江苏省律师电子证据的固定采集与展示业务操作指引

来源：中华全国律师协会信息网络与高新技术专业委员会委托江苏省律师协会电子商务与信息网络业务委员会

第一章　总　则

第一条　为指导律师正确、妥善处理在执业活动中所涉及的与电子证据有关的法律事务，帮助律师提高业务水平与办案质量，为当事人提供规范、高效、专业的法律服务，特制定本指引。

第二条　本指引所涉及的电子证据的固定采集与出示，是指律师根据《中华人民共和国律师法》第三十五条之规定，在为当事人提供民商事、行政法律服务（包括诉讼案件的代理或非诉讼法律事务的处理）中，对于与案情或代理事务有关的、以电子数据方式存在的相关信息、文件、资料等，按一定技术要求与程序，进行固定采集并运用的方式与方法。

第三条　律师办理刑事案件中，涉及到对电子证据固定采集的，建议律师通过申请人民检察院、人民法院收集、调取。律师对侦查机关、人民检察院、人民法院收集、调取电子证据，可依据本指引提出程序及方法上的建议及意见，也可以参考本指引对上述电子证据的真实性、合法性进行判断和质证。

第四条　律师在引用本指引时，应充分认识到电子证据的相关技术特点与特性。为此，在处理具体事务时，如因技术进步或其它因素，导致本指引的相关做法与实际情况不一致或不适用时，应及时咨询相关专业技术人员的意见，并根据自己的实际要求与经验，做出恰当的判断。

第五条　本指引所制定的内容作为律师在处理具体案件所涉及电子证据的固定采集与出示的执业行为参考。律师在处理上述事务中，不采取或不参考本指引所制定的内容，并不当然表明该律师实际采取的执业行为或方法存有瑕疵或不当。

第二章　电子证据概述

第六条　本章内容并非对电子证据进行理论上的探讨或研究，而是通过对电子证据的一般描述，来指导和规范律师对电子证据进行固定采集及展示的执业行为。

第七条　本指引所称电子证据（Electronic Evidence）是指能够证明相关法律事实或案件事实的、被作为证据使用的电子文件或电子数据。能够证明相关法律事实或案件事实是电子证据的重要法律特征。

第八条　上条所述电子文件（Electronic Records）是指基于电子信息技术生成的，以数字化形式存在于磁盘、光盘等数字存储设备，其内容可与载体分离，并可在其它同类或不同载体之间多次复制或转化的文件。

第九条　固定采集电子证据时，应注意下列电子文件的不同类型对固定采集技术手段的影响：

一、字处理文件，通过文字处理系统形成的文件，由文字、标点、表格、各种符号或其他编码文本组成。

所有这些软件、系统、代码连同文本内容一起，构成了字处理文件的基本要素。其中，文本内容通常成为电子证据。例如，.DOC 文档、.XLS 文档。

二、图形处理文件，通过专门的计算机应用软件系统，运行相应的辅助设计或辅助制造功能所得到的图形数据。通过图形人们可以直观地了解非连续性数据间的关系，使得复杂的信息变得清晰。例如，运用 Photoshop 软件、AutoCad 软件生成的图形文件。

三、程序文件，是由多条计算机命令集合在一起的电子文件，是程序源代码文件通过编译器翻译生成的电脑可以识别和运行的一种特殊的文件。在软件开发环境下，程序文件指的是源代码，如 ASP、C 等，在电脑使用人或用户环境下，程序文件通常指的是可以直接在电脑上运行的.EXE 文件。计算机软件就是由若干个程序文件组成的。

四、多媒体文件，是指计算机技术为基础，以计算机及其外部设备为中心，通过扫描识别、视频捕捉、音频录入等手段综合编辑而形成的多种媒体组合文件。媒体包括文本、图形、动画、动静态视频、音频等。

第十条　不同的分类方法与标准，可将电子证据分成不同的种类。本指引的

重点在于对基于计算机技术应用和互联网络技术应用中所出现的电子证据，如何进行固定采集与展示。

第十一条　电子证据通常存在于计算机的硬盘、U盘、磁（光）盘等移动存储设备。手机特别是具有计算机功能的智能手机作为电子证据的载体之一，反映或记录使用人的意思表示、行为的电子证据比其他载体中的电子证据更具有价值。

第三章　电子证据的固定与采集

第一节　电子证据的固定采集基本方法

第十二条　打印

对于可以直观或直接反映或证明案件事实的电子证据，可以直接将有关内容打印在纸张上的方式进行取证。打印后，可以按照提取书证的方法予以保管、固定，并注明电子证据打印的时间、数据信息在计算机中的位置（如存放于那个文件夹中等）或来源、取证人员等。

第十三条　拷贝

是将作为电子证据的电子文件，通过拷贝复制到U盘、移动硬盘或光盘中的方式。取证人员应当检验所准备的U盘，移动硬盘或光盘，确认没有病毒感染。拷贝之后，应当及时检查拷贝的质量，防止因保存方式不当等原因而导致的拷贝不成功或感染有病毒等。取证后，注明提取的时间并封闭。

第十四条　拍照、摄像

对于具备视听资料特征的电子证据，可以采用拍照、摄像的方法进行证据的提取和固定，以便全面、充分地反映证据的证明作用。此外，在电子证据取证过程中，对取证全程进行拍照、摄像，对被固定采集的电子证据的真实性具有一定的增强作用。

第十五条　制作司法文书

由执法机关对电子证据制作相应的检查笔录和鉴定。检查笔录是指对于取证证据种类、方式、过程、内容等在取证中的全部情况进行的记录。鉴定是专业人员就取证中的专门问题进行的认定，也是一种固定证据的方式。

第十六条　查封、扣押

申请执法机关对于涉及案件的电子证据的载体进行采取查封、扣押，将有关

载体置于执法机关保管之下。之后再对该电子证据进行分析、解读。

第十七条　公证

通过公证机构以证据保全公证的方式对有关电子证据进行公证。这是有效获取电子证据的便捷途径。

第十八条　数据解析

对于不能直接或直观的证明案件事实的电子证据，在确保数据真实的情况下，运用特定的软件工具，对相关数据进行分析、转化，使得其可以直观的形态为人们所认知或了解。

第十九条　恢复。

大多数计算机系统都有自动生成备份数据和恢复数据、剩余数据的功能。因此，当有关电子证据已经被修改、破坏的，可以通过对自动备份数据和已经被处理过的数据证据进行比较、恢复，获取电子证据，也可以使用一些专门的恢复性软件或专门设备来恢复、获取电子证据。

第二节　电子证据固定采集的注意事项

第二十条　条件允许情况下，建议由公证机关做为电子证据固定采集的主体。律师以代理人或公证委托人身份，只是对相关电子证据的固定采集进行目标、方法、步骤上的指导和要求。

律师应当注意：在司法实践中，即便经过公证的电子证据在证明效力上仍可能存有异议。

第二十一条　对电子证据固定采集的具体操作，建议由专业的技术人员或公证人员实际进行。

第二十二条　除非技术上必要，对电子证据进行固定采集的场所，建议一般应在公证机关或中立第三方的工作场所进行。

第二十三条　除非技术上必要，对电子证据固定采集所使用的计算机设备或其他数码设备，建议使用公证机关或中立第三方的设备。

第二十四条　来源于互联网的电子证据，须对证据的来源、域名、IP 等相关因素进行保存。孤立的网页文件，其真实性难以证明，证明效力很弱。

第二十五条　对电子证据固定采集过程中，应注意避免数据污染，从而影响相关电子证据的真实性。用于固定相关电子证据的载体应当是干净的、未受污染的。

第二十六条　在使用非第三方的计算机或电子设备进行电子证据的固定采集时，须由专业人员对该计算机及电子设备进行“清洁性检查”。

所谓“清洁性检查”是指对相关计算机或电子设备中的软件系统、功能、配置进行查看或固定，以确保通过该计算机或电子设备所获取的电子证据的真实性以及数据来源的唯一性。

第二十七条　如有可能，对于记录、存储电子证据初始形成的电子证据载体、设备、介质等，应当提存原物并随同电子证据一并固定采集。

第二十八条　借助某些专业的电子证据取证设备或软件，或者寻求中立的第三方提供的电子证据固定采集的相关专业技术服务，不失为对电子证据固定采集的一种有效途径。这有助于提高相关电子证据的证明力。

采取黑客手段等非法手段获取的电子证据，因其来源不具有合法性，不具有相应的证明效力。

第二十九条　鉴于电子证据的脆弱性和易篡改，应当采用适当的储存介质进行原始的镜像备份，用“镜像复制”的方法复制若干个副本。建议将其中的两个副本复制在只能写入一次的介质上（如非可擦写光盘），防止被提取到的电子证据意外被改变。

第三十条　以第三方所作的提取笔录形式将复制的时间、地点、复制的方法、处理人员、使用软硬件、复制过程等事项记录下来，以确保电子证据的合法性、真实性、关联性与完整性。

第三十一条　不得改变原始证据或原始数据。对于固定采集的电子证据进行鉴定和技术分析前，应当进行完整的备份，对备份的电子证据进行鉴定分析，不允许直接对原有存储介质直接进行技术操作。

第二节　来源于互联网络的电子证据

第三十二条　固定当前所使用的电子设备与计算机所处的网络环境是对来源于互联网络电子证据进行固定采集的前提步骤。

第三十三条　固定上条所述网络环境应当包括以下要素：

1、当前计算机连接互联网的方式：是通过局域网连接还是直接互联网；

2、在局域网环境下，相关的 IP 地址、网关设置；（如下图）

3、局域网的拓朴结构；

4、互联网的登录方式与连接方式（有线或无线、宽带或 ADSL 方式）；

5、通过局域网连接状态，主服务器与终端的权限分配与应用；

6、如当前所使用电子设备并非计算机（如智能手机等），需提供该电子设备的说明书或操作手册。

第三十四条　固定当前所使用的电子设备与计算机的自身系统配置文件（如下图）。这些文件包括但不限于：

1、当前电子设备与计算机的品牌、型号；

2、当前电子设备与计算机使用的软件：操作系统、应用程序；

3、当前计算机的硬件配置状况；

4、当前计算机系统中的哪些应用程序提供远程控制；

5、其他反映当前电子设备与计算机功能或性能的文件。

第三十五条　通过 IE 上网浏览之方式，从互联网上获取相关的电子证据，建议应事先了解域名及域名解析的相关知识。

中国互联网络信息中心（China Internet Network Information Center，简称 CNNIC，其网址为：http：//www.cnnic.net.cn/index.htm ）是经国家主管部门批准，行使国家互联网络信息中心的职责，负责管理维护中国互联网地址系统的管理和服务机构。

第三十六条　在 Windows 系列操作系统下，须运行查看本地计算机系统内的 host 文件，并对该 host 文件内容予以固定。对该文件内容的固定，能确定当前计算机访问的网站或获得之电子证据来源于互联网，确保电子证据来源的唯一性并进而保证相关电子证据的有效性与证明力。

第三十七条　不同系统的 host 文件存放路径如下：

1、WinXP/2003/Vista： C：\Windows\System32\Drivers\etc

2、WinNT/2000： C：\WINNT\System32\Drivers\etc

3、Win98/Me： C：\Windows

第三十八条　host 文件是根据 TCP/IP for Windows 的标准来工作的，它的

作用是包含 IP 地址和 Host name 主机名的映射关系，是一个映射 IP 地址和 Host name 主机名的规定，规定要求每段只能包括一个映射关系。根据 Windows 系统规定，在进行 DNS （域名系统 Domain Name System 的缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。）请求以前，Windows 系统会先检查自己的 Hosts 文件中是否有这个地址映射关系，如果有则调用这个 IP 地址映射，如果没有再向已知的 DNS 服务器提出域名解析。

第三十九条　在网络上访问网站，要首先通过 DNS 服务器把网络域名解析成 IP 地址后，计算机才能访问。也就是说 Hosts 的请求级别比 DNS 高。host 文件中，关于域名解析的优先次序为：本地硬盘-局域网-互联网。以访问 www.xxx.com 为例说明：

1）客户端首先检查本地 c：\windows\system32\drivers\etc\host 文件，是否有对应的 IP 地址，若有，则直接访问 WEB 站点，若无

2）客户端检查本地缓存信息，若有，则直接访问 WEB 站点，若无

3）本地 DNS 检查缓存信息，若有，将 IP 地址返回给客户端，客户端可直接访问 WEB 站点，若无

4）本地 DNS 检查区域文件是否有对应的 IP，若有，将 IP 地址返回给客户端，客户端可直接访问 WEB 站点，若无，

5）本地 DNS 根据 cache.dns 文件中指定的根 DNS 服务器的 IP 地址，转向根 DNS 查询；

6)根 DNS 收到查询请求后，查看区域文件记录，若无，则将其管辖范围内.com 服务器的 IP 地址告诉本地 DNS 服务器；

7）.com 服务器收到查询请求后，查看区域文件记录，若无，则将其管辖范围内.xxx 服务器的 IP 地址告诉本地 DNS 服务器；

8）.xxx 服务器收到查询请求后，分析需要解析的域名，若无，则查询失败，若有，返回 www.xxx.com 的 IP 地址给本地服务器；

9）本地 DNS 服务器将 www.xxx.com 的 IP 地址返回给客户端，客户端通过这个 IP 地址与 WEB 站点建立连接。

第四十条　确定一台计算机登录互联网的历史记录和状态，还可通过固定该计算机配置的网卡特定编号，结合网络服务提供商的服务器相关系统记录，确定

配置特定网卡编号的计算机登录互联网的历史记录和状态。

网卡特定编号，如同人的指纹一样，在全球范围内都是唯一的、不重复的。但需注意的是，网络服务提供商服务器上，关于特定编号网卡登录互联网的历史记录，其保存时间是有限的。

第四十一条　登录互联网后，打开 IE 浏览器，输入域名或 IP 地址，搜寻相关的信息，将搜寻到的信息保存在新建的文件夹中或存储介质中。所有这些操作均需同步记录及保存。

第四十二条　通过登录互联网固定采集相关来源于互联网的电子证据时，记录或保存所有操作步骤的方法通常有：

1、书面记录每个操作步骤及所获得的内容于纸质载体上；

2、对每个操作步骤所获内容进行截屏保存或打印至纸质载体上；

3、用其他电子设备对操作步骤进行同步摄像；

4、使用专用的屏幕录像软件对所有操作步骤及所获内容进行同步录像。（有关的屏幕录像软件可直接从相关的网站上下载使用。）

上述方法可以根据实际情况组合使用，但所获电子证据内容均应刻录在存储介质中（如 CD 光盘、U 盘等）。

第四十三条　注意使用互联网络资源，获得相关的电子证据或证据线索、信息。

1、工业和信息化部 ICP/IP 地址信息备案管理系统

http：//www.miibeian.gov.cn/CX/main.jsp

2、中国互联网络信息中心　http：//www.cnnic.net.cn/

3、中国万网 http：//www.net.cn/static/domain/?cid＝baidu_domain

来源于上述政府网站及中立的第三方网站的电子证据或信息通常具有较高的证明力。

第四十四条　在对计算机进行截屏过程中，需保持所截屏网页内容的完整性。如因纸张尺寸问题，不能将所截屏网页打印在同一页纸张上的，可用数页纸张连续截屏网页内容。避免截屏网页的内容缺失导致其证明力下降或丧失。

对网站网页首屏及网页次屏的截屏应当满足无缝衔接的要求。

第四十五条　经过第三方电子认证中心流转的计算机数据，具有较高的证明

力。对于此类证据的固定采集，建议通过一定的取证申请，由提供电子认证服务的网络服务提供商提供。

第三节　来源于互联网络的电子证据-电子邮件信息

第四十六条　电子邮件服务是互联网应用最为广泛的服务之一。对电子邮件信息而言，其邮件内容往往证明了一定的法律事实或行为，从此意义上说，电子邮件信息可视为证据中的书证。

第四十七条　对电子邮件信息的固定采集，除邮件内容外，对电子邮件信头的固定采集也同样重要。

第四十八条　一般情况下，电子邮件常用信头字段包括下列内容：

电子邮件常用信头字段表

字段名称描述字段名称描述

From 信件写信人 Date 信件创建日期

Sender 信件发信人 Received 信件 MTA 轨迹

Reply-to 发信回复地址 Return-path 发信人地址

To 信件主收信人 Subject 信件主题

Cc 信件辅收信人（抄送）Comments 关于信件的其他说明

Bcc 信件的密件抄送收信人 Keywords 信件主题关键字

Message-id 信件唯一标识符 Encrypted 加密信息

In-reply-to 信件被回复到 Resent-*重新分发时创建的字段

References 信件源 Content-length 信件长度

Status 由 MUA 插入标识是否信件状态

（是否新信件、已阅读、回复等）X-*信件扩展字段，由开发者创建的非标准字段

第四十九条　对电子邮件信息，建议通过公证机关以证据保全公证的形式予以固定采集。

第五十条　电子邮件信息除了保存在电子邮箱使用人的个人电脑终端上，还保存在提供电子邮件服务的网络服务提供者的服务器上。

第五十一条　在知悉电子邮箱（Email）地址，但无法掌握电子邮箱使用人计算机的情况下，可通过申请证据调取的方式向审理人民法院申请调查令，并依

此要求提供电子邮件服务的网络服务提供者提供相关的电子邮件证据。

第五十二条　如电子邮件服务来源于委托人或对方当事人自行设立的网站，需首先查明该网站所存放的物理服务器位置。

如该网站的服务器系租用电信服务器或由电信部门托管的服务器，可按第五十一条程序固定采集相关的电子邮件证据。

如该网站的服务器系委托人或对方当事人自行保管控制，可通过公证机关或审理人民法院通过证据保全之方式调取相关的电子邮件证据。

第五十三条　作为电子证据固定采集的预备措施，建议律师以恰当地方式提示当事人，在以电子邮件方式与相对人进行意思表示或进行商谈时，对接收到的电子邮件直接以邮件回复方式进行。如此，可动态记录双方意思表示的完整过程，也有助于确定相对人的真实身份。

第四节　来源于互联网络的电子证据-即时通信软件数据

第五十四条　网上聊天记录的内容是当事人法律行为或意思表示，以文字方式借助于电子形式的外在表现，具有动态证明有关法律事实、法律行为、当事人意思表示的特点。从证据形态上看，网上聊天记录集中体现了言词证据的某些特性。

第五十五条　固定采集网上聊天记录内容时，不仅应以双方个人电脑中的聊天记录为主体，还应包括即时通信软件使用人的个人资料、聊天好友资料。

第五十六条　鉴于现阶段在互联网上没有实行网络实名制，因此在固定采集此类电子证据时，应当扩大数据收集范围，尤其是反映聊天记录的用户网名与现实中自然人身份相对应的相关数据。

第五十七条　通过某一方电脑终端固定对方使用人网络身份与真实身份相对应的电子证据时，可以通过对方在互联网上的 ID、上网计算机的 IP 地址、在即时通信软件上登记的个人资料等方式单独或结合使用固定对方的真实身份这一事实。

必要时，通过网络聊天所获得的对方自认的真实身份也可以起到一定的证明作用。

第五十八条　从理论上看，行为人通过即时通信软件所产生的电子数据都会在有关的网络服务提供者提供的聊天服务器上中转、保存。但由于网上聊天系统

具有用户成员多、信息流量大等特点及时性相关规定，这些电子数据保存时间不低于60天。因此，对此类电子证据固定采集具有一定的时间要求。

第五十九条　美国微软公司（Microsoft）的即时通信软件MSN及腾迅公司（Tencent）的QQ是目前国内使用最广泛的两款即时通信软件，已形成了一个较为完善、具有相当规模的互联网即时通信体系。

第六十条　某些版本的QQ软件（如木子版QQ、珊瑚版QQ）以及其他显IP外挂程序可以在线监控对方的IP地址及使用的QQ版本，并对IP地址作出初步的物理位置判断。

第六十一条　除非有明确的方法或途径固定相关的操作内容，不建议利用即时通信软件中的文件即时传输功能来传递有关的法律文件、电子信息及电子数据。

第五节　来源于互联网络的电子证据-电子公告信息（BBS）

第六十二条　BBS的一般功能有信息发布、问题讨论、文件传输、联机交谈等。不同的BBS通常将这些功能划分为不同标题命名的“版面”。但无论如何，用户都需将传输内容上传到服务器，其他用户才有能进行访问。

第六十三条　一套完整的BBS系统由计算机硬件、软件和系统的管理者、用户共同组成。其中，硬件部分包括一台运行BBS系统程序的计算机（服务器）、连接系统与用户的设备以及用户个人电脑终端。软件部分包括系统和相应的通信程序。

第六十四条　BBS证据按存储地的不同，可以分为“存储于BBS服务器上的证据”和“存储于用户个人电脑终端上的证据”两种。具有证明力的BBS证据是存储于BBS服务器上的证据内容，这些数据包括信息发布者形成、上传和存储的数据以及由BBS服务器系统形成的数据两种， 均属于需要固定采集的电子证据内容。

第六节　来源于封闭计算机系统中的电子证据

第六十五条　本指引中所称封闭计算机系统指未连接局域网或互联网的计算机。储存在此类计算机中的、具有电子证据性质的计算机数据之载体主要是计算机硬盘。根据计算机数据产生的性质，可简单将其分为系统数据与用户数据两类。

第六十六条　Windows 系列操作系统和 UNIX 是最常见也是应用最广的两种操作系统。鉴于操作系统使用之广泛性，本指引仅涉及 Windows 操作系统中，相关电子证据的固定采集。

第六十七条　从技术上说，几乎 Windows 操作系统中的每一项事务都可以在一定程序上被审计。因此，获取各种系统日志是确定电子证据的必要步骤。

第六十八条　访问 Windows 操作系统维护的各种日志可以获得以下信息：

1、确定计算机在某一时间段内被使用和登录系统的用户；

2、跟踪登录者对特定应用程序的使用；

3、跟踪审核策略的变更，看是否有防御性的策略变化；

4、跟踪用户权限（如非法提高的访问权限）的变化，以及用户和组的变更。

第六十九条　查看注册表是获得当前计算机中，可能具有电子证据性质的系统数据的有效途径。

第七十条　在固定采集系统数据及用户数据时，为保护原始数据，确保证据的有效性不被破坏，通常情况下，采取以下三种方法进行数据备份，对系统进行完整复制：

1、利用磁盘镜像工具对移交的证据介质进行复制。

2、通过添加一个硬盘驱动器的方法创建映象。

3、通过网络发送映象。

无论以上述哪种方式固定采集系统数据，创建数据副本，都需要对原始驱动器和最后的映象文件执行数据完整性校验。

第七十一条　数据完整性校验可以通过专用的校验工具软件进行。建议使用专用的电子取证硬盘复制机（如 TALON、QUEST）进行硬盘复制。上述设备均支持 MD5 256 位校验功能，确保原始数据与复制数据的一致性。

第七十二条　在封闭的计算机系统中固定采集电子证据，尤其应注意检查并固定采集下列文件：

1、扩展名为.pst 的 Microsoft Outlook 电子邮件文件。

Windows 系列操作系统默认的存储路径为：Documents and Settings\\Local Settings\Application Data\Microsoft\Outlook ；

2、回收站中的文件；

3、扩展名为.tmp 的检查临时文件；

4、恢复被删除的文件，有相当多的工具软件如 Norton 可以恢复系统中被删除的文件；

5、Internet 历史记录；

第七节　来源于移动存储设备的电子证据

第七十三条　来源于移动存储设备的电子证据通常可分为两类：

1、保存在可移动的电磁或光学介质上的电子数据，如移动硬盘、CDROM 光盘等。此外，数码设备中使用的格式卡如 CD 卡、CF 卡、MS 记忆棒、手机中的 SIM 卡等也可以归入此类。

2、保存具备一定计算机功能的移动数字设备中的电子数据，如手机、PDA、车载 GPS 等。

第七十四条　对保存在可移动的电磁或光学介质（载体）上的电子数据，应当提取原物并将之作为证物使用。

第七十五条　由于原物是以其记载内容而非其自身作为证据使用。因此，可利用相应的硬件设备或软件工具导出或读取有关介质（载体）中的数据，并对导出或读取的数据进行分析。

第七十六条　对上述介质（载体）中的数据进行导出或读取的过程，建议通过公证机关或中立第三方进行并对全过程予以记录，以保证相关数据的真实性。

第七十七条　对于移动数字设备中的电子数据，如不具备提取保存原物之条件，应当按上条之要求与途径，对其中的电子数据进行固定采集。

第七十八条　在固定采集移动数字设备中的电子数据时，应将该设备品牌、型号、操作系统、使用说明书等内容作为环境数据一并固定采集。

第七十九条　固定采集使用手机产生的电子证据时，除了以手机为对象进行固定采集外，还可以通过该手机的通讯网络运营商（中国联通、中国移动、中国电信）进行相关电子证据的固定采集。

第八十条　固定采集通讯网络运营商所保存的手机使用产生的电子证据，建议通过以下两种途径：

1、通过互联网登录运营商的网上营业厅，查询并固定相关的电子证据信息

如通话记录、短信记录等等。同时，申请公证机关对此过程进行证据保全公证。

2、通过申请调查令的方式，向通讯网络运营商调取相关手机的通讯记录等数据或内容。

第八十一条　司法实践中，手机短信内容可作为证据使用已无争议。对手机短信内容的固定采集，建议通过公证机关对其进行证据保全的方式进行。

第八十二条　根据现行相关规定，手机号码的开通使用已实行实名制。但基于通讯网络运营商对用户通讯自由与个人隐私之保护，手机机主或使用人身份的确认，需要通过申请人民法院调查令之方式才能使固定采集的电子证据具有合法性。

第四章　电子证据的展示

第八十三条　电子证据作为一种新型的证据形式，要使其发挥证明相关法律事实、法律行为等案件事实的作用，须按照相关证据规则的要求进行证据展示。

第八十四条　在电子证据展示过程中，应充分考虑所掌握电子证据的种类、特征以及区别于其他类型证据的特点，采用科学的展示方法，以便其获得相应的证据证明效力。

第八十五条　展示的电子证据应当包括以下三个方面：

1、证据内容，即电子证据所包含的、可以用来证明某些案件事实的证据或材料。

2、附属信息，指证据内容数据产生、变更、消失的数据，如系统日志、访问时间、IP 地址、网站域名归属等。

3、环境数据，指支持电子证据的硬件及软件所产生的数据，如系统的版本数据、系统文档等。

上述三个方面如有缺失，则会直接影响电子证据的真实性、合法性、有效性，甚至导致电子证据不被采信。

第八十六条　由于电子证据的原始状态是一组电子数据（如计算机文件使用的是二进制数据。），需进行一定的程序还原才能显示其内容，并且显示或提取的都是文件的副本。通常情况下，通过以下方法来完成电子证据的展示：

1、通过计算机打印输出的方法；

2、通过计算机读取并处理移动存储介质内电子数据的方法；

3、将计算机系统本身作为证据，以模拟和演示特定条件下计算机的性能证明计算机系统本身的可靠性；

4、将计算机系统所带硬盘作为证据，通过计算机读取处理硬盘数据，展示硬盘内容作为证据展示；或，

5、上述四种方法的结合使用。

第八十七条　在电子证据展示过程中，建议以书面方式提交电子证据信息内容的目录、数据的组织方法、操作系统和应用程序以及正确读取查询信息内容的文档资料。

第八十八条　建议对电子证据的展示，在律师指导下，由专业技术人员进行操作和演示。必要时，由专业技术人员就相关技术问题直接作出说明和解释。

第八十九条　对于涉及技术问题较为专业、复杂的电子证据，建议在电子证据展示的同时，采取以下方法对电子证据中较为专业的技术部分进行解释与说明：

1、申请专家证人对电子证据中相对专业、复杂的部分进行解释与说明；

2、采取模拟演示的方法对电子证据进行解释与说明；

3、使用专用的司法分析软件如ENCASE、FTK （Forensic Toolkit），运用其中的证据监督链（Chain of Custody）信息来对电子证据尤其对其完整性与真实性进行解释与说明。

第五章　附　则

第九十条　本指引由中华全国律师协会信息网络与高新技术专业委员会委托江苏省律师协会电子商务与信息网络业务委员会制定。

第九十一条　本指引系根据现有的电子信息技术而拟定，并非强制性规定，仅供律师在实际业务中参考与借鉴。本指引将根据计算机技术、数字通讯技术及网络技术的不断发展，适时进行修订与补充。

第九十二条　本指引于二〇〇九年八月发布。

注：本指引只作为律师执业的参考。