《iOS取证实战:调查、分析与移动啊

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

出版社：机械工业出版社

作者：Andrew Hoog,Katie Strzempka

页数：260

译者：彭莉娟,刘琛梅,赵剑

《iOS取证实战:调查、分析与移动啊

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。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）。

《iOS取证实战:调查、分析与移动啊

《iOS取证实战:调查、分析与移动啊

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。

《iOS取证实战:调查、分析与移动啊

作者简介

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进行演讲。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。

《iOS取证实战:调查、分析与移动啊

书籍目录

译者序
前言
第1章 概述1
1.1 介绍1
1.1.1 策略1
1.1.2 开发者社区2
1.2 iPhone型号4
1.3 取证审查方法8
1.3.1 iPhone取证技术分级9
1.3.2 取证获取类型11
1.3.3 使用Linux取证13
1.4 小结27
1.5 参考文献28
第2章 设备特性和功能29
2.1 介绍29
2.2 Apple设备概述29
2.3 操作模式30
2.3.1 基本模式31
2.3.2 恢复模式31
2.3.3 DFU模式31
2.3.4 退出恢复/DFU模式34
2.4 安全35
2.4.1 设备设置35
2.4.2 安全擦除36
2.4.3 应用程序安全36
2.5 与iTunes的交互37
2.5.1 设备同步37
2.5.2 iPhone备份37
2.5.3 iPhone还原38
2.5.4 iPhone iOS更新38
2.5.5 应用商店43
2.5.6 MobileMe43
2.6 小结43
2.7 参考资料43
第3章 文件系统和数据存储45
3.1 介绍45
3.2 可恢复的数据45
3.3 数据存储位置46
3.4 数据存储方式48
3.4.1 内部存储49
3.4.2 SQLite 数据库文件50
3.4.3 属性列表51
3.4.4 网络54
3.5 存储器类型54
3.5.1 RAM54
3.5.2 NAND闪存55
3.6 iPhone操作系统58

3.7 文件系统59
3.7.1 卷61
3.7.2 日志62
3.7.3 iPhone磁盘分区62
3.8 小结63
3.9 参考文献63
第4章 iPhone和iPad的数据安全65
4.1 介绍65
4.2 数据安全和测试65
4.2.1 美国计算机犯罪法66
4.2.2 由管理员负责的数据保护67
4.2.3 安全测试过程70
4.3 应用程序安全76
4.3.1 移动应用程序的企业或个人客户77
4.3.2 公司或个人移动应用开发者79
4.3.3 应用开发者的安全策略79
4.4 对设备和应用的安全建议84
4.5 小结85
4.6 参考文献85
第5章 取证获取87
5.1 介绍87
5.2 iPhone取证概述87
5.2.1 调查类型87
5.2.2 逻辑技术和物理技术的区别88
5.2.3 目标设备的修改88
5.3 处理证据90
5.3.1 密码处理90
5.3.2 网络隔离91
5.3.3 关闭的设备91
5.4 映像iPhone/iPad91
5.4.1 备份获取91
5.4.2 逻辑获取97
5.4.3 物理获取97
5.5 映像其他Apple设备108
5.5.1 iPad108
5.5.2 iPod Touch109
5.5.3 Apple TV109
5.6 小结109
5.7 参考文献109
第6章 数据和应用程序分析111
6.1 介绍111
6.2 分析技术111
6.2.1 挂载磁盘映像111
6.2.2 文件雕复112
6.2.3 strings117
6.2.4 时间表创建及分析119
6.2.5 取证分析125
6.3 iPhone数据存储位置130
6.3.1 默认应用程序131

6.3.2 下载的应用程序137
6.3.3 其他相关数据140
6.4 iPhone应用程序分析和参考147
6.4.1 默认应用程序147
6.4.2 下载的第三方应用程序167
6.5 小结175
6.6 参考文献175
第7章 商用工具测试176
7.1 介绍176
7.2 数据构造176
7.3 分析方法179
7.4 CelleBrite UFED181
7.4.1 安装182
7.4.2 取证获取182
7.4.3 结果和报告183
7.5 iXAM188
7.5.1 安装189
7.5.2 取证获取189
7.5.3 结果和报告191
7.6 Oxygen Forgensic Suite2010193
7.6.1 安装195
7.6.2 取证获取195
7.6.3 结果和报告196
7.7 XRY199
7.7.1 安装200
7.7.2 取证获取200
7.7.3 结果和报告200
7.8 Lantern204
7.8.1 安装205
7.8.2 取证获取205
7.8.3 结果和报告206
7.9 MacLock Pick208
7.9.1 安装209
7.9.2 取证获取210
7.9.3 结果和报告210
7.10 Mobilyze211
7.10.1 安装212
7.10.2 取证获取212
7.10.3 结果和报告213
7.11 Zdziarski技术215
7.11.1 安装217
7.11.2 取证获取218
7.11.3 结果和报告218
7.12 Paraben Device Seizure220
7.12.1 安装222
7.12.2 取证获取222
7.12.3 结果和报告223
7.13 MobileSyncBrowser226
7.13.1 安装226

7.13.2 取证获取226
7.13.3 结果和报告226
7.14 CellDEK228
7.14.1 安装229
7.14.2 取证获取229
7.14.3 结果和报告229
7.15 EnCase Neutrino232
7.15.1 安装232
7.15.2 取证获取232
7.15.3 结果和报告233
7.16 iPhone Analyzer235
7.16.1 安装236
7.16.2 取证获得237
7.16.3 结果和报告237
7.17 小结239
7.18 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

《iOS取证实战:调查、分析与移动啊

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。

《iOS取证实战:调查、分析与移动啊

精彩短评

1、翻译的超烂。有些地方意思反了。还有译者估计没有用过iPhone……
2、此书写的原理知识还是可以的。但翻译的太晚。很多实测的数据在现在看来是没有什么效果。
3、千万不要再买这个书店的了，太垃圾了，书都是残次品！这是在亚马逊买的最差的一次！
4、书比较专业，性价比不高
5、本书讲解了ios设备中提取数据信息用于取证审查的具体方法，是数字取证领域比较前沿的技术用书。书的第4章讨论了企业管理BYOD的一些安全建议；第5章讲的是ios设备的镜像或数据获取方法；第6章是分析ios系统取证数据的方法。第5，6章是本书数字取证的技术重点。
6、图书馆
7、取证方面内容较全面，但翻译的是2011年的国外书籍，移动系统，两年变化比较大，部分内容有些过时。

《iOS取证实战:调查、分析与移动啊

章节试读

1、《iOS取证实战:调查、分析与移动安全》的笔记-第1页

本书讲解了ios设备中提取数据信息用于取证审查的具体方法，是数字取证领域比较前沿的技术用书。
书的第4章讨论了企业管理BYOD的一些安全建议；第5章讲的是ios设备的镜像或数据获取方法；第6章是分析ios系统取证数据的方法。第5，6章是本书数字取证的技术重点。

2、《iOS取证实战:调查、分析与移动安全》的笔记-第91页

第五章主要讲了ios设备上的取证获取方法，也就是制作设备的映像或获取数据，其主要有备份获取，逻辑获取，物理获取。

3、《iOS取证实战:调查、分析与移动安全》的笔记-第57页

nand闪存操作的特殊之处。
nand可以读取（页）、写入（页），擦出（块），写入时可以将bit位由1-->0，但是不能直接将bit位由0-->1，只有使用块擦除才能实现0-->1。

4、《iOS取证实战:调查、分析与移动安全》的笔记-第70页

ios设备在企业的安全使用

iphone、ipad等移动设备已经广泛应用于企业办公，如iphone同步exchange outlook的邮件，这些ios设备上将存储企业大量内部信息，很多重要的敏感数据，在设备丢失、设备网络传输、设备擦除数据后都可能存在很大的安全隐患。因此如何保证ios设备在企业中安全应用非常重要，以下就是我对ios设备安全使用的一些建议。

1.配置策略

iphone等ios设备在企业作为byod使用前，必须首先交由企业的IT管理员设置好ios的各种安全策略，如使用配置实用工具设置密码策略，还需要设置特定应用程序的授权访问控制，如访问邮件附件的应用程序允许哪些可信程序。

2.安全测试

在使用前还必须构造好测试数据，通话记录，照片，短信，联系人，打开附件的邮件，删除的邮件，exchange的日程表，web浏览记录等众多测试数据（表4-4），生成iPhone数字取证镜像，测试设备上这些存储数据在设备被盗下的安全性；测试wifi，vpn等传输过程面对中间人攻击（mitm），基带攻击等的安全性；最后检查数据擦除后，iphone上残留数据，及恢复数据的安全。

3.其他安全隐患

此外还需要注意个人下载的应用程序可能存在的安全隐患，这些应用程序不能保证敏感数据内容安全的存储在ios设备上。

《iOS取证实战:调查、分析与移动啊

版权说明