

图书基本信息

书名：<<iOS取证实战:调查、分析与移动安全>>

13位ISBN编号：9787111428626

10位ISBN编号：7111428625

出版时间：2013-6-24

出版时间：机械工业出版社

作者：Andrew Hoog,Katie Strzempka

译者：彭莉娟,刘琛梅,赵剑

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

前言

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。

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）。

内容概要

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。

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类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，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。

作者简介

作者：（美国）Andrew Hoog（美国）Katie Strzempka 译者：彭莉娟 刘琛梅 赵剑 Andrew Hoog，计算机科学家、Android取证领域的顶级专家、认证的取证分析师（GCFA和CCE）、计算机和移动取证研究员，是viaForensics（一家创新型的计算机和移动取证公司）的所有者。

电台因他写作计算机 / 移动取证指南方面的内容而做专门采访，他还经常应邀在各知名安全大会上演讲。

他致力于培养计算机和移动取证学科人才，引导并开展专家级的培训课程，并受邀为企业和执法机构授课和培训。

Katie Strzempka，viaForensics公司技术顾问，致力于取证研究、安全的审计和调查，是《iPhone取证》白皮书的合著者，也是各类iPhone取证商业工具的研究者。

她曾在财富500强公司从事了3年的信息安全工作，负责防火墙管理并协助内网和外网连接工作。

她在普度大学接受过数字取证、计算机和信息技术方面的教育多年，而今她为世界各地培养了大量移动取证研究人员。

书籍目录

译者序前言第1章 概述11.1 介绍11.1.1 策略11.1.2 开发者社区21.2 iPhone型号41.3 取证审查方法81.3.1 iPhone取证技术分级91.3.2 取证获取类型111.3.3 使用Linux取证131.4 小结271.5 参考文献28第2章 设备特性和功能292.1 介绍292.2 Apple设备概述292.3 操作模式302.3.1 基本模式312.3.2 恢复模式312.3.3 DFU模式312.3.4 退出恢复/DFU模式342.4 安全352.4.1 设备设置352.4.2 安全擦除362.4.3 应用程序安全362.5 与iTunes的交互372.5.1 设备同步372.5.2 iPhone备份372.5.3 iPhone还原382.5.4 iPhone iOS更新382.5.5 应用商店432.5.6 MobileMe432.6 小结432.7 参考资料43第3章 文件系统和数据存储453.1 介绍453.2 可恢复的数据453.3 数据存储位置463.4 数据存储方式483.4.1 内部存储493.4.2 SQLite 数据库文件503.4.3 属性列表513.4.4 网络543.5 存储器类型543.5.1 RAM543.5.2 NAND闪存553.6 iPhone操作系统583.7 文件系统593.7.1 卷613.7.2 日志623.7.3 iPhone磁盘分区623.8 小结633.9 参考文献63第4章 iPhone和iPad的数据安全654.1 介绍654.2 数据安全和测试654.2.1 美国计算机犯罪法664.2.2 由管理员负责的数据保护674.2.3 安全测试过程704.3 应用程序安全764.3.1 移动应用程序的企业或个人客户774.3.2 公司或个人移动应用开发者794.3.3 应用开发者的安全策略794.4 对设备和应用的安全建议844.5 小结854.6 参考文献85第5章 取证获取875.1 介绍875.2 iPhone取证概述875.2.1 调查类型875.2.2 逻辑技术和物理技术的区别885.2.3 目标设备的修改885.3 处理证据905.3.1 密码处理905.3.2 网络隔离915.3.3 关闭的设备915.4 映像iPhone/iPad915.4.1 备份获取915.4.2 逻辑获取975.4.3 物理获取975.5 映像其他Apple设备1085.5.1 iPad1085.5.2 iPod Touch1095.5.3 Apple TV1095.6 小结1095.7 参考文献109第6章 数据和应用程序分析1116.1 介绍1116.2 分析技术1116.2.1 挂载磁盘映像1116.2.2 文件雕复1126.2.3 strings1176.2.4 时间表创建及分析1196.2.5 取证分析1256.3 iPhone数据存储位置1306.3.1 默认应用程序1316.3.2 下载的应用程序1376.3.3 其他相关数据1406.4 iPhone应用程序分析和参考1476.4.1 默认应用程序1476.4.2 下载的第三方应用程序1676.5 小结1756.6 参考文献175第7章 商用工具测试1767.1 介绍1767.2 数据构造1767.3 分析方法1797.4 CelleBrite UFED1817.4.1 安装1827.4.2 取证获取1827.4.3 结果和报告1837.5 iXAM1887.5.1 安装1897.5.2 取证获取1897.5.3 结果和报告1917.6 Oxygen Forensic Suite20101937.6.1 安装1957.6.2 取证获取1957.6.3 结果和报告1967.7 XRY1997.7.1 安装2007.7.2 取证获取2007.7.3 结果和报告2007.8 Lantern2047.8.1 安装2057.8.2 取证获取2057.8.3 结果和报告2067.9 MacLock Pick2087.9.1 安装2097.9.2 取证获取2107.9.3 结果和报告2107.10 Mobilyze2117.10.1 安装2127.10.2 取证获取2127.10.3 结果和报告2137.11 Zdziarski技术2157.11.1 安装2177.11.2 取证获取2187.11.3 结果和报告2187.12 Paraben Device Seizure2207.12.1 安装2227.12.2 取证获取2227.12.3 结果和报告2237.13 MobileSyncBrowser2267.13.1 安装2267.13.2 取证获取2267.13.3 结果和报告2267.14 CellDEK2287.14.1 安装2297.14.2 取证获取2297.14.3 结果和报告2297.15 EnCase Neutrino2327.15.1 安装2327.15.2 取证获取2327.15.3 结果和报告2337.16 iPhone Analyzer2357.16.1 安装2367.16.2 取证获得2377.16.3 结果和报告2377.17 小结2397.18 参考文献240附录A iTunes备份位置241附录B 分析常规文件和数据类型的工具242附录C iPhone文件系统243

编辑推荐

《iOS取证实战:调查、分析与移动安全》编辑推荐：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。

版权说明

本站所提供下载的PDF图书仅提供预览和简介, 请支持正版图书。

更多资源请访问:<http://www.tushu007.com>