杜春鹏◎著

电子证据取证和鉴定

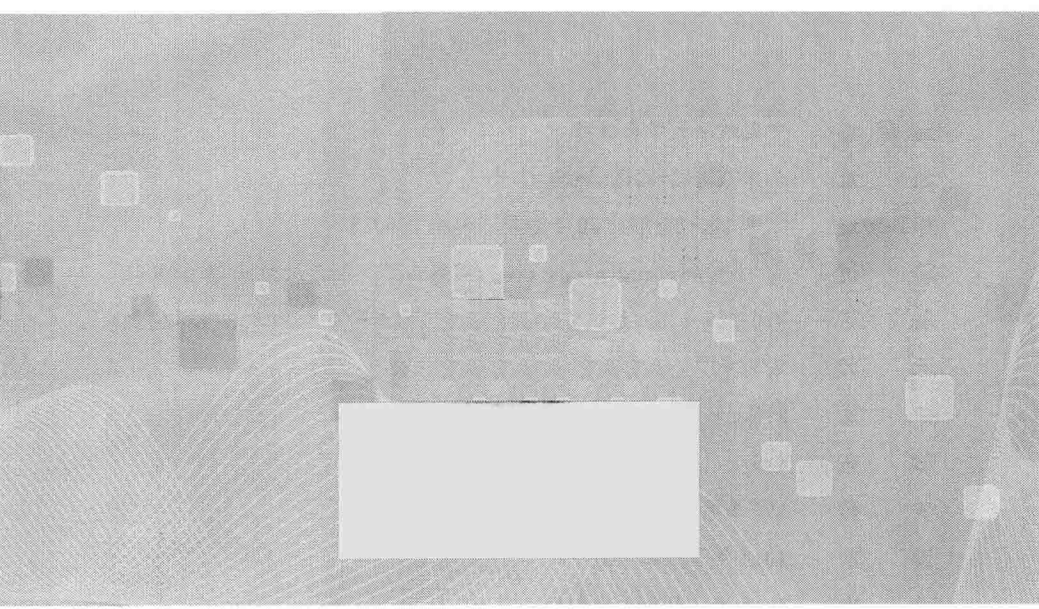
ELECTRONIC EVIDENCE FORENSICS

中国政法大学出版社

杜春鹏◎著

电子证据取证和鉴定

ELECTRONIC EVIDENCE FORENSICS



中国政法大学出版社

2014·北京

图书在版编目（CIP）数据

电子证据取证和鉴定/杜春鹏著. —北京:中国政法大学出版社，2014.6
ISBN 978-7-5620-5499-3

Ⅰ.①电… Ⅱ.①杜… Ⅲ.①电子技术－应用－证据－收集－中国
②电子技术－应用－证据－司法鉴定－中国 Ⅳ.①D925.213.4②D918.9

中国版本图书馆 CIP 数据核字(2014)第 145642 号

出 版 者　中国政法大学出版社
地　　址　北京市海淀区西土城路 25 号
邮寄地址　北京 100088 信箱 8034 分箱　邮编 100088
网　　址　http://www.cuplpress.com（网络实名：中国政法大学出版社）
电　　话　010-58908285(总编室) 58908433（编辑部）58908334(邮购部)
承　　印　固安华明印业有限公司
开　　本　880mm×1230mm　1/32
印　　张　8.5
字　　数　195 千字
版　　次　2014 年 6 月第 1 版
印　　次　2014 年 6 月第 1 次印刷
定　　价　26.00 元

序言 The preface

在20世纪后期全球范围内掀起的信息化和电子化浪潮对人类社会的生产生活带来的全方位深刻影响中，证据的电子信息化趋势便是重要变革之一，以数字式计算机、互联网络和相关系统为载体的电子证据出现在各种类型的案件中的频率和重要性与日俱增，关乎着诉讼活动的效果乃至成败。电子证据在我国出现和运用于司法实践已经有逾二十年的历史，其法律地位在2013年生效实施的《刑事诉讼法》和《民事诉讼法》中得以正式确立。可以预见的是，电子证据必定会在未来的司法实践舞台上发挥更加重要和无以替代的作用。

电子证据取证和鉴定是应用电子证据来认定案件事实的必要前提和先置程序，没有进行合乎法律和技术的双重要求的电子证据取证和鉴定工作，是无从谈及如何开展后续诉讼程序的，因此进行电子证据取证和鉴定的研究具有相当重要的理论和实践意义。电子证据取证和鉴定属于跨越文理两大学科的交叉性研究领域，其内容涵盖侦查学、证据调查学和计算机网络科学等学科。目前国内外对此领域的研究时间不久，尤其在跨学科交叉研究方面更是最近几年才刚刚出现。该研究领域的跨学科

特性和当前所处的阶段对研究者的学科背景和研究能力提出了较高要求。

本书的作者杜春鹏博士对电子证据取证和鉴定的研究立足于实践。他注意到多数此领域现有的研究在电子取证之法律属性与技术特性的融合方面体现不佳，时常出现同一部著作中技术问题和法律问题各说各是、相互割裂的状况，难以实现不同学科之间的交叉和融合，也无益于加深对电子取证和鉴定问题的实务性理解和把握。经过认真思考和交流总结，作者提出了自己的研究切入点和研究进路，即在证据科学的视角下通盘关注与电子证据取证和鉴定相关的法律和技术问题，以证据适用作为结合点将法律和技术两方面特质统合。提出电子证据取证和鉴定的总体目的和中心任务是提供满足证据能力要求的证据为相关诉讼服务，而电子证据取证和鉴定的具体方面则是实现这一目的的手段或工具。在理顺电子取证目的和取证手段的辩证关系的基础之上，作者将电子证据满足证据能力的总体要求加以分解，对可能发生影响的相关要素进行分析和梳理，并尝试提供具备一定体系化和操作性的实现思路和方案设计。作者提出电子证据取证和鉴定只有适格的主体遵循法定或推荐的程序，应用经过验证的方法和可信的工具来完成，才可能使取证和鉴定的结果更好地满足证据能力的要求并在案件中发挥其应有的证明价值。

作者对本书中所做研究的契合点把握准确，研究脉络清晰，对于如何审查使用电子证据提供了具有一定实际意义的思路与方案。当然现阶段的研究还仅仅是一个起步，必然会有部分不足，有能够进一步深入和优化的空间。杜春鹏博士在中国政法大学侦查学研究所任教，适值中国政法大学侦查学专业进行

“网络犯罪侦查”改造的发展良机，作为导师，衷心希望他珍惜专业发展的条件，坚持在这一领域持续钻研，不断取得更好的成绩！

刘 耀

摘 要 Abstract

电子证据是我国诉讼法律明确规定的证据形式，是信息时代科学证据的典型代表。电子证据取证和鉴定是对电子证据的专门性调查活动，是对电子证据进行审查运用的先置程序和条件保证。电子证据取证和鉴定的结果需要在相关性、合法性和科学可靠性方面得以有效确认，才能使所获得的电子证据满足证据能力的要求，并在案件中发挥出应有的证明力。

本书从证据科学的视角对电子证据取证和鉴定进行了系统研究，参照国内外有关质量标准和最优方法，从主体、技术、程序、工具等影响因素分析，认为电子证据取证和鉴定需要适格的调查主体，遵循法定程序和取证要求，对涉案的电子证据以科学验证的方式予以获取、识别、保存、传输、分析、鉴证，才能最终使所得的电子证据能够为法庭采纳和采信。

在上述思想的主导下，本书主体内容共包括五章：

第一章为证据科学的基本问题及电子证据取证和鉴定概述，本章首先考察了证据科学的学科属性、研究领域和发展历程，进而论及证据科学视角下电子证据取证研究所涵盖的专门问题。

第二章为电子证据取证技术，电子证据取证行为事实上几乎就是对相关技术的运用。本章列举了电子证据取证技术的范

围、分类和通用要求，随后介绍了电子证据取证的常用技术。

第三章为电子证据取证工具，电子证据取证工具是相关技术的集中承载和体现。本章首先界定了电子证据取证工具的范围和形式，随后介绍了业界主流的电子证据取证工具，电子证据取证实验室作为广义的取证工具也设专节进行研究。本章最后对电子证据取证工具做了评估并预测了其发展趋势。

第四章为电子证据取证程序，电子证据取证和鉴定应当遵循相应的取证程序。本章就电子证据取证程序从取证程序模型和标准取证程序两个层面进行了研究。

第五章为几种典型的电子证据取证类型简介，分别就最为常见的 Windows 取证、网络取证和手机取证进行了专门研究。

目录 Contents

导 论

一、研究背景

任何研究均无法脱离特定的背景条件而单独进行，研究背景的交代有助于明确研究方向和把握研究思路。对于电子证据取证和鉴定的研究背景，作者拟从下述两大方面予以展开。

（一）我国电子证据取证和鉴定工作已见端倪并得到一定发展，不仅为开展对应的研究提出了要求，同时亦为研究的进行积累了资料和素材

电子证据是人类社会生产生活发展到一定水平，尤其是在科学技术方面获得巨大进步并将之成果渗入到诉讼领域的情形下应运而生的。电子证据的产生与电子技术，尤其是电子计算机技术〔1〕密切相关，可以说没有电子计算机技术的发展就不会出现电子证据，也就无从谈及围绕电子证据所产生的各种应用以及出现的问题。电子计算机技术快速发展，相关应用不断丰富，已经渗透至人类社会生产生活的方方面面，电子证据亦

〔1〕 电子计算机技术系指将电子计算机科学原理应用于工程实践而生成的所有经验性成果和技术性成果的总和。电子技术的范围显然大于电子计算机技术，相应的电子证据的范围也要大于电子计算机证据，但是通常在并无必要做严格区分的情况下，人们常常将电子证据和（电子）计算机证据等名称通用，对此问题后文还会有进一步专门介绍。

伴随这一过程出现于司法舞台，快速覆盖了各类诉讼领域并开始发挥着愈加重要和不可替代的作用。

1. 计算机技术发展概览

计算机的英文原词“computer”最早指计算者，即具有数据计算能力的人。计算机的出现和发展大致经历了以下阶段。

人类历史上早期的计算工具主要为机械或模拟计算装置，常见的如我国古代的算盘和西方国家的机械计算尺。1801 年，法国人约瑟夫·玛丽·雅卡尔设计出一种机器，使用打孔的纸卡片来为当时的织布机编制复杂图案的程序。这种机器虽然还并非真正意义上的计算机，但是因为具备了一定的可编程性，而被认为是现代计算机发展历程中的一个里程碑。随后的计算机发展史上陆续出现了查尔斯·巴比奇、赫尔曼·何乐礼等人物，他们为推进计算机的编程思想，进行大规模自动化数据处理做出了历史性贡献。

到了 20 世纪前期，人们开发出了各种复杂的、多用途的模拟式计算机用于科学研究和其他某些专门领域。当时的计算机已经拥有较为强大的性能，在通用性方面也有显著改善，一定程度上具备了当今计算机的典型特征。1937 年，美国麻省理工学院的克劳德·香农首次在计算机技术发展领域提及数字电子技术的应用，他提出了使用开关来实现逻辑和数学运算的思路，这标志着二进制电子电路设计和应用的全新开始。1941 年出现的阿塔纳索夫 - 贝瑞计算机成为世界上首部数字电子计算机，随后英国的巨像计算机、哈佛大学的马克一号计算机、宾夕法尼亚大学的 ENIAC 计算机陆续诞生，这些计算机均基于二进制原理，使用真空管来实现编程。

在整个20 世纪50 年代，几乎由第一代真空管计算机一统天下。到1958 年，集成电路和微处理器相继问世，计算机步入第

二代。1964 年，体积更小、速度更快的晶体管计算机出现，此时集成电路开始获得广泛应用，计算机步入第三代。1972 年，基于大规模和超大规模集成电路的计算机出现，计算机步入第四代。当时 Intel 推出的 8088 处理器是第四代计算机芯片的典型代表，苹果公司则在 1976 年推出了 Apple I 计算机。

进入20 世纪 80 年代，微型计算机开始进入人们的日常办公和家庭生活领域。尤其是到了20 世纪 90 年代，多媒体技术和微软视窗操作系统问世，计算机互联网的大规模应用加速普及，电子计算机全面地进入人们的商务、政务、工作、通信、娱乐等每一个角落，人们几乎已经须臾无法离开计算机而维持正常生活。电子计算机作为人类历史上最伟大的发明之一，深刻地改变又在塑造着今天人们的生活形态，为促进人类社会发展发挥着重大的革命性作用。

2. 电子证据的出现和应用

电子证据的技术本体为电子数据，它是伴随电子信息技术的发展及其在司法领域内的应用而产生的。从广义上来说，能够证明案件事实的一切电子数据及其派生物都是电子证据。作为一类全新的证据类型，电子证据的出现和应用在全世界范围内来看也不过只有短短几十年的时间，人们对于电子证据各个方面的认识、研究和应用仍然处于相对初期的发展阶段。

伴随着以电子计算机和互联网技术为主的各项电子信息技术的深入发展和广泛应用，司法领域中各类“电子化”了的案件信息开始不断出现，在许多案件中出现的各种形式的电子数据便可能成为潜在的电子证据。电子证据是因法律和电子信息技术的结合互动而生成的新型证据，在司法领域中的作用和影响正变得愈加重要，甚至在一定程度上表征了日后诉讼证据发

展的重要方面，因而被许多学者誉为信息时代的“证据之王”。〔1〕

电子证据在自然物理特性、技术应用特性和法律适用特性等方面均与传统证据存在一定区别。第一、电子证据的生成、存储、复制和传递都要依靠电子信息技术，电子证据在技术本质上实际是电子化了的数据信息；第二，绝大部分电子数据经过处理都可以以二进制数字化信息为表现形式，即人们所熟悉的数字式计算机的信息表现形式；第三，电子证据具有传统证据的一般属性和功能，但是其法律定位、证据能力以及与其他类型证据的关系和转化等基本问题长期困扰着相关理论和实务界。在此需要提及的是，电子证据和电子数据的存在方式和技术原理是相互一致的，在不严格的情况下两者也经常出现混用，但是这两个概念之间是存在严密的区别的。〔2〕

电子证据在技术本质上依然是各种电、光、磁信号，并不能为人的感官所直接感知，只有借助各种对应的专门设备和技术，才可以使人们间接地感知、认识和研究具有各种外在表现

---

〔1〕 如中国人民大学法学院的何家弘教授就曾经指出：“从司法证明方法的历史演进看，神证、人证时代进入到物证时代是历史的进步。那么电子证据即将成为证据之王的大趋势，很可能宣告电子证据时代的来临。这将是司法证明方法的历史飞跃。”

〔2〕 就本自然段中所出现的电子数据和电子证据这两个概念，笔者认为电子数据本身是更加中性的概念，电子数据自身具有各种天然的技术性特点，是电子计算机和网络等设备运行处理的产物，当然已有的电子数据也可以作为后续运行处理的原料并生成新的电子数据。当案件中出现的电子数据对相关案件事实具有证明作用，而且又能够满足作为诉讼证据予以审查的各项要求，则可以成为进入诉讼甚至用以定案的电子证据。简单地说，电子数据是电子证据的技术本体，电子证据是用作证据的电子数据。在相关立法方面，我国2013年01月01日起实施的最新版《中华人民共和国刑事诉讼法》和《中华人民共和国民事诉讼法》已经将电子数据明确作为新的证据类型。电子数据和电子证据之间更为详尽的联系和区别可参见李学军：“电子数据与证据”，载《证据学论坛》2001年第1期，第433页。

形式的电子证据。随着技术自身的进步和应用的拓展，如今的电子证据在外在表现形式方面极为多样，其丰富程度远远超过了任何一种传统证据。从电子文档、电子邮件、电子签名、电子公告，到即时聊天、网页日志、GPS 信息，再到手机短信、网络电话和音频视频，电子证据的外在表现形式几乎无以穷尽。

电子证据在各类型的案件中均有体现，无论是专门针对互联网络和计算机，以攻击和破坏这些通信系统本身为目的的案件，还是以网络和计算机等通信设备为工具或辅助而实施的传统犯罪或其他案件，都能够留下电子证据的身影。显然，电子证据是办理此类案件的最重要角色，在其中发挥着无以替代的重大作用。同时也需要看到，电子证据在其技术属性和法律适用方面具有显著不同于传统其他诉讼证据的独特品格，其应用当中不可避免地会出现很多新情况和新问题，这需要有关理论和实务界通过持续的深入研究和实践积累来逐步应对和解决。

3. 电子证据取证和鉴定研究概况

国外计算机取证的研究和实践产生于 20 世纪中后期，在 20 世纪末期开始走上了快速发展的轨道。按照美国佛罗里达大学法证科学中心 Mark M. Pollitt 教授的报告，世界上计算机取证的发展经历了史前期（1985 年以前）、婴儿期（1985 年到 1995 年前后）、童年期（1995 年到 2005 年前后）和青春期（2005 年前后至今）四个阶段。[1] 经过前后几十年的发展，国外的计算机取证已经达到了较为成熟和完善的阶段，相关的技术产品和方法较为先进和成熟，对应不同的需求已经发展出了深入细化的

〔1〕 许榕生、杨英："国内外计算机取证发展"，载《保密科学技术》2011 年第 11 期。