及这些数据存储的格式和常规位置。这一章还详细描述了可从 iOS 设备中恢复的普通文件类型，帮助检查者了解数据是如何存储的，以便他们能够更有效地从这些文件中恢复数据。除了 iPhone 的操作系统、文件系统以及磁盘分区外，该章也概述了 iPhone 的存储器类型。

第 4 章在用户数据保护方面为企业的移动设备管理员提供了一些选择。读者可以通过 Apple 设备测试的过程，来确定可从这些设备中恢复的敏感数据类型。该章还涵盖了安全移动应用程序的沿革，这些发展激发了从用户及开发者角度进行的测试。最后，这一章就设备和应用程序安全给出了一些常规的建议，帮助用户和管理员对公司中的设备进行安全保护。

第 5 章涵盖了在 iPhone、iPad 和其他 iOS 设备上进行取证的各种获取方法，讨论了映像取证的重要性，随后对设备映像的不同方法进行了说明，并详细讲解了从 iPhone 的备份文件中恢复数据的两种方法。接下来介绍逻辑获取，最后是设备的物理获取。同时，

也概述了其他可能进行映像的 iOS 设备，这些设备包括 iPod Touch 和 Apple TV。

第 6 章全面介绍如何对 iPhone 上的数据进行分析。这一章先介绍了几种不同的分析技术，论及一些基础的方法，例如挂载磁盘映像，以及用十六进制编辑器分析映像等高级技术。每个技术都提供了实用的脚本，审查者可自行将命令复制后执行，这样有助于了解所有的步骤。随后论述了分析技术、文件系统的布局。在 3.7 节中，读者能够了解到每个数据类型的存储位置。在这一章的结尾，是一些移动应用程序的参考资料。在这里，审查者能够浏览详细的应用程序列表，并且能够从中得知每个应用程序的数据存储在哪里。

第 7 章介绍了各种移动取证工具的使用方法，以及它们之间的差异对比。概述涉及 iPhone 测试设备的数据构造过程，详细介绍了有关测试的方法论，然后对每个用于分析的软件产品进行概述。这一章的大部分内容都专注于介绍使用所列工具去测试设备的审查方法。通读学习，读者可以一步步地学习工具的安装、获取和分析，在每个工具的最后都有一个列表，列表中记录了相应工具的研究报告。

要获取代码、程序和升级包等本书配套材料，请访问：http://viaforensics.com/resources/iphone-ios-forensics-mobile-security-book。

致谢

当决定合写这本书时，我已经充分意识到它会对我的生活产生一定的影响，但却忽视了那些直接或间接被卷入其中的人。幸运的是，我能在此对他们聊表谢意。

首先要感谢的是我的家人和朋友，他们谅解我缺席了许多夜晚和周末的聚会。特别要感谢我的父亲，尽管他说“Linux 这东西我完全搞不懂”，但还是帮我审校了第 2 章。同时，要感谢我的母亲，她总是鼓励我说其实我比自认为的要聪明得多。感谢我的弟弟 Danny 在我忙碌时照顾我的狗。感谢 Jill，她一直鼓励我、陪伴我，特别是当她为我带来了曲奇饼和纸杯蛋糕时。此外，要感谢我的朋友们，他们偶尔说服我忙里偷闲地吃点寿司，玩玩飞镖。

感谢 Marcus Rogers 博士和普度大学的数字取证项目，谢谢他在我准备涉足这个领域时给予我帮助以及一直以来为我提供专业决策方面的建议。

我要特别感谢 viaForensics 公司的同伴们，感谢大家容忍着 Andrew 和我的长篇大论。非常感谢 Ted 能够编录我的 iPhone 模拟器照片；感谢 Catherine 容忍我的坏脾气；感谢 Chris，即便我嘲笑他说“不可能恢复这些视频文件”，他也从不放弃逼迫我找出分析 iPhone 的新方法。

没有我的合著者 Andrew Hoog 的帮助，这本书就不可能完成，他让我知道所有的指令都可以并且应该通过命令行来完成（尽管通过 GUI 能够快上 10 倍）。

目　录

第 1 章

概　述

1.1 介绍

移动设备在过去的几年里有了很大的发展。曾经，手机只是简单地被用于打电话。随着技术的不断成熟，手机也具备了收发短信、创建日常事务提醒和保存联系人的功能。发展至今，移动设备因功能丰富而广泛应用于人们的生活中。2010 年年初，全球约有 46 亿人拥有手机（CBS，2010）。按照这种增长速度，手机的普及将给移动设备取证带来大量的需求。

自 iPhone 在 2007 年 6 月第一次发布以来，它受欢迎的程度与日俱增，这在一定程度上得益于它先进的功能设计和实用性。用户可以通过 iPhone 实现收取邮件、拍照、浏览网页等众多功能。这些功能使得 iPhone 代替了 PC 和数码相机。除上述功能之外，iPhone 还有许多有关金融、管理或娱乐的应用供用户下载安装。

在 20 世纪 80 年代后期，Apple 公司专注于研发 Newton 平台，即个人数字助理（PDA），这个项目在 1998 年以失败告终。1997 年，史蒂夫•乔布斯担任了该公司的 CEO。在 iPhone 的构想诞生前，乔布斯决定将 Apple 公司的业务重心由 PDA 和平板电脑转移到触摸屏技术的开发上来。基于对移动电话将日趋普及的判断，Apple 公司开始研发支持图片展示、视频播放并能从 iTunes 中同步数据的移动设备。2006 年 10 月，Apple 公司的 iPhone 被授予专利；2007 年 1 月，乔布斯在 MacWorld 大会上宣布推出 iPhone（Wired，2008）。

1.1.1 策略

在过去的几年中，Apple 公司的市场策略从传统电脑领域转移出来。其提出的一些创新思想颠覆了现有的商业模式。他们开发出了几种用于支持音乐和视频播放的应用和设备，包括 Apple TV、iTunes 和各种 iPod 设备。在移动通信设备领域，他们开发了 iPhone，而在应用交付领域中开发了支持同步及下载的 iTunes 以及 App Store。最终，在以上技术的基础上，Apple 公司在平板电脑领域推出了 iPad 产品（之前推出过 Newton 设备）。

这些新产品大多数都运行 iOS 系统，但 Macintosh 工作站例外，它运行在 OS X 系统。对于是否应该将 Mac OS X 迁移到 iOS 系统或类 iOS 系统这个问题，曾经存在过一些争议。Mac OS X Lion（Mac OS 10.7 版）于 2011 年夏天对外发布，该操作系统拥有除了触摸屏之外的类似 iOS 设备的功能。2011 年 1 月，Mac App Store 发布，使用 Mac 的用户

也可以通过自己的电脑直接购买软件，方式与通过 iTunes App Store（2010 年，Apple 公司发布）购买类似。

到 2009 年，iPhone 以 4.4% 的市场份额一跃成为全球第三大智能手机生产商（McGlaun，2010）。仅在 2010 年第一季度，它的销售量就达到了 875 万台，这个数值比 2009 年同期增长了 50% 以上。iPhone 4 发布之前，Apple 公司就卖出了超过 5000 万台 iPhone，2010 年第四季度的统计显示，Apple 公司掌控了 25% 的美国智能手机市场份额（Slashdot，2011）。随着 iPhone 的极度流行以及其销量的不断攀升，iPhone 设备已经成为了许多取证研究分析的焦点。

1.1.2 开发者社区

除了在销售方面的成绩，iPhone 还有一个活跃的黑客社区，这个社区已经推出了一些支持取证的研究结果和工具。其中一些工具和技术在最初的时候被用来协助映像取证，而如今它们也用来对设备进行一些测试，使得大家能够更好地理解设备的内部机制。Cydia 就是用于这些目的的一款流行应用程序。它允许用户在已经“越狱”的 iPhone 或 iPad 上运行非 App Store 下载的程序。值得一提的是，通过这种渠道获取的应用程序可以让审查者更好地理解 iPhone 文件系统和数据内容，例如 Mobile Terminal。当然，不建议去“越狱”或者修改 Apple 设备，因为这毕竟不是合法的手段。然而，不可否认，对于审查者来说能够远程连接测试设备用于研究将是一次非常珍贵的学习经历。

另外一个在 iPhone 上普遍应用的技术是“解锁”。从 2007 年到 2011 年年初，AT&T 是在美国唯一为 iPhone 提供服务的运营商。AT&T 将 SIM 卡与 iPhone 绑定，用户的 iPhone 只能使用 AT&T 网络，如果使用其他运营商的 SIM 卡，iPhone 就会被锁住。2011 年 2 月，另一个运营商 Verizon 也开始为 iPhone 4 提供网络服务。iPhone 的使用被强制在这两个运营商之间，这使得许多 iPhone 用户更希望有其他的选择。解锁 iPhone 就是其中的一个方法，它让设备可以接入其他的运营商网络，有很多的 Apple 教学网站（例如 iClarified）提供了详细的解锁步骤。典型的步骤包括安装一个应用程序并运行，然后将 AT&T 的 SIM 卡更换成其他运营商的。这里要说明的是，Verizon 采用的是 CDMA 网络（码分多址）而不是 GSM（全球移动通信系统），为 Verizon 定制的 iPhone 版本不能够通过简单更换 SIM 卡的方式解锁。正是因为这样，用现有的方法是无法解锁 Verizon 定制的 iPhone 设备的。话虽如此，毋庸置疑的是，Apple 用户社区肯定会在不久的将来找到新的解锁方法。

Apple 开发者网站是另一个让开发者、审查者或对 iOS /OS X 系统感兴趣的人受益的资源。只要注册为 Apple 开发者，就可以下载 Xcode 和 iOS 软件开发包（SDK）来协助应用程序开发。在这个开发套件中包含了 Xcode 集成开发环境（IDE）、iOS 模拟器，以及一些 iPhone/iPad/iPod touch 应用程序开发需要的额外工具。

要使用这些工具，必须先下载并安装 Xcode 和 iOS SDK。安装好后，就能够在路径 /Developer/Platforms/iPhoneSimulator.platform 中看到工具和文件，如图 1-1 所示。

图 1-1　iPhone 模拟器和 Xcode 文件

在这个开发包中最有用的工具之一是 iOS 模拟器，如图 1-2 所示。开发人员可以通过这个程序模拟任何 Apple 设备和版本，然后在此特定型号上进行程序调试。在图 1-2 的例子中，这台 iPhone 运行在固件版本 4.2 上，还可在固件 3.2 版本（应用于 iPad）和固件 4.0.2/4.1 版本（应用于 iPhone）上模拟运行。这个软件比较消耗内存资源，所以在测试的过程中会表现得稍微慢一些。从模拟器启动的话只有一些常规的应用程序，包括图片库、设置、游戏中心、联系人和 Safari 浏览器。用户能够打开这些应用，就好像在真实的设备中一样，甚至还可以执行一些其他的功能，包括：在通话时的屏幕上端显示“通话中”状态图标、模拟内存告警、模拟物理键盘、锁定设备。但是，模拟器也有一定的局限性，它缺乏一些常用程序，例如 SMS（短信）、日历、照相机、备忘录，以及可以下载其他应用程序的 App Store。

图 1-2　iPhone 模拟器——截图

模拟器的主要作用是供程序开发者用来联调 Xcode。用 Xcode 开发的 iPhone 或 iPad 应用程序，能够在模拟器虚拟的不同固件版本中进行调试和运行，以确保这个应用程序能够按照预期的方式正常工作。

1.2 iPhone 型号

2007 年 6 月，第二代 iPhone——iPhone 2G 在美国发布。同时，也发布了 iTunes 7.3 版，该版本可支持设备的数据同步。在后续几年中，以下型号相继发布：2008 年 7 月发布 iPhone 3G，2009 年 6 月发布 iPhone 3G（s），2010 年 6 月发布 iPhone 4。

每一款设备都对应自己特有的固件版本，固件版本信息能够通过以下操作查看，设置→通用→关于本机→版本。Apple 公司会不定期发布一些新的固件升级版本，以新增某项功能、修复缺陷或安全漏洞，或辅助设备通用功能。

表 1-1 中展示了每款设备的型号编号和初始 iOS 版本。

Apple 公司也提供了一些其他的方法，可以在电话关机的时候识别设备的型号编号。首先，可查看刻在手机外壳背面的型号编号。或者，你也可以通过手机的外壳来判断，第一代 iPhone 是金属外壳，而 3G 和 3G（s）是塑料外壳。3G 与 3G（s）有所不同，3G 的银色外壳上仅仅刻了 Apple 的标志，而 3G（s）在银色外壳的背面刻了型号编号。iPhone 4 是独特的长方形设计，在转角处没有那么圆，与早期版本非常不同，很容易能识别。Apple 的知识库文章提供了详细的信息，有助于大家去了解如何识别 iPhone 型号。参见相关链接：http://support.apple.com/kb/HT3939。

表 1-1 iPhone 型号

设备	型号	可用的 iOS 版本
2G	A1203	iOS 1.0
3G	A1241	iOS 2.0
3G（s）	A1303	iOS 3.0
4G	A1332	iOS 4.0

表 1-2 中展示了各个型号（不同存储容量）的规格和功能（Costello，n.d.）。

iPhone 3G 相对于第一代 iPhone 设备有三个主要不同点。第一，新增了支持 CDMA 蜂窝协议的特性。W-CDMA 是 3G 网络的空中接口标准协议。支持此协议的目的是提高连接速率，使其更有效率，以支持更多的用户连接。第二，和 iPhone 2G 不同的是，iPhone 3G 集成了 GPS（全球卫星定位系统），这个功能在 3G（s）和 iPhone 4 中也沿用了。最后，相对于 iPhone 2G 的系统参数，iPhone 3G 提高了 NAND 闪存容量（Semiconductor Insights，n.d.）。

表 1-2 iPhone 规格

参 数	iPhone（8GB/16GB）	iPhone 3G（8GB/16GB）	iPhone 3G（s）（16GB/32GB）	iPhone 4（16GB/32GB）
歌曲容量	2 000/4 000	2 000/4 000	4 000/8 000	4 000/8 000
屏幕大小 /in	3.5	3.5	3.5	3.5
分辨率 /px	480 × 320	480 × 320	480 × 320	960 × 480
蜂窝和无线网络	Wi-Fi，GSM，蓝牙	Wi-Fi，UMTS/3G，GSM，蓝牙	Wi-Fi，UMTS/3G，GSM，蓝牙	Wi-Fi，UMTS/HSDPA/HSUPA/3G，GSM，蓝牙
GPS 功能	不支持	支持	支持	支持
支持 App Store	OS 2.0 支持	支持	支持	支持
相机（百万像素）	2	2	3	5
拍摄视频	不支持	不支持	支持	支持，每秒 30 帧带声音的 HD（720p）视频
重量（盎司）	4.8	4.7	4.8	4.8
尺寸（in）	4.5 × 2.4 × 0.46	4.5 × 2.4 × 0.48	4.5 × 2.4 × 0.48	4.51 × 2.31 × 0.37
续航能力	通话 / 视频 / 互联网：8/7/6 小时；音频播放：24 小时	通话 / 视频 / 互联网：5/7/5 小时；音频播放：24 小时	通话 / 视频 / 互联网：5/10/9 小时；音频播放：30 小时	通话 / 视频 / 互联网：7/10/10 小时；音频播放：40 小时
价格（2011 年第一季度）	停售	停售	49 美元	199 美元 /299 美元

iPhone 硬件

iPhone 也像其他复杂的电子设备一样，是集模块、芯片和来自各制造商的许多电子元件为一体的产品。由于 iPhone 复杂多样的功能，它的硬件组件也非常多。表 1-3 列出了 iPhone 3G（s）设备的大部分组件清单，其中包括了制造商信息，以及型号或零件编号。

表 1-3 iPhone 3G（s）硬件组件

功 能	厂 商	型号 / 零件编号
应用处理器（CPU）	Samsung（三星）	S5L8900B01-412MHz ARM1176Z（F）-S RISC，128MB 处理栈，封装叠加，DDR SDRAM（双倍速率同步动态随机存储器）
3D 图形加速	Imagination Technologies	Power VR MBX Lite（图形处理芯片）
UMTS 功率放大器（PA），输出功率检测器的双工器和传输滤波器	TriQuint	TQM676031，Band 1，HSUPA；TQM666032，Band 2，HSUPA；TQM616035，Band5/6，W-CDMA/HSUPA PA 双工器
UMTS 收发器	Infineon	PMB 6272 GSM/EDGE 以及 W-CDMA，PMB 5701
基带处理器	Infineon	X-Gold 608（PMB 8878）
基带的支持内存	Numonyx	PF38F3050MOYOCE-16M 字节的 NOR 闪存和 8MB 的 psuedo-SRAM
GSM/EDGE 四频放大器	Skyworks	SKY77340（824 ~ 915MHz）

（续）

功 能	厂 商	型号 / 零件编号
GPS、Wi-Fi 和 BT 天线	NXP	OM3805，PCF50635/33 的变体
通信电源管理	Infineon	SMARTi Power 3i（SMP3i）
系统级电源管理	NXP	PCF50633
电池充电 /USB 控制器	Linear Technology	LTC4088-2
GPS	Infineon	PMB2525 Hammerhead II
NAND 闪存	Toshiba（东芝）	TH58G6D1DTG80（8GB NAND 闪存）
串行闪存芯片	SST	SST25VF080B（1MB）
加速器	ST Microelectronics	LIS331 DL
Wi-Fi	Marvell	88W8686
蓝牙	CSR	BlueCore6-ROM
音频编解码器	Wolfson	WM6180C
触摸屏控制器	Broadcom（博通）	BCM5974
链路显示接口（连接显示屏与图形控制器）	（美国）国家半导体	LM2512AA Mobile Pixel Link（移动像素链路）
触摸屏线路驱动器	德州仪器	CD3239

Samsung（三星）公司的 CPU 是一款 RISC（精简指令集）处理器，它运行核心的 iPhone 进程，并与 PowerVR 公司的协同处理器联合工作以实现图形加速。大概是为了延长电池续航时间，这款 CPU 的频率被降至 412 MHz（本来可能是 667 MHz）。其他一些内部组件也按照 iPhone 型号进行了相应变化。Semiconductor Insights 公司对许多不同类型设备的内部工作原理有很深入的研究，他们的设备库包括了不少移动设备，其中也包括 iPhone。同时，他们还针对每个设备都给出了研究报告，该报告涵盖产品的描述信息，以及怎样拆卸和重新组装设备、拆卸摄像头、硬件组件等的详细说明（Semiconductor Insights，n.d.）。

基带是 iPhone 中另一个必不可少的组件。基带用来控制所有通信指令，尤其是控制连接运营商服务的通信系统。之前我们提到过设备解锁，在解锁的过程中，基带就是黑客的目标之一，通过修改基带可以让被锁的 iPhone 使用任何运营商的 SIM 卡。iPhone 出厂的每一款新设备（例如，iPhone 4）都有新的基带版本，所以解锁程序也必须不断更新。可以从 Settings（设置）→ General（通用）→ About（关于本机）→ Modem Firmware（调制解调器固件）中查看设备的基带版本，如图 1-3 所示。

基带处理器在 NOR 闪存中有自己独立的 RAM（随机存储器）和固件，与其他的核心资源分开。基带处理器作为主 CPU 的资源器件。比如，Wi-Fi 和蓝牙由主 CPU 来管理，而基带处理器的 NVRAM 中则存储着它们的 MAC 地址。

下面是由 Semiconductor Insights 公司提供的手动将 iPhone 3G（s）拆卸后的照片，图 1-4 是设备的正面，图 1-5 是设备的背面。

图 1-3 基带版本——调制解调器固件

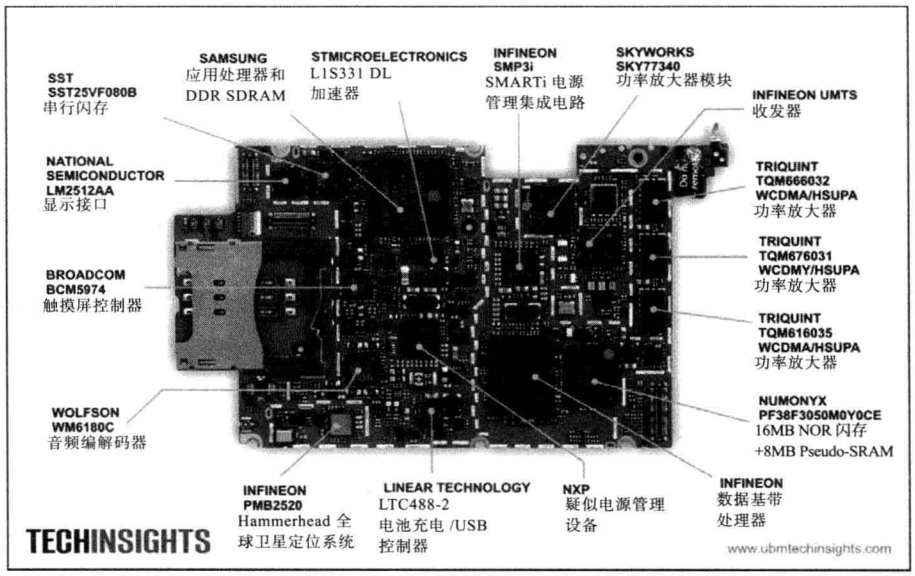


图 1-4 iPhone 拆卸图 – 正面