第3章 电子数据的封存、固定和提取

对于作为证据的电子数据，应注意保护电子证据的完整性、真实性和原始性。对不同类型的电子数据的取证程序存在一定的差别，根据不同的场景和要求，可分为收集和提取、调取和冻结、扣押、封存和固定。

3.1 电子数据的封存

在GA/T 1174—2014《电子证据数据现场获取通用方法》中，对电子设备和存储介质的封存有如下要求。对于已经关闭的系统，在法律允许的范围内并在获得授权的情况下，应对相关电子设备和存储介质进行封存，方法如下：

(1) 采用的封存方法应当保证在不解除封存状态的情况下无法使用被封存的存储介质和启动被封存的电子设备。

(2) 封存前后应当对被封存电子设备和存储介质进行拍摄或者录像并进行记录，照片或者录像应当从各个角度反映设备封存前后的状况，清晰反映封口或张贴封条处的状况。

(3) 对系统附带的电子设备和存储介质也应实施封存。

2016年颁布的《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》第八条规定："收集、提取电子数据，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。封存电子数据原始存储介质，应当保证在不解除封存状态的情况下，无法增加、删除、修改电子数据。封存前后应当拍摄被封存原始存储介质的照片，清晰反映封口或者张贴封条处的状况。封存手机等具有无线通信功能的存储介质，应当采取信号屏蔽、信号阻断或者切断电源等措施。"

在法律允许的范围内并在获得授权的情况下，结合实际情况进行分析，对系统是否需关闭做出判断并采取相应的措施。对于不能关闭的电子设备和存储介质，应遵循以下几点：

(1) 采用的封存方法应当保证在不解除封存状态的情况下，电子设备和存储介质可保持原有运行状态。

(2) 对于有特殊要求的电子设备和存储介质(如手机等无线设备),应保证电子设备和存储介质的封存方式完全屏蔽,不因电磁等影响而发生实质性改变。

(3) 封存前后应当对被封存电子设备和存储介质进行拍摄或者录像并进行记录,照片或者录像应当从各个角度反映设备封存前后的状况,清晰反映封口或张贴封条处的状况。对于无法计算存储介质完整性校验值或制作备份的情形,应当封存原始存储介质,并记录不计算完整性校验值或制作备份的理由。

3.2 电子数据的固定

电子数据取证是一个复杂的调查分析的过程,取证调查人员需要综合考虑数据的原始性、有效性和合法性等各种因素。由于电子数据证据可能随时因各种原因丢失或者发生变化,从而影响证据的效力,因此,在取证过程中,取证调查人员应尽可能避免直接对数据进行操作;同时,取证调查人员应获取待取证设备的磁盘镜像等备份文件,并基于这些备份文件进行取证分析,以防止原始数据被篡改。

上述获取磁盘镜像的做法旨在确保镜像文件的原始性和有效性。磁盘镜像是保证检材的真实性、唯一性,并防止数据被篡改的一种做法,是固定电子数据证据的一种方式。但是,值得注意的是,制作磁盘镜像并不适用于所有的数字设备。例如,由于智能手机中复杂的安全机制和数据加密算法,使得获取手机设备的磁盘镜像特别困难。针对智能手机等设备,目前普遍采取的是获取其备份文件的做法,该方法被视为电子数据的提取。

本节以获取设备的磁盘镜像为主,详细阐述电子数据固定过程中涉及的工具以及镜像文件的格式。

证据数据获取是对电子设备存储、处理、传输的数据进行搜索、分析、截获,获得证据数据的过程。在证据数据发现和提取过程中,采取技术措施或记录相关信息,保护证据数据完整性,在电子数据固定过程中,应注意以下事项:

(1) 证据固定原则。电子数据的固定应遵循及时性、依法、备份、证据原始性、环境安全和监督原则。

(2) 记录检材。取证调查人员进行电子数据证据固定前,应对检材进行唯一性编号,然后对送检设备逐一拍照,并记录检材的特征。

(3) 固定证据的方法。按照相关规定,应根据不同的条件选择不同的固定证据的方法。在多数情况下,对于计算机内置硬盘,应从主机中拆卸下来,在进行编号、正反面拍照之后,再连接取证工作站或硬盘复制机,采用镜像或克隆副本的方式进行证据固定。根据取证原则,证据固定应该对完整的磁盘创建镜像文件,这样可以包含所有的数据信息。大多数取证工具支持对物理磁盘或逻辑磁盘的数据获取功能,通常情况下,应该选择获取物理磁盘;但是,在物理磁盘被加密或者部分损坏的情况下,则应优先选择获取逻辑磁盘。

3.2.1 数据固定工具

目前,对硬盘数据的获取主要采取对硬盘进行镜像的方式,在国内外市场上,相关的

专业取证设备较多。例如，硬盘复制机能够通过对目标硬盘的快速物理复制，实现对硬盘数据的完整获取；硬盘写保护设备能够配合磁盘镜像软件实现对硬盘数据的全面获取。

1. 硬盘复制机/硬盘写保护设备

硬盘复制机是电子数据取证中最常见的镜像设备。它基于位对位(bit-to-bit)的方式对硬盘进行复制，能够将硬盘的所有数据通过物理复制的方式进行克隆。硬盘复制机支持的复制方式包括硬盘到硬盘、分区到分区、硬盘到分区、分区到硬盘、硬盘到文件和分区到文件等方式。

因为硬盘复制机采用基于物理扇区的复制，能够完整地复制物理磁盘中的所有数据，所以，取证调查人员能够在创建的磁盘镜像中进行数据恢复等操作。此外，由于硬盘复制的过程能够完全脱离计算机使用，且能够直接连接硬盘执行操作，因此能够充分加快数据传输的速度。

目前市场上主流的硬盘复制机，支持包括 IDE、SATA、mSATA、SAS、SCSI、USB 和 PCIe 等接口。取证调查人员在进行证据固定工作时，应注意硬盘复制机和数据线是否支持相应的硬盘设备。

使用硬盘复制机对原始硬盘进行副本制作，制作的硬盘副本与原始硬盘的数据完全一致，并且可以通过校验算法进行一致性验证。目前，硬盘复制机主要的校验算法包括 SHA-1、SHA-256、MD5 和 CRC32。通过一致性校验，制作的磁盘镜像文件能够作为电子证据被法律认可。因此，通过硬盘复制机进行数据固定已经得到了全世界大多数国家执法部门的认可。

硬盘复制机的作用是能够直接克隆源数据盘或生成镜像文件，这样相对快速且方便；相较于硬盘复制机，硬盘写保护设备的特性在于，能够作为保护桥将磁盘直接接入计算机中进行分析，配合 FTK Imager 等磁盘镜像工具也能够创建完整的磁盘镜像文件。

图 3-1 和图 3-2 分别是美国 Logicube 公司推出的硬盘复制机和硬盘写保护设备。国内的美亚柏科、奇安信和白虹软件等公司也有各自的硬盘复制机设备。

图 3-1　美国 Logicube 公司的硬盘复制机

图 3-2　美国 Logicube 公司的硬盘写保护设备

2. 镜像软件

目前，市场上常见的镜像软件有 X-Ways Forensics、EnCase Imager、FTK Imager 和 MyHex 等。

FTK Imager 是美国取证厂商 AccessData 公司提供的证据获取及数据提取的免费工具。它支持多种镜像文件格式，包括 DD、E01、L01、DMG、VMDK、VHD 等。可以获取物理磁盘、逻辑磁盘、内存、受保护的文件(如当前系统的注册表文件)，安装后复制安装目录

到任意地方都可以直接运行。

MyHex 是武汉天宇宇达科技有限公司研发的一款免费的数字取证工具，支持创建 DD、E01 等格式的镜像文件，具有十六进制查看、数据恢复、手工分析工具，支持数据恢复、文件系统底层分析、数据格式分析、数据预览等功能。

3. 取证启动盘

由于专业的硬盘复制设备价格昂贵，且不能适用于所有的取证环境。因此，取证专家研究并推出了多种能够用于获取原始存储介质数据的工具，例如 PALADIN、WinFE、Kali Linux 以及 DEFT Linux 等。在以 PALADIN 和 Kali Linux 为代表的 Linux 启动盘中预置了 Linux 在线取证分析工具。而在定制的 WinFE 启动盘中可以预安装 X-Ways Forensics、MyHex、FTK Imager 等镜像获取工具。

PALADIN 启动盘是美国 Sumuri 公司开发的用于电子数据取证的 Linux 取证套件，基于 Ubuntu 系统。简单来说，PALADIN 启动盘中包含一个工具集，集成了 Autopsy 等知名开源取证工具，其中包含几十个类别的上百种取证小工具，支持创建镜像文件和镜像文件的格式转换。

WinFE 是微软高级取证技术专家 Troy Larson 开发的，全称为 Windows Forensic Environment。WinFE 的早期版本只是简单地将两个注册表键值添加到启动盘中，阻止启动时对磁盘自动挂载卷。目前的 WinFE 可以在 UEFI 和传统系统上加载并启动，无须更改 BIOS 设置，可以定制后用于启动微软公司的 Surface Pro 等设备，对其内置的固态硬盘制作镜像，并支持 BitLocker 解锁。

3.2.2　镜像文件的格式

镜像文件是从源存储介质复制生成的一个或一组文件，利用该文件或文件组中存储的数据可重新创建源存储介质存储的数据比特流。常见的镜像文件有原始格式镜像(DD)、EnCase 格式镜像(E01) 和高级取证格式镜像(AFF)等格式。

1. 原始格式镜像

原始格式镜像也称为 DD 镜像、RAW 格式镜像，是采用对源存储介质进行逐比特复制的方法生成的一个或一组文件。原始格式镜像文件与源存储介质的大小完全一致。在原始格式镜像文件中，没有额外的空间用于存储元数据以及取证信息记录。源存储介质序列号、调查员姓名、哈希值等信息通常存入单独的文件。原始格式镜像文件主要有 dd、001、img，raw 和 bin 等扩展名。

2. EnCase 格式镜像

EnCase 格式镜像是 EnCase 软件的私有镜像文件格式，最早起源于 EWF(Expert Witness Format，专家证人格式)，后来经过演变形成了目前的镜像文件格式。该镜像文件内部可以存储源存储介质序列号、调查员姓名、哈希值等元数据信息，支持数据压缩，可以节省存储原始格式镜像文件所需的空间。EnCase 格式镜像包含两种物理镜像格式，扩展名分别为 e01 和 ex01。此外，Encase 还支持两种逻辑镜像格式，扩展名分别为 l01 和 lx01。

3. AFF 格式镜像

针对 EnCase 格式镜像和原始格式镜像的不足，AFFLIB 公司于 2006 年推出了开源的镜像文件格式 AFF，全称为 Advanced Forensics Format（高级取证格式），这种格式是公开而且可扩展的。相较于 EnCase 格式镜像，AFF 格式镜像同样以压缩片段的方式保存磁盘镜像；和 EnCase 格式镜像不同的是，AFF 格式镜像既可以将元数据保存在镜像文件内部，也同时允许元数据单独保存在一个文件中。

4. 虚拟磁盘格式

在数字取证中，经常会涉及各种各样的虚拟磁盘文件，这些文件中存储着操作系统、文件系统和应用程序数据。常见的虚拟磁盘文件主要有 VMDK、VHD 和 VDI 等格式。VHD 是 Virtual Hard Disk（虚拟硬盘）的简称，能够由部分版本的 Windows、Virtual PC、Virtual Box 等直接创建。VDI 是 Virtual Disk Images（虚拟磁盘镜像）的缩写，是 Virtual Box 软件的虚拟磁盘文件。VMDK 是 VMware 软件的虚拟磁盘文件。在创建磁盘时，如果设置磁盘的大小可以增加，文件名的文件编号部分将包含字母“s”，例如 Windows 7-s001.vmdk；如果设置预分配全部磁盘空间，文件名的文件编号部分将包含字母“f”，例如 Windows 7-f001.vmdk。

3.3 电子数据的提取

在某些情形下，基于客观原因，无法扣押电子数据的原始存储介质。2016 年发布的《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》第九条规定：“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。”可以进行电子数据提取的情况包括：

（1）原始存储介质不便封存的。

（2）提取计算机内存数据、网络传输数据等未存储在存储介质上的电子数据的。

（3）原始存储介质位于境外的。

（4）其他无法扣押原始存储介质的情形。

在国内外的司法调查、企业调查和应急响应等案例中，满足上述条件的情况有很多，以下给出示例。

原始存储介质不便封存的。例如，在调查涉及企业服务器的案件时，由于其服务器的数据存储容量巨大，且相关设备由于业务连续性必须保持其运转。

提取计算机内存数据、网络传输数据等不是存储在存储介质上的电子数据的。例如，在被恶意程序感染并控制的主机中，恶意代码活跃在内存当中，且文件系统中并无程序的实体文件。在这种情况下，调查人员必须提取内存中的数据，将其转储为内存镜像文件，再做进一步分析。

原始存储介质位于境外的。例如，在涉及色情网站的案件中，原始数据往往存储在境外的服务器中，调查人员无法直接前往调查取证，为获取相关痕迹，只能设法进行在线

提取。

其他无法扣押原始存储介质的情形。例如，某些计算机的硬盘被 BitLocker 等工具进行了加密保护，如果没有密钥或密码，一旦系统关机，将无法解密其中存储的数据。在这种情况下，取证调查人员应及时从正在运行的计算机中提取数据。

针对上述情形，取证调查人员需要使用在线提取或远程提取等方法提取电子数据，同时记录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，对在线提取电子数据的过程应进行全程录像记录，显示提取电子数据的时间、原始存储介质所处的原始状态、提取的工具和方法，并最后计算提取的电子数据的完整性校验值。

3.3.1　在线数据

在线提取是在目标系统运行的情况下获取目标系统中的电子数据的过程。在线提取的方法可以是复制、下载或使用专用的在线提取工具。在线提取的对象可以是远程正在运行的服务器、网站中的数据或现场正在运行的 PC 中的数据。这些数据包括文档、视频、图片、网页等与案件相关的一切电子数据。在线提取流程主要包括以下步骤：

(1) 对现场、屏幕进行拍照录像，记录正在运行的计算机的系统时间，并记录与授时中心标准时间的差异。

(2) 使用在线取证软件提取相关电子数据，保存在目标存储介质中，并计算和记录哈希值。针对现场正在运行的 PC，提取的电子数据应包含内存、正在运行的聊天工具中的聊天记录、已经打开的网页、邮件客户端中的邮件以及加密分区中的文件等数据。

(3) 针对远程正在运行的服务器、网站中的电子数据进行在线提取时不仅要对现场、屏幕进行拍照和录像，还要根据远程主机数据获取规范和网站数据获取技术规范对在线提取的环境进行记录，如服务器基本信息、网站获取参数、代理服务器信息、网站登录用户密码等。

3.3.2　易失性数据

易丢失数据的提取和固定应遵照以下步骤：

(1) 固定保全内存数据，特别是打开并未保存的文档、最近的聊天记录、用户名及密码、其他取证活动相关的文件信息。

(2) 获取系统中相关电子数据证据的信息，包括：存储介质的状态，确认是否存在异常状况等；正在运行的进程；操作系统信息，包括打开的文件、使用的网络端口、网络连接(其中包括 IP 地址信息、防火墙配置等)；尚未存储的数据；共享的网络驱动和文件夹；连接的网络用户；其他取证活动相关的电子数据信息。

(3) 确保证据数据独立于电子数据存储介质的软硬件、逻辑备份证据数据以及属性、时间等相关信息。

由于反取证技术、系统运行与内存交换机制等原因，传统的基于文件系统的取证技术难以有效提取相关数字证据。具体难度主要体现在以下方面：

(1) 操作系统内核通常会及时释放内存页面，使暂存于内存或交换页面文件中的相

关证据信息在关机后消失，造成事后无证可取。

(2) 内存中通常存放有解密密钥、应用程序口令、恶意代码、进程信息、注册表信息、网络连接、系统状态等重要的证据，传统取证方法难以获取，只有通过分析物理内存镜像和页面交换文件的二进制数据才能够获取。

(3) 计算机关闭之后，内存数据清空，只有在计算机处于运行状态时才可以获得内存数据。因此，为了有效而全面地提取与网络攻击有关的信息、加密密钥、未保存的信息，应及时、规范地进行内存取证。

内存取证也称内存转储，指采用基于内核模式驱动程序的内存获取方法，通过内核模式驱动程序读取目标系统中内核内存区对象，以此获取物理内存数据，并保存为镜像格式。内核模式驱动程序位于系统内核层，可轻松绕过系统安全机制而完整地读取内存区对象。

有很多能够获取物理内存数据的工具，例如 Magnet RAM Capture 和 Dumpit 等工具。本书后面的章节将会重点介绍内存分析的方法和工具。

3.3.3 非易失性数据

在应急响应等事件调查场景中，取证调查人员无法或者无须获取完整的证据文件。在这种情况下，一般只需要对特定目录下的文件或符合特定条件的文件进行提取，如只提取部分关键的痕迹文件。一些取证软件可以对特定时间、特定类型和特定大小的文件进行筛选和提取。此外，取证调查人员也可以根据需要筛选并提取浏览器历史记录、注册表和日志等文件。

在这种情况下，取证调查人员可以选择制作逻辑磁盘镜像文件，对所需的文件和目录进行提取。逻辑磁盘镜像文件的优点是可以将原始文件和目录的文件系统相关属性同时保留，原始文件的时间属性、大小、存储位置均保持不变。这种方法的缺点是逻辑磁盘镜像文件需要特定软件才可以打开，并非通用格式。常见的逻辑磁盘镜像文件主要有 CTR、A01 和 L01 等格式。

3.4 电子数据的校验

在数字取证中，当取证调查人员进行证据固定时，完整复制源存储介质或制作源存储介质的镜像后，需计算电子数据和存储介质的完整性校验值，并进行记录。同样，在提取电子数据时也应当场计算完整性校验值。

完整性校验值即哈希值，哈希值(或哈希函数值)被定义为：由数学算法和任意大小的文件(如电子邮件、文档、图片或其他类型的数据)生成的固定长度的数字和字母字符串。这个生成的字符串对于一个文件是唯一的，并且哈希函数是一个单向函数，即计算的哈希值不能被反转以找到可能生成相同哈希值的其他文件。

3.4.1 哈希算法

目前，常用的哈希算法主要有 MD5、SHA-1 和 SHA-256 等，哈希算法主要有以下

特性：

（1）确定性。即特定的输入将始终提供相同的哈希值。

（2）发生哈希碰撞的概率很低。即两个不同的输入同时具有完全相同的哈希值的可能性非常小，甚至几乎不存在。

（3）计算速度快。即哈希值计算的速度特别快。

（4）对输入的任何更改都会更改输出。即一旦输入发生更改，输出也将会被更改。

基于以上特性，在数字取证中，哈希算法在数据的一致性和完整性校验等方面得到了充分的应用：

（1）文件校验。由于哈希算法的特性，使其成为应用最广泛的一种文件完整性校验算法。在数字取证中，为确保流程的严谨、证据链的完整和证据的可靠，证据固定期间制作证据文件时应计算源存储介质、目标存储介质或证据文件的哈希值。在电子数据司法鉴定中，需计算和校验哈希值以确保数据的原始性和完整性。数据的完整性校验常使用 MD5、SHA-1 及 SHA-256 等哈希算法。计算的对象可以是硬盘、分区或特定文件。

（2）数据保护。哈希算法还可用于对重要数据的保护。早些年，部分网站因数据库信息泄露，数据库中存储的用户密码并未采用任何安全保护机制，因此，大量用户的明文密码直接泄露。此后，国内外厂商纷纷注重数据的安全保护，并多采用哈希算法保护明文密码，甚至采用基于不同的加盐变换的哈希算法、多轮哈希值计算等方式提高数据的安全性。

3.4.2　哈希碰撞

如果不同的信息通过某种哈希算法进行计算生成的哈希值相同，就称之为哈希碰撞。

中国密码学专家王小云院士先后于 2004 年和 2005 年在国际密码大会上公布了 MD5、MD4、HAVAL-128、RIPEMD 及 SHA-1 算法存在的安全隐患，提出了密码哈希函数的碰撞攻击理论，即模差分比特分析法，破解了包括 MD5、SHA-1 在内的 5 个国际通用哈希算法，并将比特分析法进一步应用于带密钥的密码算法（包括消息认证码、对称加密算法、认证加密算法）的分析。利用 FASTCOLL 工具对两个不同的程序附加不同的代码，普通计算机在数秒内即可生成具有相同 MD5 哈希值的可执行程序。由此可见，MD5 及 SHA-1 哈希算法不再安全。

在数字取证领域，存在一定的哈希碰撞概率的 MD5、SHA-1 散列算法是否还可以继续用于司法领域的数据完整性校验呢？为避免哈希碰撞和减少不必要的数据安全等问题，在数字取证中，取证调查人员宜采用碰撞概率较低的 SHA-256 等哈希算法。

3.4.3　哈希库

取证调查人员经常需要在嫌疑人的计算机中查找和分析可疑的文件。通常，文件查找的直接方法是在磁盘中遍历搜索和查看每一个文件。但是，手工查找和遍历的做法不仅耗时、效率低下，而且容易漏掉重要文件。利用哈希值校验功能，取证调查人员可以预先构建一个特定文件的哈希库，然后将哈希库中保存的哈希值与磁盘中的所有文件的哈希值进行比较，从而将查找和筛选的过程自动化，这种方法称为哈希比对。

哈希库是哈希值组成的集合，常用于表示一类数据。Windows 操作系统中的很多程序和文件都是标准的，不易被改动，且不包含个人数据。因此，在数字取证中，利用哈希库能够将大量的已知文件从当前案件的数据中过滤出来，从而节省后期数据搜索的时间，提升数据分析效率。

为了减少案件中已知的或无关的文件数量，取证调查人员可以通过导入自行下载、购买或定制的哈希库，从而快速地过滤与案件无关的数据。常用的取证工具，例如 X-Ways Forensics、鉴证大师等，都具备哈希库维护的功能。

3.5 习题与作业

1. 什么是镜像文件？常见的镜像文件有哪几种？

2. 针对电子数据可以进行封存、提取和固定。请论述三者的区别及各自的实施要点。

3. 什么是内存取证？为什么要提取内存数据？

4. 什么是哈希？主要的哈希算法有哪些？

5. 实验和测试报告：磁盘镜像和挂载工具评测报告。

磁盘镜像工具是取证分析的重要工具，其效果和速度与证据固定结果有直接的关系。镜像挂载工具能够将磁盘镜像中的分区/卷挂载到当前文件系统中，一般支持多种镜像格式，如 DD、E01、DMG 等，也支持虚拟磁盘格式，如 VHD、VMDK 等。调查员可以利用镜像挂载工具辅助分析镜像文件中的数据。在一次关于恶意代码的应急响应服务中，你作为一名电子数据取证人员，需要携带一款磁盘镜像工具进行证据固定，同时需要使用一款镜像挂载工具将镜像文件挂载到要取证的文件系统中。请针对目前国内外具有镜像制作和镜像挂载功能的软件进行对比、评测，列出你认为比较理想的磁盘镜像和挂载工具，并说明理由。请根据如下结构撰写评测报告，需注意图文并茂。评测报告需要包括以下内容：

第一部分　磁盘镜像工具概述

(1) 为什么需要进行证据固定？

(2) 镜像文件的格式有哪些？

(3) 目前可用的磁盘镜像工具有哪些？给出名称、版本、厂家和工具概述。

(4) 测试环境和方案，包括运行环境、测试样本描述、使用的测试方法等。

(5) 测试过程和结果，说明原始磁盘大小、镜像格式、速度以及哈希结果是否一致。

第二部分　镜像挂载工具概述

(1) 什么是镜像挂载工具？镜像挂载工具的作用是什么？

(2) 镜像挂载工具有哪些？给出名称、版本、厂家和工具概述。

(3) 测试环境和方案。

(4) 镜像挂载工具的具体操作步骤(选一个工具重点描述即可)。

第三部分　测试结果和结论

给出总体意见。说明你在应急响应和取证工作中会携带并使用哪些工具。

本章参考文献

[1] CALLAGHAN P. Why Hash Values Are Crucial in Evidence Collection & Digital Forensics. Pagefreezer[EB/OL]. https://blog.pagefreezer.com/importance-hash-values-evidence-collection-digital-forensics.

[2] 刘浩阳. 电子数据取证[M]. 北京：清华大学出版社，2015.

[3] 喻海松. 刑事诉讼法修改与司法适用疑难解析[M]. 北京：北京大学出版社，2021.

[4] 公安部信息系统安全标准化技术委员会. 电子数据存储介质复制工具要求及检测方法：GA/T 754—2008[S]. 北京：公安部，2008.

[5] 公安部信息系统安全标准化技术委员会. 电子数据法庭科学鉴定通用方法：GA/T 976—2012[S]. 北京：公安部，2012.

[6] 公安部信息系统安全标准化技术委员会. 数字化设备证据数据发现提取固定方法：GA/T 756—2021[S]. 北京：公安部，2021.

[7] 公安部信息系统安全标准化技术委员会. 法庭科学远程主机数据获取技术规范：GA/T 1476—2018[S]. 北京：公安部，2018.

[8] 公安部信息系统安全标准化技术委员会. 法庭科学现场勘查电子物证提取技术规范：GA/T 1564—2019[S]. 北京：公安部，2019.

[9] 公安部信息系统安全标准化技术委员会. 法庭科学网站数据获取技术规范：GA/T 1478—2018[S]. 北京：公安部，2018.

[10] 司法部司法鉴定科学技术研究所. 电子数据证据现场获取通用规范：SF/Z JD0400002—2015[S]. 北京：司法部，2015.