电子证据认知新思路

基于实验的直观体现方式

New Ideas of Electronic
Evidence Cognition:

Based on the Intuitive Experience of the Experiment

方玉珍 / 著

制出版社
PUBLISHING HOUSE

电子证据认知新思路

基于实验的直观体现方式

New Ideas of Electronic Evidence Cognition:

Based on the Intuitive Experience of the Experiment

方玉珍 / 著

中国法制出版社
CHINA LEGAL PUBLISHING HOUSE

图书在版编目 (CIP) 数据

电子证据认知新思路：基于实验的直观体现方式 / 方玉珍著. —北京：中国法制出版社，2019.1

ISBN 978-7-5093-9965-1

Ⅰ. ①电… Ⅱ. ①方… Ⅲ. ①电子—证据—研究 Ⅳ. ① D915.130.4

中国版本图书馆 CIP 数据核字（2019）第 016014 号

策划编辑：马 颖

责任编辑：王雯汀 封面设计：杨泽江

电子证据认知新思路：基于实验的直观体现方式

DIANZI ZHENGJU RENZHI XINSILU：JIYU SHIYAN DE ZHIGUAN TIXIAN FANGSHI

著者 / 方玉珍

经销 / 新华书店

印刷 / 北京京华虎彩印刷有限公司

开本 / 880 毫米 ×1230 毫米 32 开 印张 / 8.75 字数 / 186 千

版次 / 2019 年 1 月第 1 版 2019 年 1 月第 1 次印刷

中国法制出版社出版

书号 ISBN 978-7-5093-9965-1 定价：39.00 元

北京西单横二条 2 号 邮政编码 100031 传真：010-66031119

网址：http://www.zgfzs.com 编辑部电话：010-66060794

市场营销部电话：010-66033393 邮购部电话：010-66033288

（如有印装质量问题，请与本社印务部联系调换。电话：010-66032926）

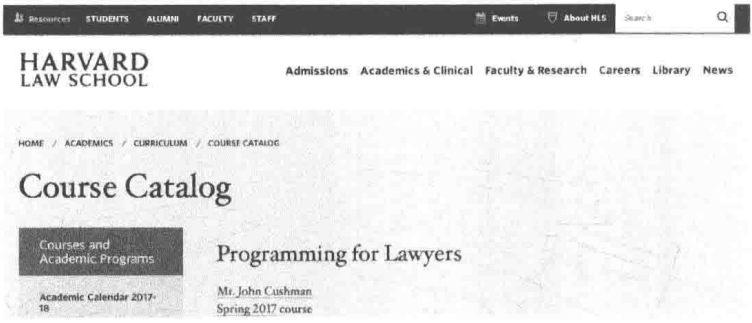
一、概述

有些人以为，电子证据离自己很远，基本上无须触碰，殊不知，电子证据与我们的日常生活息息相关，并且随着大数据、物联网的普及，它更加深入到了我们生活以及法律关系的每个角落。曾经某一个案件用了QQ聊天记录作为证据时还是新闻，但现在已成为稀松平常的事情。今天，电子证据不仅是线索发现、心理分析与情报挖掘的重要来源，更是独立的证据。

不知不觉中，我们已身处电子证据时代，法律人甚至是普通人都不得不直面，谁也不能置身事外。如同信息素养的养成，法律人甚至是普通人也需要养成电子证据知识素养，即需要对电子证据具备基本的认知能力，了解一些身边的电子证据知识。

哈佛大学法学院已将编程入门课纳入教学大纲，甚至将其列为知识产权法、科技法等方向的必修课程。[①]

① https://hls.harvard.edu/academics/curriculum/catalog/default.aspx?o=71516，最后访问时间：2017年11月5日。



也如同法科学生在通过司法考试之余，有的学生会去考注册会计师、考专利代理人、考雅思托福等一样，虽然目前还没有见到将电子证据认知纳入优先考虑的条件，但笔者认为这只是时机还未到而已。

其实，合格的法律人甚至是普通人都应当是终身学习者，普通人甚至是法律人对电子证据的认知并不需要达到鉴定人的程度，只需要具备一定的认知能力或者提取能力即可。但是说到认知电子证据，很多人都会觉得比较枯燥乏味，学习起来非常吃力或者觉得电子证据非常神秘、威严、崇高。所以，为了让法律人甚至是普通人“读懂”电子证据，进而举一反三地加以应用，笔者认为电子证据认知需要新思路，且认为基于直观、有趣体验的实验方法是电子证据认知的重要方法。

任何一项课题的研究都要依据一定的方法来进行，实验研究法就是其中一种重要的方法。有趣的实验就像一粒粒“催化剂”，能迅速激发读者（学习者）的探究兴趣与热情；直观、简化的实验就像一颗颗“速效丸”，“剂量小”但“威力大”，与其他方法相比更能够令人信服地估计因果关系，且成本低廉。

本书主要分基础篇和实验篇。

二、基础篇

在基础篇中，笔者提出在电子证据时代，电子证据既是线索发现、心理分析与情报挖掘的重要来源，同时更是独立的电子证据。但是在司法实践中，却存在法官对电子证据的认识不统一影响法律的确定性、电子证据不可靠的传统观念禁锢着人们的行为、普通当事人亲身提取电子证据的需求与现实存在矛盾等问题，笔者对这些问题进行了分析，认为造成这些问题的根本原因是人们——尤其是法律人与普通人对电子证据的产生与运行机制的认知不够，需要加深认识。

对电子证据的研究一直就有，但是大多处于语言文字描述的层面，或者是晦涩难懂，或者是不带问题的截图说明，无法引发人们的思考。笔者认为法律人或普通人对电子证据的认知是一种跨界学习过程，需要新思路，需要注意方法与技巧，比如最好直观有趣，如此才能引发“外行”持续学习的热情；比如要注重认知电子证据现象背后的本质，如此才能令“外行”灵活运用，举一反三；再如最好可以复用与重现，进而坚定其内心对电子证据的信心；等等。笔者认为无须千言万语，且看如下示例便可理解。

例如，在讲述数据恢复背后的原理时，如果面对的是计算机专业的读者，可以如此介绍：对于 FAT 文件系统，硬盘上的数据按照其不同的特点和作用大致分为 5 部分：MBR 区、DBR 区、FAT 区、DIR 区和 DATA 区。其中，MBR 由分区软件创建，而 DBR 区、FAT

区、DIR 区和 DATA 区由高级格式化程序创建。文件系统写入数据时只是改写相应的 FAT 区。而对于 NTFS 文件系统，也有 MBR 区和 DBR 区，其作用与 FAT 文件系统大致相同，与 FAT 文件系统的不同之处在于 NTFS 中有一个被称为主文件表（MFT）的文件，用于记录每个文件的目录信息。MBR 即主引导记录区，位于整个硬盘的 0 磁道 0 柱面 1 扇区。在总共 512 字节的主引导扇区中，MBR 的引导程序占其中的前 446 个字节，随后的 64 个字节为 DPT（硬盘分区表），包含四个分区信息，每个分区占 16 个字节，最后的两个字节“55 AA”是分区结束标志。

硬盘主引导扇区由 5 个部分组成：

1.0000H~008AH 的 139 字节的引导程序部分；

2.008BH~00D9H 的 79 字节的错误信息数据区；

3.00DAH~01BDH 的 228 个全 0 字节；

4.01BEH~01FDH 的 64 个字节，是硬盘的四个分区表信息；

5.01FEH~01FFH 的 2 个字节“55 AA”，是硬盘主引导扇区结束（有效）标志。

……

如果面对的是法科读者，上述数据恢复背后的技术原理便如同天书一样了，法科读者即使费力费时地理解了，他们也记不牢，且没有实际意义。

而实验则正好满足这些要求，实验直观有趣，通过可重复的实验模拟可以用来感受隐蔽的电子证据规律，这些是再严谨翔实的文字也不足以道明的感受等。于是笔者提出基于实验直观体验的电子

证据认知新思路，并从电子证据实验第一例、何谓电子证据、如何进行电子证据实验等方面进行相关论证。

三、实验篇

接下来笔者在实验篇中尝试解决于基础篇中提及的问题。

（一）实验篇的设计目标

首先，通过再认识电子证据重塑人们心中的观念，笔者主要尝试通过对电子证据系统性及其伪造篡改的可追踪性实验及相关阐述来改变人们心目中电子证据不可靠的传统观念。

其次，按照电子证据广义工作流程的顺序进行分别阐述，主要包括对电子证据取证准备、电子证据的提取与保全、电子证据的分析、电子证据的举证与质证、电子证据的认证等环节的重要问题或争议问题进行实验认知与相关讨论，希望法律人甚至是普通人能够看“懂”这些电子证据知识、能够成功“操作”这些电子证据实验的同时还能够有所思考。

（二）实验篇的框架结构说明

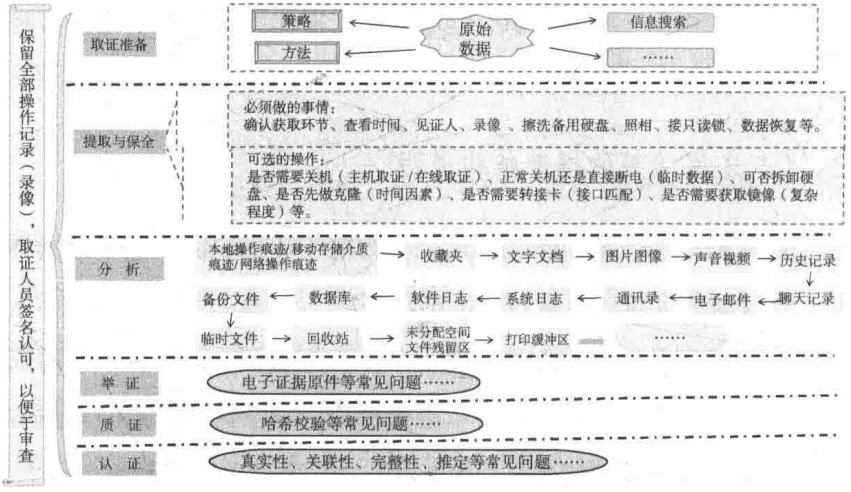
广义的电子证据工作流程可以分为电子证据取证、电子证据举证、电子证据质证、认证四个大的环节。

其中取证是指调查人员为揭示案件真相或证明事实主张，而依法展开的收集提取证据、初步审查分析证据以及保全证据的专门活动。取证是司法证明的第一步。

司法证明的取证主体是各种调查人员。例如，审判人员、公诉人员、侦查人员、行政执法人员、纪检监察人员、公证人员、仲裁人员、律师与各类案件的当事人等。

司法取证的方法纷繁复杂，既包括法律法规明文规定的各种措施或手段，如询问、讯问、辨认、搜查、勘验、检查、调查实验、鉴定以及保全方法，还包括法律法规未作规定的但实际上广泛采用的措施和手段。

另外，由于电子证据取证环节的内容较为广泛，所以笔者对其进行了细分，细分后，电子证据工作流程可以分为电子证据取证准备、电子证据的提取与保全、电子证据的分析、电子证据举证、电子证据质证、电子证据认证这六个重要环节，如下图所示。每个阶段所处的环境和面对的对象皆有所不同：取证准备阶段；电子证据的提取与保全阶段；电子证据分析阶段；电子证据举证阶段、电子证据质证阶段、电子证据认证阶段。



需要注意的是，电子证据虽然已经具有独立的法律地位，但是由于其蕴含着“技术”特性，为了获得法庭的认可，电子证据取证，也即电子证据的取证准备、提取、保全与分析过程需要遵循相关的程序规范。也就是说在电子证据的获取、实验室分析等取证过程中应当最大限度地确保电子证据的完整性和前后连贯性，其中的任意一个环节、过程都要处于一个完整、可信的证据监督链中，如此才能减少电子证据举证、质证、认证过程中的争议。

实验篇根据细分后的电子证据工作的六个环节分别切入，分六个章节进行了实验认知，各个章节阐述的内容要点如下。

1. 电子证据的观念重塑章节说明

电子证据时代，电子证据不可靠的传统观念禁锢了人们的思想与行为，已经不合时宜，需要重塑，为了突出这一点，同时也为了强调电子证据的系统稳定性，笔者特意将观念重塑设立为独立的章节。

当然，电子证据的观念是宏观层面的内容，在其他所有章节都会有所体现，并非某一章所独有的。

2. 电子证据的取证准备章节说明

在取证准备阶段，需要客观分析取证对象了解案件信息，制定取证策略、计划和目标；确定取证人员，选择和准备合适的取证工具；了解电子证据存储环境并做好收集、提取电子证据的各项准备，做好电子证据分析的环境准备。在某些特殊环境下，还需要获得法律授权，准备好相关法律手续。

详言之，需要了解案件类型、案件背景等案件信息，并通过信息搜索等方式搜索案件嫌疑人相关信息；需要做好人员准备工作，

此处的人员可能包括现场勘查人员、安保人员、协助人员、第三方证人等；需要了解证据的存储环境，计算机系统的种类、数量、容量、网络结构等信息，准备好证据提取工具、证据存储对象和封条标签等。结合案情，准备相应的“人”与“物”。

该章，笔者主要通过实验认识取证准备中的信息搜索等相关问题，有网络信息搜索实验、本地计算机信息搜索实验，以及最佳计算机搜查实验。

3. 电子证据的提取与保全章节说明

电子证据产生后必定被存储于某介质上，如计算机磁盘、U 盘等，需采用一定工具及时进行提取与保全。

电子证据的提取保全阶段，需要先收集，并通过硬件克隆或软件镜像方法提取介质上的所有数据（通常以文件或者文件包的形式存储于载体上），即逐比特的克隆和镜像现存的正常文件、隐藏文件、加密文件、日志文件、临时文件、历史记录，以及已被删除的但通过技术可恢复的文件残留区、未分配空间、交换空间等，该克隆和镜像完整记录了磁盘上的所有信息，然后再封存载体或介质。

在收集和提取数据的过程中需要计算哈希值，获得电子证据“指纹”。电子证据被提取后，需要尽可能地将所有文件包括恢复后的被删文件用安全、纯净、无毒的载体存放，有条件的还需对其进行封盘刻录备份，从而保证备份文件与原始文件的一致性。下一步即可在不污染原始介质的情况下做后续的证据分析工作。证据分析阶段的工作是在确保证据文件不被破坏的前提下对获取的存储设备进行深入检查，发现可能的电子证据并生成报告，以便提交给法庭

作为诉讼证据。

实践中，电子证据的提取主要分为现场提取、远程提取和移动端提取。

（1）现场提取

对于刑事案件来说，现场提取即现场勘验。现场勘验是指在案发现场实施勘验，以提取、固定现场存留的与犯罪有关的电子证据和其他相关证据，现场勘验应由县级以上公安机关相关部门负责组织实施，必要时可以指派或聘请具有专门知识的人参加。现场勘验过程可以依次细分为以下环节。

1）控制现场环节

控制现场环节需要遵循两个基本原则：①保障人身安全：防止现场勘查过程中因被调查人不配合产生冲突，或其他可能造成人身伤害的情形；②保障设备安全：防止现场勘查过程中直接或间接地破坏证物或设备。

控制现场环节需要注意的事项：针对高楼，要防止对象抛弃计算机存储介质到窗外。楼层相对较低时，需要避免对象跳窗逃窜的可能性；特别需要注意防止出现因破门时间长，现场遭到嫌疑人损毁、对象被烧毁等现象。另外需要阻止正在破坏的行为，如果发现硬盘正在格式化、碎纸机正在工作的情况应立刻停止或切断该设备的电源，如果打印机正在打印，应该让其继续打印。

2）现场拍照环节

到达现场时，首先需要按照整体到局部的规则拍照，另外在对现场展开调查前，应通过拍照、录像等方式记录下当时的状态，如

设备的位置、连接状态、显示器屏幕信息等。

3）收集相关证物环节

在此环节中，需要识别和收集可能的物理证据或物理介质，如嫌疑人的计算机、移动硬盘、U 盘、手机、数码相机、数字存储卡、各种连接线等可能包含证据的介质，注意此环节不仅需要收集有存储功能的设备，还需要收集一些外部设备、相关的纸质材料和文件，搜查要全面，避免遗漏重要物证，对待现场的存储设备要像对待尸体一样慎重，因此需要具备一定的经验和灵敏度。

4）处理计算机环节

处理计算机的总体原则：如果计算机处于开机状态，别立即关机；如果计算机处于关机状态，那么别立即启动它的系统。

现场处于开机状态的计算机，需要收集、固定内存信息等易失性数据，这对于取证当前进程信息、网络信息、用户账户和密码相当关键。很多操作系统、商业或开源的取证工具都有获取内存镜像的功能。

提取与固定现场内存易失数据的大致流程如下：①退出垃圾清理类软件；②禁用屏保及电源休眠；③通过与国家授时中心标准时间做对比进行时间核准且固定；④提取和固定剪切板数据；⑤提取和固定内存易失数据；⑥提取和固定桌面信息。如果桌面信息是文档类的文件可以通过另存为方式提取固定，否则可以通过拍照录像等方式提取固定；⑦应用程序数据固定，特别是对在线 QQ 等即时通信记录、即时通信信息进行提取和固定；⑧加密磁盘的检查与固定，尤其需要注意对 EFS 加密文件的提取和固定；⑨关闭机器。

如果此环节的计算机系统处于关机状态，那么需要提取时间信息，并且需要在拔掉硬盘数据线和硬盘的电源线的基础上进入BIOS记录机器当前时间。

5）介质复制环节

通过硬盘复制机进行位对位的复制，或者通过软件制作源盘镜像，并且推荐每个源盘做两个以上的证据副本。注意目标对象硬盘必须为擦除过的“干净”的空硬盘。

6）填写相关清单环节

主要填写现场勘验记录、勘验检查照片信息、固定电子证据清单、封存电子证据清单、现场勘验记录签名等相关表格。

7）封存证物，并专人运输专人保管证物环节

根据《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》，能够扣押电子数据原始存储介质的，应当扣押、封存原始存储介质，并制作笔录，记录原始存储介质的封存状态。无法扣押原始存储介质的，可以提取电子数据，但应当在笔录中注明不能扣押原始存储介质的原因、原始存储介质的存放地点或者电子数据的来源等情况，并计算电子数据的完整性校验值。由于客观原因无法或者不宜扣押原始介质和提取电子数据的，可以采取打印、拍照或者录像等方式固定相关证据，并在笔录中说明原因。

收集、提取电子数据，应当制作笔录，记录案由、对象、内容、收集、提取电子数据的时间、地点、方法、过程，并附电子数据清单，注明类别、文件格式、完整性校验值等，由侦查人员、电子数据持有人（提供人）签名或者盖章；电子数据持有人（提供人）无

法签名或者拒绝签名的，应当在笔录中注明，由见证人签名或者盖章。有条件的，应当对相关活动进行录像。

封存证物的总体原则：保证封条位置正确，不破坏封条则无法使用设备。需要将可移动介质标上标签，装入防静电袋，封口处贴封条；证物须贴标签，注明提取时间、人员姓名以及设备的名称、型号等信息。

另外，需要注意收集和提取的原始存储介质或者电子数据，应当以封存状态随案移送。

（2）远程提取

远程提取是指通过网络对远程目标系统实施勘验，以提取、固定远程目标系统的状态和存留的电子证据。

远程提取的对象主要包括远程服务器、网站页面内容、邮箱内容等。远程勘验的一个重要前提是需要已知对象的账号和密码。

远程提取的常见方法有：1）在线提取，如下载转储；2）通过PicPick软件或HyperSnap软件或键盘PrtSc键进行截屏；3）通过Camtasia或Snagit或屏幕录像专家或Screen2EXE进行录像。

远程提取的主要步骤包括：1）录屏软件全程开启；2）通过国家授时中心，记录勘验开始并截图；3）跟踪站点路由信息，查看本地与站点如何建立连接，并截图；4）清除本机相关缓存信息，并截图；5）通过已知的账号密码登录目标站点，并对首页进行截图；6）提取相关的电子数据：截图重要页面；数据库和表格；系统运行进程信息；交易清单列表等。如果调查的是邮件，那么将其导出为标准eml邮件格式后截图，并检查确认其在本地邮件客户端能正常访问；7）计

算出所有截图、导出的文件、录制的全程视频文件的校验值并存档；8）将所有相关文件和值均存放到“干净”的目标硬盘。

（3）移动端数据提取

Android、iOS 等移动智能终端操作系统为用户提供了一个安全的操作系统环境，同时也限制了用户权限，使其无法访问文件系统的某些区域。为了能完整提取设备存储的镜像，一般需要在取证中获取 ROOT 权限。对 Android 设备的 ROOT 或对 iOS 的越狱（Jailbreak）是获取管理员权限的手段，然而 ROOT 或越狱会对检材造成少量数据更改，因此必须谨慎小心。

在智能终端证据提取中，破解和绕过锁屏密码是获取访问权限的关键。iOS4 及以下设备，已有较为成熟的技术暴力破解简单密码，之后的 iOS 设备已难以被破解。

Android 设备的锁屏密码绕过相对简单一些，不少 Android 设备都可以通过进入 Recovery 模式来绕过锁屏密码。对于无法获取访问权限或遭受损坏的智能终端设备，可通过芯片级的数据提取技术来获取电子证据。Android 设备提供了硬件 JTAG “调试接口”获取设备存储芯片中的物理数据。然而在设备被全盘加密的情况下，还需要破解出密钥，这些技术仍然是安全研究中的开放问题，没有成熟的方案。

电子证据的提取与保全过程涉及的内容其实非常广博与繁杂；提取与保全的方法是每个普通当事人都较为关心的；提取与保全的合法性、完整性、无损性更是法律人需要考量的。由于受限于积累的素材，笔者仅对最近较为关注的问题进行了实验研究，如存储介

质的“清洁性”研究，电子证据法律规范的技术化趋势等。

4. 电子证据的实验室分析章节说明

电子证据分析是对已扣押、封存、固定的电子证据的副本进行检验，以发现和提取与案件相关的线索和证据。

在对电子证据进行审查分析前，若未获取到电子数据存储介质副本，应当对电子数据存储介质拆封过程进行录像，并将电子数据存储介质通过写保护设备接入检查设备进行检查；有设备条件的，应当制作电子数据备份，对备份进行检查；无法使用写保护设备且无法制作备份的，应当注明原因，并对相关活动进行录像。

对原始介质克隆或镜像获得的原始介质的副本包含了原始介质上的所有可见和不可见数据，其中大部分数据是与案件事实无关的，必须综合分析并区分有关数据和无关数据。目前，电子数据所依赖的介质的存储空间越来越大，要在海量的数据中找到与案件事实相关的证据实则困难，因此必须根据案件类型，确定重点关注的点，之后采用一定的分析技术对关注点进行审查分析。电子证据的分析阶段是电子证据取证流程中最核心最重要的阶段，涉及的技术非常广。主要采用的有对比分析与关键字查询技术、文件类型签名分析技术、各类解密技术、IP 地址追踪技术、浏览器浏览痕迹分析技术、操作痕迹分析技术、移动存储介质使用痕迹分析技术、日志分析技术、电子邮件追踪技术等。

简言之，最佳电子证据的审查与分析过程即对获取的数据副本进行分析处理，搜索、提取与案件相关联、能够证明犯罪事实的数据。