

<<iOS取证分析>>

图书基本信息

书名：<<iOS取证分析>>

13位ISBN编号：9787121173943

10位ISBN编号：7121173948

出版时间：2012-8

出版时间：电子工业出版社

作者：肖恩·莫里西

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>

<<iOS取证分析>>

内容概要

本书介绍了针对苹果公司iPhone、iPad和iPod Touch设备的取证调查步骤、方法和工具，主要内容包括苹果移动设备的历史、iOS操作系统和文件系统分析、搜索与获取及时间响应、iPhone逻辑获取、逻辑数据分析、Mac和Windows计算机中的证据、地址位置信息分析、媒体注入与分析、网络分析等。

本书中介绍的取证步骤和方法在美国是可以被法庭所接受的。

本书适合计算机取证专业人士、执法人员、律师、安全专家，以及对此感兴趣的人员和教育工作者阅读。

本书也可供执法培训机构，以及开设有计算机取证、信息安全和电子物证等相关专业的高等院校作为教材使用。

<<iOS取证分析>>

作者简介

作者:(美)Morrissey

<<iOS取证分析>>

书籍目录

- 第1章 苹果移动设备的历史1
 - 1.1 iPod2
 - 1.2 iPhone的演变2
 - 1.2.1 ROCKR2
 - 1.2.2 苹果iPhone 2G简介3
 - 1.2.3 3G的iPhone4
 - 1.2.4 iPhone 3G[S]5
 - 1.2.5 iPhone 46
 - 1.3 苹果iPad6
 - 1.4 内部构造：iPhone和iPad的硬件7
 - 1.4.1 2G版iPhone的内部构造7
 - 1.4.2 iPhone 3G的内部构造9
 - 1.4.3 iPhone 3GS内部构造11
 - 1.4.4 iPhone 4的内部构造12
 - 1.4.5 iPad 内部构件13
 - 1.5 苹果App Store应用程序商店15
 - 1.6 iPhone黑客的兴起18
 - 1.7 小结18
- 第2章 iOS操作系统和文件系统分析19
 - 2.1 iOS特性的演变19
 - 2.1.1 iOS 119
 - 2.1.2 iOS 221
 - 2.1.3 iOS 322
 - 2.1.4 iOS 423
 - 2.2 应用软件的发展25
 - 2.3 iOS文件系统26
 - 2.3.1 HFS+ 文件系统26
 - 2.3.2 HFSX28
 - 2.4 iPhone分区和卷信息28
 - 2.4.1 OS分区31
 - 2.4.2 iOS系统分区32
 - 2.4.3 iOS数据分区35
 - 2.5 SQLite数据库37
 - 2.5.1 通讯录数据库37
 - 2.5.2 短信数据库37
 - 2.5.3 通话记录数据库38
 - 2.6 分析数据库38
 - 2.6.1 提取SQLite 数据库中的数据39
 - 2.6.2 Plist 属性列表文件45
 - 2.6.3 查看Plist属性列表文件45
 - 2.7 小结48
- 第3章 搜索、获取和事件响应49
 - 3.1 美国宪法第四修正案50
 - 3.2 通过手机追踪51

<<iOS取证分析>>

- 3.3 逮捕中的手机搜查51
- 3.4 技术进步和苹果iPhone52
- 3.5 如何搜查苹果设备53
- 3.6 隔离设备56
- 3.7 开机口令57
- 3.8 识别越狱的iPhone58
- 3.9 收集iPhone中的信息59
- 3.10 对iPhone连接过的Mac/
Windows计算机进行响应61
- 3.11 小结62
- 3.12 参考文献62
- 第4章 iPhone逻辑获取64
- 4.1 从iPhone、iPod Touch、iPad
中获取数据64
- 4.1.1 使用mdhelper软件获取数据65
- 4.2 可用的工具和软件68
- 4.2.1 Lantern68
- 4.2.2 Susteen Secure View 282
- 4.2.3 Paraben Device Seizure89
- 4.2.4 Oxygen Forensic Suite 201091
- 4.2.5 Cellebrite98
- 4.3 比较工具和结果101
- 4.3.1 购买软件需要考虑的因素102
- 4.3.2 Paraben Device Seizure
软件的结果102
- 4.3.3 Oxygen Forensic Suite 2010
软件的结果102
- 4.3.4 Cellebrite的结果103
- 4.3.5 Susteen Secure View 2
软件的结果103
- 4.3.6 Katana Forensics Lantern
软件的结果103
- 4.3.7 有关支持的问题104
- 4.4 小结104
- 第5章 逻辑数据分析105
- 5.1 搭建一个取证工作站105
- 5.2 资源库 (Library) 域110
- 5.2.1 通讯录111
- 5.2.2 缓存 (Caches) 114
- 5.2.3 通话记录116
- 5.2.4 配置概要117
- 5.2.5 Cookie117
- 5.2.6 键盘118
- 5.2.7 日志120
- 5.2.8 地图122
- 5.2.9 地图历史记录122
- 5.2.10 备忘录123

<<iOS取证分析>>

- 5.2.11 系统偏好设置123
- 5.2.12 Safari 浏览器124
- 5.2.13 记忆休眠状态125
- 5.2.14 短信和彩信126
- 5.2.15 语音信箱128
- 5.2.16 网络应用程序129
- 5.2.17 WebKit129
- 5.3 系统配置数据132
- 5.4 媒体域 (Media Domain) 134
 - 5.4.1 媒体文件目录134
 - 5.4.2 Photos.sqlite数据库139
 - 5.4.3 PhotosAux.sqlite 数据库139
 - 5.4.4 语音备忘139
 - 5.4.5 iPhoto相片140
 - 5.4.6 多媒体141
- 5.5 第三方软件142
 - 5.5.1 社交网络分析142
 - 5.5.2 Skype143
 - 5.5.3 Facebook145
 - 5.5.4 AOL AIM146
 - 5.5.5 LinkedIn146
 - 5.5.6 Twitter147
 - 5.5.7 MySpace147
 - 5.5.8 Google Voice148
 - 5.5.9 Craigslist151
 - 5.5.10 具备分析和挖掘功能的软件152
 - 5.5.11 iDisk152
 - 5.5.12 Google Mobile153
 - 5.5.13 Opera154
 - 5.5.14 Bing154
 - 5.5.15 文档和文档恢复155
- 5.6 反取证软件和过程157
 - 5.6.1 图片储藏库159
 - 5.6.2 Picture Safe159
 - 5.6.3 Picture Vault160
 - 5.6.4 Incognito Web Browser161
 - 5.6.5 Invisible Browser162
 - 5.6.6 tigertext162
- 5.7 越狱166
- 5.8 小结166
- 第6章 Mac和Windows计算机中的证据167
 - 6.1 Mac计算机中的证据167
 - 6.1.1 属性列表文件167
 - 6.1.2 MobileSync数据库168
 - 6.1.3 苹果备份文件的演变168
 - 6.1.4 密码锁定证书170

<<iOS取证分析>>

- 6.2 Windows计算机中的证据170
 - 6.2.1 iPodDevices.xml170
 - 6.2.2 MobileSync备份171
 - 6.2.3 密码锁定证书172
- 6.3 苹果移动设备备份文件分析172
 - 6.3.1 iPhone Backup Extractor172
 - 6.3.2 JuicePhone173
 - 6.3.3 mdhelper175
 - 6.3.4 Oxygen Forensics Suite 2010
- 手机取证套件176
- 6.4 Windows的取证工具和备份文件177
 - 6.4.1 FTK Imager178
 - 6.4.2 FTK 1.8178
 - 6.4.3 技巧和诀窍180
- 6.5 小结181
- 第7章 地理位置信息分析182
 - 7.1 地图应用程序182
 - 7.2 图片和视频的地理标记189
 - 7.3 基站数据198
 - 7.3.1 GeoHunter202
 - 7.4 导航应用程序205
 - 7.4.1 Navigon206
 - 7.4.2 Tom Tom209
 - 7.5 小结210
- 第8章 媒体注入211
 - 8.1 什么是数字版权管理 (DRM) 211
 - 8.1.1 数字版权管理的法律要素212
 - 8.1.2 案例分析：手机越狱214
 - 8.1.3 案例分析：苹果与Psystar215
 - 8.1.4 案例分析：在线音乐下载217
 - 8.1.5 案例分析：索尼BMG案件217
 - 8.1.6 DRM的未来218
 - 8.2 媒体注入219
 - 8.2.1 媒体注入工具219
 - 8.3 验证镜像225
 - 8.4 小结227
 - 8.5 参考文献229
- 第9章 媒体注入分析231
 - 9.1 使用Mac分析注入媒体231
 - 9.2 邮件234
 - 9.2.1 IMAP234
 - 9.2.2 POP邮件235
 - 9.2.3 Exchange236
 - 9.3 数据恢复 (碎片重组) 238
 - 9.3.1 MacForensicsLab238
 - 9.3.2 Access Data取证分析套件241

<<iOS取证分析>>

9.3.3 FTK和图片244

9.3.4 EnCase249

9.4 间谍软件252

9.4.1 Mobile Spy252

9.4.2 FlexiSpy255

9.5 小结256

第10章 网络分析257

10.1 关于证据链的考虑257

10.2 网络101：基础知识258

10.3 网络201：高级部分264

10.3.1 DHCP264

10.3.2 无线加密和身份认证265

10.3.3 取证分析266

10.3.4 网络流量分析268

10.4 小结272

<<iOS取证分析>>

章节摘录

版权页：插图：3.1 美国宪法第四修正案 美国宪法第四修正案最基本的权利就是禁止“无理搜查和扣押，（Henderson,2006）。

虽然Henderson以及其他很多案例都在强调这个权利，但是美国最高法院仍然解释说，并没有法律规定警察不能检查你的金融记录、电话、电子邮件、网站交易记录。

警察进行搜查应当取得搜查证，以保证第四修正法案的个人权利不被侵犯，特殊情况除外。

然而，有些搜查违背了合理的、要求保护个人隐私的期望，却并不违法（StiUwagon,2008）。

搜查证要求的免责条款包括经当事人同意、公共调查、突发事件和逮捕时进行的搜查。

一般来说，合理的隐私期望必须是“实际的隐私期望”，而且该期望必须是“被社会认可为合理的”（Stillwagon,2008）。

关于手机，联邦法院和美国司法部门把无线电子设备看做是“封闭的容器”，可以进行合法分析，并且认为，手机和其他密封容器一样，合法逮捕时是“可搜查”的。

某些情况下，警察可以不用搜查证就进行搜查。

如果警察在没有搜查证的情况下进行搜查，触犯了个人隐私，那么法院就必须拒绝采用本次搜查获取的证据（Stillwagon,2008）。

是否可以采用从无线设备中获取的证据，各个法院的认定不同，因为有的法院认为手机采用的技术与寻呼机的技术相似，因此证据合理，可以被采纳；另一些法院的看法则相反。

但是，法院准许对手机进行搜查的特殊情况，是针对的“逮捕附带搜查，（Stillwagon,2008）。

此类搜查必须是发生在合法逮捕的情境中，而且搜查只能在被捕嫌犯可控制的范围内发生。

逮捕之后的搜查期间，警察能够搜查任何物品，当然也包括嫌犯可控范围之内的手手机。

两个标志性的案件：美国Olmstead案件（277 U.S.438，1928）和Katz案件（398 U.S.347，1967），缩小了第四修正案的解释范围（Henderson,2006）。

Olmstead案件里，法院判定政府可以监听手机通话而不违反第四修正案。

之后，Katz案件里，法院澄清第四修正案保护的不是地方，而是人。

这两个案件得出一个共同的结论：对使用手机拨通号码与第三方交流信息，第四修正案无法满足其合理的、保护隐私的要求。

3.2通过手机追踪 对执法部门的工作人员来说，手机最大的优点，就是在任何时间下都可以追踪到特定手机的位置（Henderson,2006）。

如果警察能够追踪一部手机，也就意味着他们能够追踪一个人的位置。

警官能够通过追踪手机记录从而将一些犯罪嫌疑人与案件联系起来（Walsh,D.,&Finz,s.,2004）。

例如，在Scott Peterson谋杀案中，警官查阅了Scott Peterson的手机位置信息，公诉人依据此信息把他与犯罪现场联系起来，最终判定他谋杀妻子的罪名成立。

美国联邦通信委员会（FCC）于2001年启动了一个计划，迫使手机运营商推出一种新技术，这种技术使用多个重叠的蜂窝基站更精确地定位到手机的位置（Fletcher,F.,&Mow,L.,2002）。

继而紧急救援机构进一步运用手机追踪技术，可帮助紧急救援人员迅速到达救援现场。

警察和政府官员之后发现这个技术还有另一个用途：追踪疑犯、进行调查、破案和检举犯罪（Henderson,2006）。

因此，如果你不想被追踪，那么你唯一的选择就是不携带手机。

<<iOS取证分析>>

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>