电子取证的法律规制

主编/刘品新

中国法制出版社
CHINA LEGAL PUBLISHING HOUSE

电子取证的法律规制

中国法制出版社
CHINA LEGAL PUBLISHING HOUSE

图书在版编目（CIP）数据

电子取证的法律规制/刘品新主编. —北京：中国法制出版社，2010.2

ISBN 978-7-5093-1714-3

Ⅰ.①电… Ⅱ.①刘… Ⅲ.①电子技术-应用-证据-调查-研究 Ⅳ.①D915.13②D918

中国版本图书馆 CIP 数据核字（2010）第 015132 号

策划编辑　周琼妮　　封面设计　蒋怡

电子取证的法律规制

DIANZI QUZHENG DE FALU GUIZHI

主编/刘品新

经销/新华书店

印刷/河北省三河市汇鑫印务有限公司

开本/880×1230 毫米 32　　印张/13　字数/228 千

版次/2010 年 2 月第 1 版　　2010 年 2 月第 1 次印刷

中国法制出版社出版

书号 ISBN 978-7-5093-1714-3　　定价：32.00 元

北京西单横二条 2 号　邮政编码 100031　　传真：66031119

网址：http://www.zgfzs.com　　**编辑部电话：66067023**

市场营销部电话：66033393　　**邮购部电话：66033288**

前　言

“不是我不明白，是这个世界变化太快!”在人类大步迈向信息社会的今天，这句流行语几乎成为了各行各业的真实写照。法学研究如此，立法、司法领域亦然。

上个世纪90年代中期，大约还是在我本科毕业前夕，中国获准加入国际互联网。随后的一年内，全国范围的公用计算机互联网络开始提供服务。自此，普通国人开始了一种新的生存方式，中国快速进入互联网时代。那个时候，很少有人能够预测到司法领域会遭遇来自网络信息技术的巨大冲击。像很多年轻人一样，我只是在憧憬何时能够拥有一台神奇的个人台式机。这一愿望到硕士研究生毕业的1998年变成现实，我付出的代价是咬咬牙花光了所有的积蓄。

过去拥有个人微机的日子是非常愉悦的。打打文字，玩玩游戏，一天一天就这样不知不觉地过去了。由于那时我的主修专业是侦查学，我很快发现了电脑的一个特别价值，那就是它可以充当“计算机犯罪侦查”研究的得力助手。现在回想起来，当时我写的很多稚嫩的文字（诸如“高科技滋生的病毒”、“计算机盗窃犯罪揭秘”、“网络黄潮”、“‘黑客’与‘跨客’”等等）之所以能够印成铅字发表，在很大程度上得益于我的“老式奔Ⅲ兄弟”。

时光荏苒，岁月如梭，计算机及网络技术在中国的发展真是日新月异。从门户网站到专业网站，从电子邮件到电子公告板，从网络聊天到网络电话，从博客到播客，从电子商务到电子政务，从网络安全到个人信息保护，从自动搜索到人肉搜索……形形色色的新事物层出不穷，让人眼花缭乱。这十多年来的网络发展史，就是各种新概念与新理念粉墨登场的历史。从现实与趋势来看，网络对人类生活的深远影响远未结束！

或许囿于专业的局限，我一度关注网络信息技术引发的新的取证手段——电子证据鉴定。早期的时候，从英美法系国家传来一组新的词汇“Computer Forensics”、“Cyber Forensics”以及“Digital Forensics”等，我最初以为它们就是直译的“计算机法（庭）科学”，即电子证据鉴定之意。事实证明，这属于一个表面化的误判，它们的外延远远超出专家开展的电子证据鉴定，而是涵盖各种各样的利用计算机或网络的取证措施。这就是如今我更愿意将此类取证措施统称为“电子取证”（或“计算机取证”）的个中讲究。

2005年伊始，我有幸应邀参加了国内几次“计算机取证技术峰会”，并成为中国电子学会计算机取证专家委员会的委员。这样，我就有了同国内外电子取证专家面对面交流的宝贵机会。在同他们的交谈中，我意识到包括计算机搜查、电子证据鉴定、电子证据保全在内的各种电子取证措施都将面临一个接受法律约束

的问题，有感而发，我申请了教育部的人文社会科学研究项目——“计算机取证的法律规制”，并顺利获准。

此后，我和我的团队便致力于该项目的交叉研究，我本人还以此项目获得国家留学基金委员会的资助，赴美国访学一年。我和团队成员一直努力做到治学勤勉，期望在“计算机取证的法律规制”方面有所建树。然而说实话，我们时常感觉到自己的研究落后于电子取证技术、案例乃至法律的发展。往往是我们对一些存在的现象或问题尚未形成成熟的认识时，新的此类现象或问题又接踵而至了。

像“杜宝良现象”、“周正龙拍虎”、“香港艳照门”、“手机实名制”、“铜须门”以及公安机关发动的几次网上专项斗争，都促使我面对现实加以思考，写出了诸如《电子警察执法：谨防走入误区》、《手机实名制的价值平衡》等几篇应景之作。

最为特别的是，2006 年岁末我还被动地体验了一把“人肉搜索”：一个取名“建行的草莓”的网友在海南三亚旅游时拾到一部数码相机，将相机中部分照片发送到新华网论坛上，发动网友寻找失主。短短几天内，南北网友纷纷跟帖或以其他方式提供线索，顺利物归原主……热情的网友们接力上演了一幕寒冷冬天的温暖故事。正是由于较早地体验这件事，我能够客观地评断“人肉搜索”的利与弊，能够自信地展望“人肉搜索”的更迅猛发展（参见拙文《“网络通缉/通报”的法律规制》）。这两年的情势已

经验证了这一论断。是啊，“不求最好，但求最肉！”这怎么成为了时下社会的最高追求目标之一？

其实，我在电子取证研究或实务方面的“被动”经历绝不限于此。像去年我申报的最高人民检察院检察理论课题“电子证据收集和运用问题研究”，是受朋友的鼓动；像今年我申请中国人民大学物证技术鉴定中心增设“电子证据鉴定”业务，则是受跨国公司的推动……电子取证显然是一个朝气蓬勃的领域，身在其中者不向前行断然不行。

俗话说，没有规矩，不成方圆。实践中已然涌现了大量的电子取证行为，国家不从法律制度上规范显然是不行的。我们注意到，一些发达国家陆续颁行了各种专门性的电子证据规则或手册，我国公安部和最高人民检察院也在创设有关的电子证据鉴定规则、计算机现场勘查规则。在研究此类规则和参与规则制定的过程中，我们深刻意识到，国内在这一方面的艰巨工作只是开了个头，未来还有相当长的一段路要走。这正是我们努力推出本作品的意义所在。

最后，我还要将团队同仁在课题结项时领悟到的两个新观点，提早以简明的语言奉献给大家（法学领域写成宏篇大论常常费时而低效）：

——电子取证的提出不仅意味着一切传统取证措施的电子化，也意味着一些全新的取证措施的出现；

——电子取证的形式多样，但基于其在技术方面日渐趋同，因此在法律规制方面也呈现出趋同的规律。

是为余论，仅供品评之用。

刘品新

2009 年 11 月 11 日

目　录

前　言 …… (1)

第一章　导论 …… (1)

一、引言 …… (1)

二、电子取证的含义 …… (2)

三、电子取证的基本程序 …… (6)

四、电子取证的法律挑战与因应 …… (10)

五、小结 …… (26)

第二章　计算机搜查 …… (27)

一、引言 …… (27)

二、计算机搜查的含义 …… (28)

三、计算机搜查的程序 …… (32)

四、计算机搜查的法律挑战与因应 …… (35)

五、小结 …… (49)

第三章　计算机现场勘验 …… (51)

一、引言 …… (51)

二、计算机现场及现场勘验的含义 …… (52)

三、计算机现场勘验的程序 …… (55)

四、计算机现场勘验的法律挑战与因应 …… (71)

五、小结 …… (85)

第四章　电子证据鉴定 …… (87)
一、引言 …… (87)
二、电子证据鉴定的含义 …… (88)
三、电子证据鉴定的程序 …… (100)
四、电子证据鉴定的法律挑战与因应 …… (114)
五、小结 …… (139)
第五章　网络监控 …… (141)
一、引言 …… (141)
二、网络监控的含义 …… (143)
三、网络监控的程序 …… (146)
四、网络监控的法律挑战与因应 …… (152)
五、小结 …… (166)
第六章　网络过滤 …… (168)
一、引言 …… (168)
二、网络过滤的含义 …… (174)
三、网络过滤的程序 …… (182)
四、网络过滤的法律挑战与因应 …… (190)
五、小结 …… (203)
第七章　网络通缉 …… (205)
一、引言 …… (205)
二、网络通缉的含义 …… (206)
三、网络通缉的程序 …… (209)

四、网络通缉的法律挑战与因应 …… (218)
五、小结 …… (222)
第八章 网络搜索 …… (224)
一、引言 …… (224)
二、网络搜索的含义与功能 …… (226)
三、网络搜索的法律问题及程序规制 …… (232)
四、侦查机关网络侦查的基础工作建设 …… (241)
五、小结 …… (243)
第九章 网络侦查陷阱 …… (245)
一、引言 …… (245)
二、网络侦查陷阱的含义 …… (249)
三、网络侦查陷阱的侦查价值 …… (256)
四、网络侦查陷阱的程序 …… (259)
五、网络侦查陷阱的法律挑战与因应 …… (266)
六、小结 …… (270)
第十章 网络公证 …… (271)
一、引言 …… (271)
二、网络公证的含义 …… (273)
三、网络公证的程序 …… (278)
四、网络公证的法律挑战与因应 …… (284)
五、小结 …… (295)
第十一章 电子证据保全 …… (297)

一、引言 …… (297)
二、电子证据保全的含义 …… (298)
三、电子证据保全的程序 …… (304)
四、电子证据保全的法律挑战与因应 …… (341)
五、小结 …… (359)

附录：《中华人民共和国电子取证规则》
（学者建议稿） …… (360)

后记 …… (402)

第一章

导 论

一、引言

马家爵杀人案是一起引发国人广泛关注的名案。作案人的作案手段是传统类型的，而警方开展缉捕却依赖了新式的电子取证。其破案情节往往为人们所忽略。

2004年2月23日下午1时20分，昆明市公安局接报，称在云南大学学生公寓宿舍内发现一具男性尸体。经现场勘查和访问，在该宿舍柜子内共发现4具被钝器击打致死的男性尸体，同宿舍的学生马家爵却失踪了。昆明一家银行的录像资料显示，马曾于2月15日下午持其中两名死者的存折到银行取走了4000元钱。种种迹象表明，马有重大犯罪嫌疑。当地公安机关迅速成立了“2·23”专案组开展工作，当日即通过公安部向全国发出通缉令，重金悬赏通缉马家爵。与此同时，调查专家使用专业技术手段，对马在宿舍内使用过的电脑进行硬盘数据分析，发现他出逃前对硬盘进行过格式化，但硬盘中存储的信息仍被恢复了出来。这些电子数据表明，他在出逃前三天基本上都在搜集有关海南省的信息，尤其是有关三亚市旅游、交通和房地产的信息。根

据这一线索，警方调整了通缉重点，很快于3月15日在三亚市将马缉拿归案。①

显而易见，电子取证在本次抓捕中起到了非常重要的作用。这并不是孤立的个案，电子取证在当今的司法实践中大展身手早已是不争的现实。无论是在打击网络色情、网络诈骗、网络赌博等高科技犯罪案件的活动中，还是在调查杀人、爆炸、恐怖等传统犯罪案件的过程中，电子取证已悄然成为一种出奇制胜的必要手段。当然，电子取证也遭遇到了一些法律方面的障碍，所获取的材料往往多用作办案线索而非定案证据。那么，人们究竟应该如何客观认识电子取证这一新生事物？法律又应该如何规制这一取证手段？要回答这些问题，不妨从电子取证的基本含义谈起。

二、电子取证的含义

电子取证是伴随着信息技术的飞速发展而出现的一个新事物。迄今为止，人们依然众说纷纭，尚不存在大一统的概念。从英文表达来看，主要用语有“E-discovery”和“Computer Forensics”之别。前者又称为“Electronic Evidence Discovery”，是指对

① 参见关非：《小荷才露尖尖角——国内计算机取证技术市场面面观》，载《信息网络安全》2005年第9期。

电子文件或电子数据的获取;[①] 后者又称为“Cyber Forensics”、“Digital Forensics”，是指对以比特形式存储或传递的数据加以恢复、保存、检查的各种工具或技术。[②] 它们之间的区别主要在于由谁具体负责取证工作，前者往往是诉讼各方当事人及其律师，后者则限定为特别聘请或委派的计算机专家（包括一些专业公司的技术人员）。从中文表述来看，电子取证、计算机取证、电子证据的收集等术语也常常被混用。其实，它们的含义是在“大同”的前提下存在“小异”，并没有严格区分的必要。

关于什么是电子取证，我国学术界亦存在广狭义两种观点。狭义说将电子取证与“Computer Forensics”等同起来。例如，有人认为，电子取证是“将计算机系统视为犯罪现场，运用先进的技术工具，按照规程全面检查计算机系统，提取、保护并分析与计算机犯罪相关的证据，以期据此发起诉讼”。[③] 取证的主要过程包括保护和勘查现场、获取物理数据、分析数据、追踪源头、提交结果等。也有人认为，电子取证“也称计算机法医学，它是指运用计算机辨析技术，对计算机犯罪行为进行分析以确认罪犯及计算机证据，并据此提起诉讼。也就是针对计算机入侵与犯罪，

---

① Hon. Shira A. Scheindlin & Jeffrey Rabkin, “Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?”, 41 Boston College Law Review (2000), p. 333.

② Erin Kenneally, “Computer Forensics”, 27 Magazine of Usenix & Sage (2002), p. 8.

③ 王彩玲、陈贺明：《浅析计算机犯罪取证与反取证》，载《吉林公安高等专科学校学报》2007年第2期。

进行证据获取、保存、分析和出示。”① 还有人认为，电子取证就是“运用软件技术和工具，按照预定的步骤检查计算机系统和相关外部设备，保护、提取和分析计算机系统和相关外部设备，保护、提取和分析计算机犯罪的痕迹，并产生具有法律效力的电子证据的过程”。②

广义说则认为电子取证包括但不限于特殊的技术手段。例如，有人认为，电子取证是指对能够为法庭接受的、足够可靠和有说服性的，存在于计算机和相关外设中的电子证据的确认、保护、提取和归档的过程。③ 还有人认为，所谓电子取证是指对存储在计算机系统或网络设备中潜在电子证据的识别、收集、保护、检查、分析以及法庭出示的过程。电子取证不单单是计算机或网络的技术问题，还涉及法律和道德规范。④

我们赞同广义说。虽然电子证据是带有一定高科技色彩的新型证据，但从司法实践来看，获取电子证据并不限于技术手段，也不限于专家提取，普通的当事人完全可以利用一般经验予以事先保全或事后收集。换言之，专家在电子取证方面虽然作用巨大，但并不能掩盖普通当事人在电子取证方面的特殊作用。特别

---

① 张斌、李辉：《计算机取证有效打击计算机犯罪》，载《网络安全技术与应用》2004 年第 7 期。

② 苏成：《计算机取证与反取证的较量》，载《计算机安全》2006 年第 1 期。

③ 王玲、钱华林：《计算机取证技术及其发展趋势》，载《软件学报》2003 年第 9 期。

④ 赵小敏、陈庆章：《计算机取证的研究现状及趋势》，载《网络安全技术与应用》2003 年第 9 期。

是从制度建设的角度来看，构建一个国家的电子取证制度绝不应忽略普通人的作为。

准确把握电子取证的概念，还需要注意以下几点：其一，取证手段是借助计算机等电子设备；其二，取证对象主要是处于虚拟空间的电子证据；其三，取证主体呈现多元化的特点，即实施电子取证的人不能局限于某些特殊的群体。无论是侦查人员、司法人员、行政执法人员、诉讼各方当事人及其律师，还是网络服务提供商、民间技术专家等，都有可能在电子取证领域一试身手。

随着国内外司法实践的日新月异，如今电子取证已经发展为一个庞杂的取证手段群。以证据来源为标准，它可分为单机取证、网络取证与相关设备取证；以取证时刻潜在证据的特性为标准，它可分为静态取证与动态取证;[①] 以取证时间为标准，它可分为事后取证与事前取证；以调查人员是否需要亲临证据现场为标准，它可分为临场取证与远程取证;[②] 以技术手段为标准，它可分为数据获取、数据恢复、数据分析与数据鉴定等；从诉讼措施的角度为标准，它可分为计算机搜查、计算机现场勘验、电子

① 静态取证所收集的是存储在未运行的计算机系统、未使用的存储器或独立的磁盘、光盘等媒介上的静态数据，这些数据不会随着计算机电源的切断而消失；动态取证所收集的是切断计算机电源后就会消失的各类易失性数据，如计算机当时运行的进程信息、内存数据、网络状态信息、网络数据包、屏幕截图和交换文件拷贝等等。

② 远程取证是指通过远程连接的方式，从正在运行的计算机系统中获取电子证据的方式。