第 5 章

电子数据取证

5.1

电子数据取证概述

2004年2月23日下午1时左右,昆明市公安局接到报案称,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,而同宿舍学生马加爵失踪了。通过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。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,重金悬赏通缉马加爵。公安部技术专家对马在宿舍内使用过的电脑进行分析,发现他出逃前曾对硬盘进行过格式化,专家对硬盘进行了电子数据恢复,发现马加爵在案发前后曾经大量浏览海南的旅游、出租屋、房地产以及交通等信息,其中尤为关心三亚地区。针对这些情况公安部门立刻制定了周密的抓捕预案,最终于3月15日在三亚市将马缉拿归案。此案的成功破获,电子数据取证技术为公安机关提供了准确而详细的情报,起到了至关重要的作用。

时至今日,随着人工智能、虚拟现实、物联网、云计算、大数据等技术的进步,现实社会中的犯罪类型已经向网络空间迁移,并且滋生出网络空间特有的犯罪类型。据统计,中国网络犯罪占犯罪总数的1/3,并以每年近30%的速度增长。可以预见,未来绝大多数犯罪都会涉及网络,甚至杀人、强奸等恶性犯罪亦不例外。“互联网+犯罪”时代,电子数据无疑成为证明网络犯罪事实的重要依据。面对网络犯罪持续高发、形式多变的复杂态势,对网络犯罪侦查打击也提出了顺势变革的要求,而在推进“以审判为中心”的诉讼制度改革的背景下,证据标准要求做到“案件事实清楚,证据确实、充分”。

电子数据取证作为一门法庭科学,已融入各个警种的业务,在现场勘查、情报搜集、数据鉴定、案件分析、技术支持等方面起到重要支撑作用。由于电子数据的存在形态和取证模式与传统证据存在较大差异,其收集和使用对传统刑事诉讼规则带来了巨大冲击和挑战。面对新形势的迫切要求,公安机关亟待提升电子数据取证意识和能力。

除在刑事执法领域能更加强有力地支撑打击各类犯罪外,电子数据取证技术应用日益广泛,早已扩展到知识产权保护、纪检监察、工商管理、税务稽查、企业内部调查、民事诉讼等领域,与社会生活的关系也越来越密切。

5.1.1 电子数据的概念及界定

电子数据(electronic data)是一种新的证据类型,常用中文表述方式包括“电子证据”“数字证据”“计算机证据”“电子物证”等。英文表述方式包括“electronic evidence”

“computer evidence”“digital evidence”等。2012年,《中华人民共和国刑事诉讼法》修正,首次明确了“电子数据”这一称谓,并确立了电子数据法定证据种类的地位。目前,刑事、民事、行政三大诉讼法均承认了电子数据独立的法律地位,对电子数据这一新型证据类型的称谓也予以统一,这是我国证据种类立法的巨大进步,电子数据已经成名副其实的“证据之王”,电子数据取证司法应用空间日益广阔。

广义上讲,只要以电子形式存储、处理、传输的信息都是电子数据。从技术层面来看,电子数据,是指基于计算机应用、通信和现代管理技术等电子化技术手段形成包括文字、图形符号、数字、字母等的客观资料。而狭义上的电子数据即三大诉讼法中所规定的电子数据。电子数据取证指的是运用计算机及相关科学、技术原理和方法获取电子数据以证明某个客观事实的过程,它包括电子数据的确定、收集、保护、分析、归档以及法庭出示等环节。

2016年最高人民法院、最高人民检察院和公安部(简称“两高一部”)联合发布的《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》(以下简称《规定》)第一条采取“概括+例举+排除”的方式,对电子数据作了明确界定,具体如下。

电子数据是案件发生过程中形成的,以数字化形式存储、处理、传输的,能够证明案件事实的数据。

电子数据包括但不限于下列信息、电子文件:

- (1) 网页、博客、微博客、朋友圈、贴吧、网盘等网络平台发布的信息;
- (2) 手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信信息;
- (3) 用户注册信息、身份认证信息、电子交易记录、通信记录、登录日志等信息;
- (4) 文档、图片、音视频、数字证书、计算机程序等电子文件。

以数字化形式记载的证人证言、被害人陈述以及犯罪嫌疑人、被告人供述和辩解等证据,不属于电子数据。确有必要的,对相关证据的收集、提取、移送、审查,可以参照适用本规定。

针对《规定》第一条给出的概念和界定,需要注意以下几个问题。

定义中将电子数据限定为“案件发生过程中”,是为了将案件发生后形成的证人证言、被害人陈述以及犯罪嫌疑人、被告人供述和辩解等电子化的言词证据排除在外。不宜将“案件发生过程中”狭义理解为必须是实行行为发生过程中。例如,性侵犯罪发生前行为人与被害人往来的短信、网络诈骗实施前行为人设立的钓鱼网站等,只要与案件事实相关的,均可以视为“案件发生过程中”形成的电子数据。

《规定》列举了多种电子数据类型,对不同类型的电子数据的取证程序要求可能存在差别,如对于通信信息的收集、提取可能涉及技术侦查措施,应当经过严格的批准手续。

证据具有三性,即客观性、关联性和合法性。作为证据的种类之一,电子数据无疑也应具备此三性,即:电子数据必须是客观存在的;且与需要证明的案情之间有一定的关系或联系;由法定机关、法定人员依照法定程序收集和取得。符合以上特性的电子数据才认定为证据,否则不能作为法定证据来使用。

5.1.2 电子数据的特征

电子数据和传统证据相比,最本质的区别在于其存在形式。电子数据是世界万物的数字化。电子数据与其他传统证据相比,除了同样具备客观性、关联性和合法性三个基本特性外,由于其存在形式的特殊性,电子数据还具有以下几方面的特性。

1. 无形而有万形

电子数据虽然客观存在,但非物理实体,必须依赖介质存储、传输和处理,表现形态千变万化。可称得上是“无形而有万形”。

这里所说的“形”是指物体的物理形态,电子数据是客观存在的,却没有一般物体的形。现代计算机采用二进制编码,即0和1。电子数据最本质的或者最原始的状态就0和1编码的组合。这些0和1要借助光、磁、电等介质进行存储、传输和处理。其记录的内容不但肉眼看不到,具有无形性,而且单凭人的思维难以解读,只有通过一系列的运算、编译操作,把难以理解的0和1转换为人可以识别的文字、图案、视频、音频、动画等形式,通过显示器、打印机等输出设备显示或打印后才能为人识别。随着技术的发展,未来电子数据还有可能衍生出其他的表现形态。

电子数据的载体是各种电子设备,随着物联网技术的发展和万物互联时代的到来,越来越多的设备具备了智能处理功能。要求公安民警注意学习了解相关知识,有利于案件现场迅速有效地捕捉到电子数据证据。同时还要注意到,现在电子设备普遍具备网络连接性能,云技术的蓬勃发展带来了云存储的概念,电子数据既可以存在于本地的客户端,也可以保存在云端的服务器,所以找寻电子数据的过程中,不要忽略基于网络的电子数据取证。

2. 脆弱性与稳定性并存

电子数据自身的特点决定了其存储、传输、处理容易受到篡改或破坏。存储环境影响、操作不当、设备故障、人为故意都有可能改变甚至破坏电子数据的内容。因此,对电子数据的操作应严谨规范,避免对电子数据篡改破坏。对收集的电子数据应妥善保管,远离磁场、高温环境,避免静电、潮湿、灰尘和试剂的腐蚀。应采用适当的存储介质进行电子数据的保全备份。对存储介质操作前应先进行写保护,并打封签字,避免介质损坏或被修改,取证后封存。

电子数据具有脆弱性的同时,又具有稳定的另一面。绝大多数情况下对于电子数据的增加、删除、修改都会留有一定的痕迹,而且适宜的情况下被破坏的数据可以通过技术手段被恢复到破坏前的状况。同时电子数据可以方便精确地进行复制,如果不考虑人为篡改、差错和故障等因素,复件内容与原件内容完全一致,且可长期无损保存。

3. 易失性与持久性并存

在一些场景下,电子数据具有易失性。如大家熟悉的内存又叫做随机存取存储器(random access memory, RAM),这种存储器在断电时将丢失其存储内容。内存的取证分析可以查看分析系统进程、系统服务、网络连接等重要数据。内存分析有一个非常经典的工具 Volatility,用于解析内存镜像信息,在案件现场勘验中遇到开机的设备,不能贸然

关机封存,应当充分考虑到电子数据的易失性,及时固定电子数据证据。

当存储条件适宜时,电子数据又可以长期无损保存。比如2019年10月28日上午,重庆市万州区一辆公交车与小轿车在万州长江二桥相撞后,公交车直接坠入江中。10月31日凌晨潜水人员将行车记录仪以及SD卡打捞出水后,公安机关经过模拟实验,对SD卡内数据进行成功修复,终于提取到事发之前车辆内部的监控视频。

5.1.3 电子数据取证的基本原则

电子数据自身的特点决定了其取证过程要科学严谨,符合客观规律,遵循普遍性指导原则,同时也要依据其独特性遵循特定原则,目的就是保证电子数据的完整性、取证过程的可溯性、取证过程的合法性。业内普遍认同四个基本原则,即:不损害原则;避免使用原始证据原则;证据及时固定原则;遵循相关的法律法规、操作规范的原则。综合国内外提出的电子数据取证原则,归纳如下。

1. 普遍性指导原则

1) 合法性原则

证据的收集、固定、保全要严格按照相应法律法规及标准实施,电子数据取证的主体、程序、手段都必须合法。

2) 及时高效性原则

电子数据证据具有较强的时效性,如网络连接、系统日志、进程通信等都会发生动态变化,因此进行电子数据取证时应做好充分预案,及时采取保护措施,尽力避免证据的销毁和破坏。在确定取证对象之后,应该尽早收集证据,保证相关电子数据没有受到任何破坏或损失。

3) 客观全面性原则

要全面收集能够反映案件真实情况的电子数据,并且要求在收集时,既收集存在于计算机软硬件上的电子数据,也收集其他相关设备中的电子数据;既收集文本,也收集图形、图像、动画、音频、视频等各种信息。

4) 建立证据保管链原则

自确定取证对象起,就必须建立电子证据保管链记录。在取证过程中,以发现取证对象为起点,以取证结束为终点,记录整个取证过程。采用录像、拍照或者笔录等方式,准确连续记录整个取证过程,包含时间、地点、人员、设备型号、开关机状态、正在运行的程序、现场操作过程和方法、取证分析操作过程和方法、所使用的软硬件技术等,避免人为破坏电子数据,保证数据真实可靠。另外在取证后也要记录电子数据的保管、流转等情况。

5) 保密性原则

电子数据取证人员在取证过程中,往往会接触涉及国家秘密、商业机密、个人隐私等方面的信息。取证人员应该在自己的本职工作范围内进行取证,不查阅与取证无关的其他信息,若因工作需要了解上述信息,应对信息进行严格保密。

2. 特定原则

1) 无损取证原则

一是要保障电子数据处于安全的环境之中,应妥善保存,在提取、运输、保存、分析和检验的过程中必须避免受到高磁场、高温、灰尘、积压、潮湿、腐蚀性化学试剂等因素的影响,造成电子证据的变化或丢失。

二是取证过程必须保障电子数据的完整性,利用相关的专业设备或软件,在提取电子数据时使用只读锁等专业设备和方法保证介质处于只读模式,确保数据的清洁,保证数据的无损,提取到真实完整的数据。

三是要确保电子数据的安全无损,尽量避免直接在原始数据上进行取证操作。这点可以通过保全备份技术实现,原始电子数据可以通过克隆或镜像技术进行复制之后再对拷贝数据进行分析。

2) 具备专业技能原则

进行电子数据取证操作的人员应该具备相应的技术基础和实际操作水平,异常情况下,如果有人提出必须访问目标计算机中的原始数据,该人必须有能力完成并且解释该行为的原因和后果,并给出证据。

3) 可追溯原则

电子数据取证活动需要明确记录并保存。取证过程可以根据记录文档进行追溯和重复,并得到相同的结果。

5.1.4 电子数据取证的一般步骤

1. 电子数据的发现

电子数据的发现指在侦查和现场勘查中发现涉案电子数据。在获得法律授权、确定人员和装备的情况下明确取证对象目标,决定哪些设备和数据应该被获取。如硬盘、U盘、照片、图表、文档、数据库等。如果进行现场取证,还应获取案件有关的额外信息,如:电子邮箱;ISP 登录用户名;网络拓扑图;用户、系统日志;用户名、密码等。

2. 电子数据的获取

电子数据的特性决定了获取的步骤应十分谨慎,任何错误行动都将破坏证据,并可能导致完全不同的结果。电子数据必须保存于原始状态中,防止被不正确的处理方法所影响、损坏或者被删除。进行电子数据获取时应采取写保护(只读)技术,根据案件情况采用磁盘复制(克隆或镜像)、文件拷贝及易失性数据提取技术等方法。

3. 电子数据的固定

电子数据的固定,保证了现场勘查和侦查获得数据的完整性和真实性。对作为证据使用的电子数据,应当采取扣押和封存电子数据原始存储介质、计算电子数据完整性校验值、制作和封存电子数据备份、冻结电子数据、对收集和提取电子数据的相关活动进行录像等方法保证其完整性。由于客观原因无法或者不宜收集、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。

4. 电子数据的分析

电子数据分析的目的是为了证实信息的存在、信息的来源及信息传播途径,重构犯罪行为、动机及嫌疑人特征。分析是电子数据取证的核心和关键,是最体现取证人员取证能力的环节。不同类型的案件需要采取不同的分析方法,如系统仿真、数据恢复、文件过滤、关键词搜索、统计比对、密码破解等技术。

5. 电子数据的展示

电子数据取证的最后阶段,也是最终目的,是整理并展示取证分析结果,以形成“证据链”供法庭作为诉讼证据。取证人员将获取的相关证据和原始记录,按照司法要求以一定的格式客观、准确地报告事实,并形成鉴定意见或者检验报告。意见或报告里要体现犯罪行为的时间、地点、直接证据信息、系统环境信息,同时要包括取证过程以及对电子数据的分析结果和报告。

5.2

电子数据取证规范

电子数据之所以能成为一种新的证据种类,就是因为它与传统证据之间存在诸多差异。俗话说,“没有规矩,不成方圆。”电子数据证据走向成熟,规范电子数据的提取和运用,更好地证明案件事实,一定要有完备的法律法规和标准规范体系来加以规制。

电子数据证据规制既要基于法律规则又要基于技术规则。技术规则必须为法律所用,法律规则对电子数据的取证行为做出规范。现行的法律法规及标准,都是充分考虑到电子数据的技术特点,经过了无数次实践摸索而形成的。

5.2.1 电子数据取证相关法律法规

在刑事司法领域执法和司法实践推动下,基于公安机关打击网络犯罪案件中电子数据取证经验,我国刑事司法领域逐步建立起电子数据取证规则体系。作为2012年《中华人民共和国刑事诉讼法》新增的法定证据种类,电子数据在证明案件事实的过程中发挥着越来越重要的作用。针对司法实践中产生的新情况和新问题,立法机关通过司法解释、规范性文件等方式,对电子数据的收集与提取、移送与展示、审查与判断作了全面规定,通过建立和完善见证人规则、专家辅助人规则、笔录规则、鉴定规则等,构建起了我国刑事电子数据的规则体系。

2012年以前,对电子数据的大多数规定仅仅局限于鉴定的范畴,极少有文件提及电子数据收集提取的问题。在案件侦查、起诉和审判的实践过程中,多将电子数据转化为其他证据类型使用。

2012年,修改后的《中华人民共和国刑事诉讼法》将电子数据确立为法定证据类型,从根本上确立了电子数据的独立证据地位。同年,最高人民法院出台了《关于适用〈中华人民共和国刑事诉讼法〉的解释》(法释〔2012〕21号),其中第九十三条和第九十四条对电子数据审查判断的最基本原则进行了规定。

2014年,两高一部联合出台了《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》(公通字〔2014〕10号),其中专设一章对电子数据的收集、提取等专门性问题进行了明确。

2016年,两高一部又联合出台了《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》(法发〔2016〕22号,以下简称“两高一部《规定》”),进一步统一了公检法部门在司法实践中对电子数据的认识和判断标准,提出了电子数据收集提取、审查判断的具体方法,明确了电子数据真实性、合法性、关联性审查的原则,确立了“扣押原始存储介质为主、提取电子数据为辅、打印拍照为例外”的电子数据取证原则。

为使各地公安机关更好地执行“两高一部《规定》”,规范公安机关在办理刑事案件过程中的电子数据取证工作,公安部于2018年12月13日发布了《公安机关办理刑事案件取证规则》(公通字〔2018〕41号),共5章61条,实际上是根据两高一部《规定》的相关要求,对公安机关办理刑事案件收集、提取涉案电子数据作出的进一步细化规定。主要明确了:电子数据取证的阶段划分;强调了原始存储介质的扣押封存;电子数据现场取证规范;“拍照打印”方式的适用情形;无见证人时录像规范;登记保存的适用情形;网络在线提取和远程勘验的区别;网络在线提取的适用范围;冻结电子数据的程序和期限问题;电子数据检查的性质;电子数据检查见证人等问题。

2021年6月22日,两高一部发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见(二)》,针对司法实践中存在的新的突出问题,如跨境电信网络诈骗犯罪案件的取证等问题进行了规定。

目前,我国已经形成了比较完善的电子数据取证法律法规及标准体系。除三大诉讼法及其司法解释之外,还有大量的相关司法解释、部门规章以及规范性文件涉及电子数据证据。刑事司法领域电子数据取证相关法律法规见表5-1。同时,越来越多的民事案件也涉及电子数据,相关法律法规如表5-2所示。民事诉讼案件在证明分类、证明对象、证明程度方面与刑事案件有区别,但电子数据技术原理及基本原则是相通的。本节主要介绍刑事案件电子数据取证规则。

表 5-1 刑事司法领域电子数据取证相关法律法规

法律	中华人民共和国刑事诉讼法(2018年修正)
司法解释(司法解释性质文件)	最高人民法院、最高人民检察院、公安部、国家安全部、司法部《关于办理死刑案件审查判断证据若干问题的规定》 最高人民法院关于适用《中华人民共和国刑事诉讼法》的解释

续表

司法解释(司法解释性质文件)	最高人民法院刑事诉讼规则(试行) 最高人民法院、最高人民检察院《关于办理走私刑事案件适用法律若干问题的解释》 最高人民法院、最高人民检察院、公安部《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》 最高人民法院、最高人民检察院、公安部《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》(一)、(二) 最高人民法院、最高人民检察院、公安部《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》 最高人民法院、最高人民检察院《关于办理扰乱无线电通讯管理秩序等刑事案件适用法律若干问题的解释》
部门规章	公安机关办理刑事案件程序规定
规范性文件	最高人民检察院《电子证据勘验程序规则》(试行) 计算机犯罪现场勘验与电子证据检查规则 公安机关执法细则(第三版) 公安机关办理刑事案件电子数据取证规则

表 5-2 民事诉讼电子数据取证相关法律法规

法律	中华人民共和国民事诉讼法
司法解释(司法解释性质文件)	最高人民法院关于适用《中华人民共和国民事诉讼法》的解释 最高人民法院关于民事诉讼证据的若干规定 最高人民法院关于互联网法院审理案件若干问题的规定
规范性文件	杭州互联网法院民事诉讼电子数据证据司法审查细则(试行) 广东广州南沙法院互联网电子数据证据举证、认证规程(试行) 北京互联网法院电子诉讼庭审规范(试行)

5.2.2 电子数据取证相关标准及规范

根据《中华人民共和国标准化法》及《标准化工作指南》(GB/T 20000),对电子数据取证标准做如下界定:电子数据取证标准是指电子数据取证领域需要统一的技术要求,按照规定的程序经协商一致制定供电子数据取证相关从业人员共同使用和重复使用的文件。电子数据取证标准为电子数据的确定、收集、保护、分析、归档、鉴定以及法庭出示等环节提供规则、指南或特性。

电子数据取证是一个动态的过程,包括确定、收集、保护、分析、归档、鉴定、法庭出示等多个环节。值得注意的是,随着电子数据取证领域的扩展,电子数据取证标准的实施主体除侦查人员外,还有技术支持人员、第三方鉴定机构人员、电子数据取证产品提供商等。同时,律师、公证人员、法官等也需要密切关注电子数据取证标准的实践运用。

电子数据取证标准用于指导电子数据取证工作,提升电子数据取证工作的质量,规范电子数据取证工作流程。推进电子数据取证标准化工作,加强电子数据取证标准建设,对规范电子数据取证工作、维护司法公正、保障人民合法权益有着重要的意义。

电子数据取证相关标准和规范主要集中在刑事执法领域和司法鉴定领域。

1. 刑事执法领域

在刑事执法领域,《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》第二条规定:“侦查机关应当遵守法定程序,遵循有关技术标准,全面、客观、及时地收集、提取电子数据。”第七条规定:“收集、提取电子数据,应当由两名以上侦查人员进行,取证方法应当符合相关技术标准。”第二十四条规定:“对收集、提取电子数据是否合法,应当着重审查以下内容:(一)收集、提取电子数据是否由二名以上侦查人员进行,取证方法是否符合相关技术标准。”

《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》中关于电子数据的取证与审查部分第十三条规定,“收集、提取电子数据,应当由两名以上具备相关专业知识的侦查人员进行。取证设备和过程应当符合相关技术标准,并保证所收集、提取的电子数据的完整性、客观性。”

《公安机关办理刑事案件电子数据取证规则》第一章总则第二条规定:“公安机关办理刑事案件应当遵守法定程序,遵循有关技术标准。”第三章电子数据的检查和侦查实验第四十五条规定:“电子数据检查应当符合相关技术标准。”

2. 司法鉴定领域

《全国人民代表大会常务委员会关于司法鉴定管理问题的决定》(2005年2月28日第十届全国人民代表大会常务委员会第十四次会议通过)第十二条规定:“鉴定人和鉴定机构从事司法鉴定业务,应当遵守法律、法规,遵守职业道德和职业纪律,尊重科学,遵守技术操作规范。”

2016年颁布的《司法鉴定程序通则》(司法部令第132号)第二十三条规定:“司法鉴定人进行鉴定,应当依下列顺序遵守和采用该专业领域的技术标准、技术规范和技术方法:(一)国家标准;(二)行业标准和技术规范;(三)该专业领域多数专家认可的技术方法。”

《公安机关电子数据鉴定规则》(公通字〔2017〕6号)第三十五条规定:“鉴定人应当按照本专业的技术规范和方法实施鉴定,并全面、客观、准确地记录鉴定的过程、方法和结果。”

截至2021年6月,我国电子数据取证相关标准包括推荐性国家标准4项,公共安全行业标准36项,司法鉴定技术标准17项,认证认可行业标准8项,详见表5-3。

表 5-3 电子数据取证相关标准

推荐性国家标准	GB/T 29360—2012 电子物证数据恢复检验规程 GB/T 29361—2012 电子物证文件一致性检验规程 GB/T 29362—2012 电子物证数据搜索检验规程 GB/T 31500—2015 信息安全技术存储介质数据恢复服务要求
公共安全行业标准	GA/T 754—2008 电子数据存储介质复制工具要求及检测方法 GA/T 755—2008 电子数据存储介质写保护设备要求及检测方法 GA/T 756—2008 数字化设备证据数据发现提取固定方法

续表

公共安全行业标准	<p>GA/T 757—2008 程序功能检验方法</p> <p>GA/T 828—2009 电子物证软件功能检验技术规范</p> <p>GA/T 829—2009 电子物证软件一致性检验技术规范</p> <p>GA/T 976—2012 电子数据法庭科学鉴定通用方法</p> <p>GA/T 977—2012 取证与鉴定文书电子签名</p> <p>GA/T 978—2012 网络游戏私服检验技术方法</p> <p>GA/T 1069—2013 法庭科学电子物证手机检验技术规范</p> <p>GA/T 1070—2013 法庭科学计算机开关机时间检验技术规范</p> <p>GA/T 1071—2013 法庭科学电子物证 Windows 操作系统日志检验技术规范</p> <p>GA/T 1170—2014 移动终端取证检验方法</p> <p>GA/T 1171—2014 芯片相似性比对检验方法</p> <p>GA/T 1172—2014 电子邮件检验技术方法</p> <p>GA/T 1173—2014 即时通讯记录检验技术方法</p> <p>GA/T 1174—2014 电子证据数据现场获取通用方法</p> <p>GA/T 1175—2014 软件相似性检验技术方法</p> <p>GA/T 1176—2014 网页浏览器历史数据检验技术方法</p> <p>GA/T 1474—2018 法庭科学 计算机系统用户操作行为检验技术规范</p> <p>GA/T 1475—2018 法庭科学 电子物证监控录像机检验技术规范</p> <p>GA/T 1476—2018 法庭科学 远程主机数据获取技术规范</p> <p>GA/T 1477—2018 法庭科学 计算机系统接入外部设备使用痕迹检验技术规范</p> <p>GA/T 1478—2018 法庭科学 网站数据获取技术规范</p> <p>GA/T 1479—2018 法庭科学 电子物证伪基站电子数据检验技术规范</p> <p>GA/T 1480—2018 法庭科学 计算机操作系统仿真检验技术规范</p> <p>GA/T 1554—2019 法庭科学 电子物证检验材料保存技术规范</p> <p>GA/T 1564—2019 法庭科学 现场勘查电子物证提取技术规范</p> <p>GA/T 1568—2019 法庭科学 电子物证检验术语</p> <p>GA/T 1569—2019 法庭科学 电子物证检验实验室建设规范</p> <p>GA/T 1570—2019 法庭科学 数据库数据真实性检验技术规范</p> <p>GA/T 1571—2019 法庭科学 Android 系统应用程序功能检验方法</p> <p>GA/T 1572—2019 法庭科学 移动终端地理位置信息检验技术方法</p> <p>GA/T 1663—2019 法庭科学 Linux 操作系统日志检验技术规范</p> <p>GA/T 1664—2019 法庭科学 MS SQL Server 数据库日志检验技术规范</p> <p>GA/T 1713—2020 法庭科学 破坏性程序检验技术方法</p>
司法鉴定技术标准	<p>SF/Z JD0400001—2014 电子数据司法鉴定通用实施规范</p> <p>SF/Z JD0401001—2014 电子数据复制设备鉴定实施规范</p> <p>SF/Z JD0403001—2014 软件相似性检验实施规范</p> <p>SF/Z JD04020001—2014 电子邮件鉴定实施规范</p> <p>SF/Z JD0400002—2015 电子数据证据现场获取通用规范</p> <p>SF/Z JD0402003—2015 即时通讯记录检验操作规范</p> <p>SF/Z JD0403003—2015 计算机系统用户操作行为检验规范</p> <p>SF/Z JD0403002—2015 破坏性程序检验操作规范</p> <p>SF/Z JD0401002—2015 手机电子数据提取操作规范</p> <p>SF/Z JD0402002—2015 数据库数据真实性鉴定规范</p> <p>SF/Z JD0402004—2018 电子文档真实性鉴定技术规范</p> <p>SF/Z JD0403004—2018 软件功能鉴定技术规范</p> <p>SF/Z JD0404001—2018 伪基站检验操作规范</p>