

电子证据调查指南

主 编 / 戴士剑 刘品新

副主编 / 陈景春 滕 达 方 勇 丁丽萍

审 定 / 陈 刚 李学军 杜春鹏



DIANZI ZHENGJU DIAOCHA ZHINAN



中国检察出版社



电子证据调查指南

主 编 / 戴士剑 刘品新

副主编 / 陈景春 滕 达 方 勇 丁丽萍

审 定 / 陈 刚 李学军 杜春鹏

DIANZI ZHENGJU DIAOCHA ZHINAN

中国检察出版社

图书在版编目 (CIP) 数据

电子证据调查指南/戴士剑, 刘品新主编. —北京: 中国检察出版社, 2014. 7

ISBN 978 - 7 - 5102 - 1128 - 7

I. ①电… II. ①戴… ②刘… III. ①电子 - 证据 - 研究
IV. ①D915. 130. 4

中国版本图书馆 CIP 数据核字 (2014) 第 006388 号

电子证据调查指南

戴士剑 刘品新 主编

出版发行: 中国检察出版社

社 址: 北京市石景山区香山南路 111 号 (100144)

网 址: 中国检察出版社 (www. zgjccbs. com)

电 话: (010)88960622(编辑) 68650015(发行) 68636518(门市)

经 销: 新华书店

印 刷: 三河市西华印务有限公司

开 本: 720mm × 960mm 16 开

印 张: 44 印张

字 数: 808 千字

版 次: 2014 年 7 月第一版 2014 年 7 月第一次印刷

书 号: ISBN 978 - 7 - 5102 - 1128 - 7

定 价: 99.00 元

检察版图书, 版权所有, 侵权必究
如遇图书印装质量问题本社负责调换

序 拥抱电子证据的时代

我们身处在网络的时代。不知不觉间，网络已经渗入到我们生活的方方面面，人们已越来越离不开智能手机、数码产品和网络技术。与此同时，电子数据也日益成为发现犯罪、证明犯罪的重要线索和证据。与这一证据种类关联的技术门类与专业生态亦蓬勃生长。因为这样的背景，电子证据得以在两大诉讼法的修订中获得了独立的证据地位。

种种迹象表明，在科技信息化的前提之下，传统观念里的检察技术工作正无可避免地面临着巨大的战略转型。中国人民大学法学院教授何家弘认为，就司法证明方法的历史而言，人类曾经从“神证”时代走入“人证”时代，又从“人证”时代走入“物证”时代。也许，我们即将走入另一个司法证明时代，即电子证据时代。何教授带有强烈预见性的评论，给检察机关抛出了一个历史性的命题。如何从执法理念的高度完成这次转型，是检察技术人的使命。

今年以来，高检院检察技术信息研究中心正在倾力搭建检察机关电子证据云平台，试图为检察技术工作的战略转型开辟一条路径。这个富有建设性的平台的思路是，采用云计算架构，在高检院司法鉴定中心构建大规模高性能的电子证据分析鉴定平台，实现对电子证据的快速镜像和取证分析；引入大数据理念，构建电子证据管理平台，实现对海量电子数据的存储、归档和快速查询检索，通过数据的碰撞发现线索，为职务犯罪侦查指明方向。当然，建设中的这个云平台还会为侦查监督、审查起诉、控告申诉乃至民行检察工作等等提供服务。

一个并不遥远的场景是，通过云计算架构，基层检察机关只需要通过简单的客户端软件即可接入这个平台，实现电子证据的远程取证和分析鉴定。因无需往返移交设备或者介质，取证与鉴定将变

得更加经济、安全和高效。

本书采用全新的视角，从司法实务的角度观察电子数据，探索技术与司法实务的契合，不仅适合技术人员参考研读，更适合侦查、公诉等司法实务人员学习借鉴。在本书中，作者提出了电子信息无处不在，在司法活动中，信息系统扮演着“沉默的现场知情人”的角色，因为这种无处不在，其为侦查工作服务具有天然性；又因为其技术性，如何展现这个“沉默的现场知情人”所掌握的案情，是技术人员所必须完成的任务。配合作者今年已经上架的《数据恢复技术》（经典重现版），对于帮助司法实务人员从技术和实务工作等多个视角来理解和应用电子数据，具有重大的意义和价值。

本书主要作者戴士剑是我国数据恢复技术学科的奠基人，在计算机取证、信息安全领域有着独特的影响，出版多本专著和论文。1997年毕业于合肥炮兵学院作战指挥专业，曾就职总装备部某研究所，获全军科技进步一等奖一项，三等奖多项，自2009年加入检察技术队伍，到最高人民检察院司法鉴定中心工作，一直致力于促进检察系统电子证据学科的发展与建设。

作为戴士剑同志的领导，我乐于并支持该书的出版，预祝该书成为我们理解和应用电子数据的得力助手。

是为序。

最高人民法院检察技术信息研究中心主任

赵志刚

目 录

序 拥抱电子证据的时代	赵志刚 (1)
导 言	(1)
第一章 电子证据概述	(4)
第一节 电子证据的概念与表现形式	(4)
一、电子证据的概念	(4)
二、电子证据的表现形式	(6)
第二节 电子证据与传统证据的关系	(7)
第三节 法律中的“电子证据”	(9)
一、《刑事诉讼法》中的电子证据	(9)
二、《民事诉讼法》中的电子证据	(9)
三、“两个证据规定”中的电子证据	(10)
第四节 电子证据的分类与特征	(11)
一、电子证据的分类	(11)
二、电子证据的特征	(12)
第五节 信息系统在案件中的地位与作用	(18)
一、对象论	(18)
二、工具论	(19)
三、线索论	(20)
四、沟通渠道论	(21)
五、现场论	(23)
六、其他观点	(33)
第六节 电子证据的相关界定	(35)
一、现有的一些鉴定类型	(35)
二、计算机犯罪与计算机证据的区别	(39)
三、电子数据与视听资料的关系	(39)

第二章 通信技术基础与证据调查	(42)
第一节 信息与信号	(42)
一、信息	(42)
二、信号	(43)
第二节 通信发展简史	(46)
一、古代通信技术	(48)
二、“电力”通信时代	(49)
三、现代通信网络	(50)
四、有线电报和无线电报	(51)
第三节 模拟通信与数字通信	(57)
第四节 移动通信技术原理	(57)
一、移动通信的发展历史	(59)
二、蜂窝电话基本原理	(61)
三、关键术语	(62)
四、系统的主要特点	(66)
五、SIM 卡	(67)
第五节 手机在侦查中的应用	(70)
一、定位功能	(70)
二、信息截获	(71)
三、手机信息获取	(73)
四、可获取手机信息类型	(79)
第六节 手机的扣押	(80)
第七节 SafeMobile 盘石手机取证分析系统功能介绍	(81)
第八节 VAT - CelAn 手机行为分析系统功能介绍	(81)
一、工具功能特点	(82)
二、主要分析模块介绍	(86)
三、多机关联分析模块介绍	(89)
四、智能报告生成	(91)
第九节 效率源一站式智能手机专业取证系统介绍	(92)
一、产品概述	(92)
二、操作使用介绍	(99)
三、系统管理	(114)
四、辅助功能	(119)

第三章 声纹与测谎	(121)
第一节 声波、声波数字化及声纹鉴定	(121)
一、声波	(121)
二、声波数字化	(124)
三、声纹鉴定	(127)
第二节 测谎与情感分析	(132)
一、测谎与测谎技术	(132)
二、测谎的功能	(134)
三、测谎技术在我国的应用	(136)
四、测谎技术的局限性	(137)
第三节 语音情感分析	(139)
一、人类的发音机制	(140)
二、LVA 分析原始值	(141)
三、LVA 分析的谎言类型	(142)
四、LVA6.5 工作模式	(143)
五、LVA 技术在检察系统的应用	(145)
第四章 计算机证据调查技术基础	(146)
第一节 信息技术	(146)
一、信息构成	(146)
二、信息载体	(146)
三、信息技术	(147)
第二节 计算机系统	(149)
一、二进制	(149)
二、微型计算机系统结构	(152)
三、内存与字节	(156)
四、编码	(158)
第三节 存储层次	(174)
一、应用程序层	(178)
二、操作系统与文件系统层	(188)
三、文件签名	(191)
四、存储设备层	(196)
第四节 计算机搜查	(197)
一、是否需要申领搜查证	(201)
二、如何确定搜查的范围	(203)

三、如何保护其他人员的合法权益	(205)
四、第三方如何进行必要的协助	(206)
第五节 证据固定的三大技术基础	(208)
一、只读的概念	(211)
二、镜像的概念	(211)
三、数字指纹的概念	(214)
第六节 内存信息的获取	(220)
第七节 带电移机	(221)
第五章 密码学基础及其在取证中的应用	(222)
第一节 传统安全与保密	(222)
第二节 加密通信模型	(228)
第三节 古典密码学	(230)
一、移位加密法	(234)
二、关键词加密法	(236)
三、仿射加密法 (Caesar 的穷举变种)	(240)
四、多文字加密法 (Playfair)	(240)
五、置换加密法	(241)
第四节 现代密码学	(241)
第五节 密码算法	(246)
第六节 解密技术	(247)
第七节 解密的应用	(254)
第六章 信息安全与网络取证技术基础	(258)
第一节 信息安全概念	(258)
一、保密性 (Confidentiality)	(259)
二、完整性 (Integrity)	(260)
三、可用性 (Availability)	(261)
四、真实性 (Authenticity)	(261)
五、不可抵赖性 (Non-repudiation)	(261)
第二节 单机信息安全的由来	(261)
第三节 网络信息安全	(265)
一、网络基础	(270)
二、OSI 参考模型与 TCP/IP 协议簇	(275)
三、互联网服务	(287)
四、网络互连设备	(294)

五、网络信息传输	(298)
第四节 网络信息服务过程	(301)
一、PSTN 公共电话网	(301)
二、通过局域网网关接入	(307)
三、DDN 专线	(308)
四、CATV 接入和电力线接入	(308)
五、卫星接入	(309)
六、光纤接入	(309)
七、无线接入	(309)
八、FTTX + LAN 接入方式	(310)
九、移动接入方式	(310)
第五节 网络取证原理	(311)
第六节 网络信息安全	(313)
一、网络身份的确认	(318)
二、访问控制	(324)
第七节 网络安全威胁	(331)
第八节 安全技术	(332)
一、加密	(332)
二、认证和识别	(333)
三、权限控制	(334)
四、安全工具分类	(335)
第九节 信息战	(336)
第十节 信息犯罪	(338)
一、信息犯罪的起源	(338)
二、信息犯罪的特点	(338)
第十一节 网络证据调查	(341)
第七章 电子数据勘验与鉴定程序规则	(343)
第一节 现场勘验	(343)
第二节 程序规则	(345)
第八章 单机证据分析	(354)
第一节 安全策略	(355)
第二节 日志的查看	(357)
第三节 Windows 登录类型	(363)
第四节 其他日志	(364)

第五节 其他痕迹	(367)
第六节 内存转储	(369)
一、内存固定	(370)
二、在线信息获取	(370)
第七节 pagefile. sys	(374)
第八节 hiberfil. sys	(374)
第九节 临时文件和各类镜像文件	(374)
第十节 系统分析与监控工具	(376)
一、虚拟机	(376)
二、文件监控	(379)
三、注册表监控	(380)
四、系统文件监控	(381)
五、进程分析	(383)
第十一节 自启动分析	(395)
一、AUTOEXEC. BAT	(395)
二、“启动”菜单	(397)
三、WIN. INI 与 SYSTEM. INI	(398)
四、WININIT. INI 与 WINSTART. BAT	(400)
五、Config. sys	(402)
六、USERINIT. INI	(402)
七、Dosstart. bat	(402)
八、注册为系统服务	(402)
九、驱动级木马	(402)
十、DESPTOP. ini 和 FOLDER. HTT	(404)
十一、注册表启动	(404)
十二、Explorer. exe 启动	(408)
十三、屏幕保护启动方式	(408)
十四、依附启动	(409)
十五、脚本启动	(409)
十六、计划任务启动方式	(410)
十七、AutoRun. inf 启动方式	(410)
十八、start 命令	(411)
十九、控制面板启动	(411)
二十、修改组策略	(411)

二十一、修改文件关联	(413)
二十二、添加到流媒体中	(414)
第十二节 如何查看木马	(414)
一、系统自带工具	(414)
二、防病毒工具	(415)
三、微点自主防御软件	(416)
四、IceSword	(418)
五、knlsc	(419)
第十三节 信息隐藏	(419)
一、通过文件属性进行隐藏	(419)
二、超级隐藏	(420)
三、变换扩展名	(421)
四、特殊目录/文件名	(424)
五、加密	(426)
六、网页加密	(426)
七、设置访问权限	(426)
八、回收站隐藏	(428)
九、System Volume Information	(429)
十、捆绑隐藏	(432)
十一、添加到文件后	(433)
十二、流方式隐藏	(433)
十三、利用设备名	(436)
十四、嵌入/信息隐藏	(438)
第十四节 数码照片中的隐私信息	(440)
第十五节 WORD 文档中的隐私信息	(446)
一、访问记录	(446)
二、临时文件	(447)
三、WBK 文件	(448)
四、虚拟内存文件与休眠文件	(448)
五、非法操作时所产生的“被挽救的文档”	(448)
六、Temp 目录	(449)
七、回收站目录	(449)
八、剪贴板	(449)
九、摘要	(449)

十、WORD 口令破解	(452)
第十六节 上网痕迹与邮件	(455)
第十七节 证据分析专业工具	(456)
一、EnCase	(456)
二、FTK	(481)
三、盘石介质取证分析系统 SafeAnalyzer	(495)
四、X - Ways	(550)
五、其他工具	(550)
第十八节 溯源性分析	(551)
一、硬件系统	(552)
二、软件系统	(552)
三、溯源性	(554)
第十九节 存储介质检验	(558)
第二十节 鉴定分析工作的应用	(558)
第二十一节 电子证据让虚假鉴定显原形	(559)
第九章 网络证据分析	(562)
第一节 网络数据包协议解析	(562)
一、HTTP 数据包分析	(562)
二、电子邮件数据包分析	(564)
三、即时通信数据包分析	(565)
四、FTP 数据包分析	(567)
五、P2P 共享文件数据包分析	(568)
六、Telnet 数据包分析	(569)
七、VOIP 数据包分析	(569)
八、HTTP 视频流数据包分析	(570)
九、HTTPS/SSL 数据包分析	(571)
十、WLAN 数据包介绍	(572)
第二节 网络事件处理与取证	(572)
一、网络舆情	(572)
二、社会关系排查	(579)
三、网络洗钱	(582)
四、网络诽谤与人身攻击	(584)
五、网络谣言	(588)
六、网络诈骗	(591)

七、网络水军与网络推手	(593)
八、网络删帖	(596)
九、网络侵权	(597)
第三节 网络线索应用	(597)
第四节 网站远程固定工具	(601)
第十章 动态仿真分析系统	(603)
第一节 工具简介	(603)
一、概述	(603)
二、主要功能	(603)
第二节 软件安装	(604)
一、系统要求	(604)
二、SafeVM Pro 安装升级	(604)
第三节 操作方法	(607)
一、设备连接	(607)
二、系统仿真	(607)
三、提取密码 Hash 值	(614)
四、启动失败配置	(614)
第四节 仿真系统在木马调查中的使用	(616)
一、操作系统仿真	(617)
二、搭建网络环境	(618)
三、木马行为分析	(619)
第五节 在线动态数据分析出现问题的应对	(619)
一、64 位系统仿真失败	(620)
二、启动虚拟机时出现 “The physical disk is already in use” (物理磁盘已被使用) 字样	(620)
三、Unix/Linux、Windows 双系统启动失败	(621)
四、切换到虚拟机系统, 键盘及鼠标没有反应	(622)
第六节 ATT-3000	(622)
第十一章 电子邮件调查	(623)
第一节 电子邮件的发送和接收	(623)
第二节 电子邮件地址构成	(624)
第三节 电子邮件起源	(626)
第四节 电子邮件服务器系统	(627)
第五节 使用电子邮件的两种常用方式	(627)

一、客户端方式	(627)
二、WEB 方式	(628)
第六节 电子邮件真实性判定	(629)
第七节 电子邮件的鉴定思路	(641)
第八节 典型案例	(644)
一、北京大学顶替上学的邮件	(644)
二、垃圾电子邮件典型案例	(647)
三、劳动争议中电子邮件证据	(648)
四、邮箱泄密典型案例	(648)
第十二章 网络公证与打击侵权盗版	(651)
第一节 网络公证概述	(651)
一、网络公证的含义	(651)
二、美国网络公证发展概述及对我国公证行业的借鉴意见	(654)
三、美国网络公证行动对于我国公证行业的借鉴意义	(654)
第二节 网络公证与电子商务	(656)
一、网络诚信问题已成为电子商务发展的“瓶颈”	(656)
二、充分发挥电子认证服务与网络公证服务的作用，对于构建 诚信网络有现实意义	(656)
第三节 网络公证与互联网知识产权保护	(657)
一、网络环境下的知识产权保护现状	(657)
二、网络公证与网络环境下的知识产权保护	(658)
第四节 小结	(660)
第十三章 电子证据工具体系与取证云	(661)
第一节 取证工作云	(661)
一、应用背景	(661)
二、取证工作云的业务	(663)
三、工作云平台结构	(663)
四、工作云平台业务之间的关系	(664)
五、工作云平台业务流程	(665)
六、后端分析	(666)
第二节 取证服务云	(666)
一、应用背景	(666)
二、取证服务云的数据采集	(666)
三、取证服务云的业务	(667)

第十四章 网上交易、跨国犯罪与国际协作	(669)
第一节 网上交易平台	(669)
第二节 网游交易平台	(670)
第三节 主要跨国犯罪类型	(671)
一、洗钱	(671)
二、恐怖行动	(671)
三、盗窃文物和艺术品	(672)
四、侵犯知识产权	(672)
五、非法买卖武器	(672)
六、劫机	(672)
七、海盗	(672)
八、抢劫地面交通工具	(673)
九、骗保	(673)
十、计算机犯罪	(673)
十一、生态犯罪	(673)
十二、贩卖人口	(673)
十三、人体器官交易	(674)
十四、非法贩卖毒品	(674)
十五、虚假破产	(674)
十六、参与非法经营	(674)
十七、贪污受贿	(674)
第四节 国际反贪局联合会	(675)
第五节 引渡制度	(676)
一、概念	(676)
二、发展历史	(676)
三、引渡主体	(676)
四、引渡对象	(678)
五、引渡理由	(678)
六、引渡效果	(680)
第六节 《网络犯罪公约》	(680)
第十五章 电子数据综合应用	(683)
第一节 电子数据综合应用的实际做法	(683)
第二节 结语	(684)

导 言

2013年7月15日晚，京东商城CEO刘强东和一名女下属，几乎同时，分别在各自微博中贴出了一张“阳台上的西红柿”的图片。网友“精心”比对后觉得，两张图片里可能是同一个西红柿……于是，一段绯闻就诞生了。虽然两张图片很快都被删除，刘强东更高呼“八卦，八卦”，自称“躺着中绯闻枪”，但网友快手留存的截屏图依旧在微博上被大量转发，八卦史称“西红柿门”。

“晒生活”，是微博的一个特色。7月15日18:28，京东商城小家电采销总监庄佳（微博名@VikiZhuang）发布了三张西红柿熟透的照片，配文中称：“惊喜地发现结出小番茄啦，只有三只，舍不得摘~”

仅仅11分钟后（当日18:39），京东商城CEO刘强东也在其新浪微博上更新了一张西红柿照片，并介绍说：“阳台上的西红柿终于熟了。”

都种了西红柿，都恰好成熟了。原本普通的“晒生活”照，经网友的仔细研究，发现两张图中的西红柿，无论从长相、大小，还是图中阳台的方位布置，几乎是一模一样。关于两组图片中“是同一个西红柿”的猜想，点燃了网友的八卦热情，引来了大量的转发、评论。

当晚，@VikiZhuang和刘强东先后都删除了西红柿的图片。

有网友评论：“世界上没有两枚一模一样的西红柿，如果有，那就是爱情。原来，不只东京有爱情故事，京东也有。”

而下面的晒微博就没有那么幸运了：

有网友爆料，一“局长”与女性朋友在微博上互相传情，一时间你来我往，很是热闹，想不到“局长”也是性情中人，毫不掩饰自己“多情本色”。表达感情，本是在QQ上倾诉衷肠，属于自己的私密生活，用不着用微博直播自己的感情经历，搞得满城风雨，但是“局长”毫不吝啬地通过微博向大家坦诚了自己作为一名国家干部上班聊天，开房安排情人“宝贝”的真实生活。

微博直播后，引得网友啧啧称奇，有好奇的网友甚至打起了“学习局长”、“爱你就要喊出来”的勇气。有网友指出，这名“局长”是溧阳市一局级机关的领导。下午6点钟左右，看两人的微博聊天内容已经删除一空，但是两人“情意绵绵”的痕迹还是被细心的网友一一收藏。