ICS 13.31
CCS A92

MR

中华人民共和国市场监管行业标准

XX/T XXXXX—XXXX
代替 XX/T

市场监管电子数据取证规范

General specifications for electronic data forensics in market regulations

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局　　发 布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由国家市场监督管理总局提出并归口。

本文件起草单位：国家市场监督管理总局执法稽查局、标新科技（北京）有限公司、中检美亚（北京）科技有限公司。

本文件主要起草人：

市场监管电子数据取证规范

1 范围

本文件规定了市场监督管理行政执法电子数据取证的基本原则、取证前准备、取证工具、查封扣押原始存储介质、现场提取电子数据、网络在线提取电子数据、补充事项等内容。

本文件适用于市场监督管理行政执法活动中电子数据的取证工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 29361 法庭科学 电子数据文件一致性检验规程

ISO/IEC 27037 信息技术-安全技术-电子证据识别、收集、获取和保存指南

GA/T 754 电子数据存储介质复制工具要求及检测方法

GA/T 756 法庭科学 电子数据收集提取技术规范

GA/T 1070 法庭科学 计算机开关机时间检验技术规范

GA/T 1174 电子证据数据现场获取通用方法

GA/T 1564 法庭科学 现场勘查电子物证提取技术规范

GA/T 1568 法庭科学 电子物证检验术语

SF/Z JD0400001 电子数据司法鉴定通用实施规范

SF/Z JD0400002 电子数据证据现场获取通用规范

3 术语和定义

下列术语和定义适用于本文件。

3.1 电子数据 electronic data

与案件相关，以数字化形式存储、处理、传输，能够证明案件事实的信息。

3.2 存储介质 storage medium

具备数据信息存储功能的电子设备、硬盘、光盘、U 盘、记忆棒、存储卡、存储芯片等载体。

[来源:GA/T 1568 2.5]

3.3 完整性校验值

又称哈希值，是通过特定的散列算法把任意长度的输入数据变换成固定长度的输出值，用于标识电子数据的唯一性或完整性。

3.4 重案要案

金额巨大，社会影响恶劣，上级督办等。

3.5 易失性数据 volatile data

存在于网络中传输的数据或运行于计算机等电子设备中随电源切断或关机而消失的数据。

[来源:GA/T 1568 2.71]

4 取证基本原则

4.1 不损坏原则；

4.2 禁止使用原始证据；

4.3 记录所做的操作；

4.4 遵循相关的法律法规。

5 取证前准备

对于一般案件，携带 6.1、6.2 中的取证工具，在不破坏检材的情况下（特殊情况向直属领导报备后执行)，技术人员对现场存在的电子证据做到应取尽取。

对于重案要案，宜指派或者聘请专业人员协同取证并提前开会，制定计划。内容包括：案件类型、检材所在场所，大致设备数量，可能涉及的设备类型，同步时间地点，强调注意事项，需要携带的工具。

6 取证工具

6.1 通用工具

市场监督管理行政执法电子数据取证通用工具包括但不限于：

——数码照相机；

——数码摄像机或者执法记录仪；

——防静电手套；

——标签贴纸；

——封条；

——其他通用工具。

6.2 专用工具

市场监督管理行政执法电子数据取证专用工具包括但不限于：

——录屏工具；

——容量大小合适的取证专用空白存储介质以及转接只读接口和数据线；

——内存固定工具；

——硬盘复制工具；

——完整性校验工具；

——其他专用工具。

7 查封、扣押原始存储介质

7.1 在案件查办过程中，发现与案情相关的电子数据，能查封扣押原始存储介质的，应查封扣押原始存储介质，对存储介质做唯一性标识并制作笔录，拍照记录原始存储介质扣押前后的状态；

7.2　如有手机开机密码、云账号密码、隐私密码等，应当场了解清楚，填写在便签纸上贴在手机背面，将处理后的手机放入专用袋；

7.3　查封、扣押视频监控主机，应记录视频监控主机的品牌名称、监控存储介质（如储存卡、硬盘录像机或者专业的存储设备）等；

7.4　查封、扣押具有无线通信功能的原始存储介质，应对其进行信号屏蔽、信号阻断或者切断电源等；

7.5　查封、扣押原始存储介质，应当依照《中华人民共和国行政强制法》规定的程序进行，并当场交付实施行政强制措施决定书和清单，写明原始存储介质名称、编号、数量、规格型号及其来源等,由执法人员、持有人（提供人）签名或者盖章。

8　现场提取电子数据

8.1　计算机数据现场提取

8.1.1　开机状态提取

8.1.1.1　开启录像设备，确保对现场环境和计算机原始状态进行全程录像；

8.1.1.2　对有屏保密码的设备应现场获取或使用免安装设备和免系统注册软件解除密码，对获取的密码应验证并记录；

8.1.1.3　不能解除屏保密码时应采用切断电源的方式先关闭检材设备，并按照 8.1.2 进行提取；

8.1.1.4　记录检材的系统时间和北京时间；

8.1.1.5　手动提取易失性数据，如：内存数据固定、剪切板、正在运行的程序数据固定，常见的运行 程序主要有：

——加密容器：有加密容器需要在解密情况下优先镜像固定，如：TrueCrypt、VeraCrypt、BitLocker 等常见的加密工具下的加密情况（有条件的需要现场验证密码的正确性）；

——通讯软件：有已经运行登录的常见的通讯工具（如微信、QQ 、阿里旺旺、电子邮箱等），可以通过软件自带的消息导出功能导出聊天记录，没有导出功能的需通过截图工具进行关键聊天截图；

——最近打开的文件：有已经与运行的 Office 文档、广告、设计等创作软件直接截屏后，进行另存一份到存储介质；

——浏览器：通过浏览器设置选项的历史记录里查看后台登录记录，书签里查看收藏的网址，设置里查看记住的浏览器账号密码。（有条件的需要现场验证密码的正确性）。

8.1.1.6　若虚拟机、VPN 等特殊软件正在运行，应记录使用状态，并记录本环境所接入互联网中的 IP；

8.1.1.7　使用在线取证软件在线提取易失性数据时，保存在有唯一性编号的专用存储介质中，并计算、记录哈希值；

8.1.1.8　以上提取完成后，直接拔掉电源线；

8.1.1.9　有条件的可以绘制网络拓扑图；

8.1.1.10　封存检材。

8.1.2　关机状态提取

8.1.2.1　对现场进行拍照并录像，包括检材的铭牌，设备序列号等信息；

8.1.2.2　对检材进行唯一性编号；

8.1.2.3　对检材的连线及设备接口一对一进行唯一性编号；

8.1.2.4　对现场进行拍照或者录像，包括检材的品牌，唯一性编号等信息；

8.1.2.5　有条件的可以绘制网络拓扑图；

8.1.2.6　封存检材。

8.2　本地服务器数据现场提取

8.2.1　服务器现场取证时，应收集服务器的下列情况：服务器物理环境、服务器网络环境、服务器操作系统、服务器所有磁盘阵列类型；

8.2.2　服务器如使用磁盘阵列,需要关机取出存储硬盘单个固定数据,应提前记录好阵列磁盘顺序、相应配置等信息；

8.2.3　服务器如需要关机应按正常流程关机，避免部分程序在后期仿真分析时出现异常；

8.2.4　如遇到大容量阵列存储且不考虑数据恢复的情况,可使用类 PE 工具引导服务器对阵列中正常数据进行固定；

8.2.5　其他取证步骤与 8.1 一致。

8.3　手机数据现场提取

8.3.1　开启执法记录仪，确保对整个执法过程进行全程录像；

8.3.2　第一时间将手机开启飞行模式；

8.3.3　对现场进行拍照并录像，包括手机的品牌，唯一性特征（如 IMEI 号）等信息；

8.3.4　记录手机的系统时间和北京时间；

8.3.5　开启手机录屏或其他录像设备，确保能够拍到手机屏幕内容；

8.3.6　有手机开机密码、云账号密码、隐私密码等，有条件的当场了解清楚，并进行验证解锁；

8.3.7　进入手机后对手机内的关键页面进行截图，APP 安装包及数据进行复制导出，有条件的可以 使用手机取证设备快速提取截图、关键 APP 及用户数据；

8.3.8　将导出的截图、关键 APP 及用户数据进行哈希值计算；

8.3.9　将导出数据和哈希值一并存入取证专用空白存储介质。

8.4　专用设备数据现场提取

专用设备主要包含工控机、控制计算机和视频监控设备。

其中，工控机取证工作应聘请专业技术人员办理，控制计算机取证按 8.1 给出的步骤办理，视频监控取证按 8.4.1-8.4.5 步骤办理。

8.4.1　停止正在进行的录像操作；

8.4.2　对现场、视频监控的屏幕进行拍照并录像；

8.4.3　记录监控录像机的系统时间和北京时间；

8.4.4　查找录像中的可以作为关键的录像文件，条件允许的情况下应继续查找日志文件进行导出；

8.4.5　对录像文件和日志文件进行复制，并计算哈希值后存储到携带的取证专用空白存储介质，并在存储介质上贴上标签加以说明。

9　网络在线提取电子数据

9.1　网络在线取证

9.1.1　计算机远程取证查看要点应包括：网站的 ICP 备案信息（确认网站普通人可以访问）、网站关

于公司的信息、经营人信息；域名 Whois 信息，阿里云腾讯云信息；网站会员名单、回扣计算、数据库数据等；

9.1.2　实施网络在线电子数据取证前，应对用来提取电子数据的计算机系统、设备的硬件、软件环境进行检测，确保完整、可靠，处于正常可运行状态；

9.1.3　开始录屏：在取证计算机上运行屏幕录像软件开始录屏，同时对提取操作现场使用外置相机拍照或者摄像机对整个操作过程进行录像；

9.1.4　校对时间：浏览器搜索北京时间进行时间校准；

9.1.5　全盘杀毒：使用杀毒软件、安全卫士进行全盘查杀（以保证取证计算机未受病毒和木马感染入侵）；

9.1.6　清除浏览器缓存：在 IE 浏览器的 Internet 选项下的“常规”选项中选择删除“浏览历史记录”并删除默认网址，输入“about:blank”或者使用组合快捷键 Ctrl+Shfit+Delete 调出清除页面；

9.1.7　关闭浏览器代理：在“连接”选项中点击“局域网”设置（以保证取证电脑没有连接网络代理）；

9.1.8　检查 host 记录：用记事本打开检查取证电脑 hosts 文件，注释或者删除缺省以外的记录，停留 3 秒；

9.1.9　检查 IP 地址：在 cmd 命令窗口输入“ipconfig/all”查看本地电脑 IP 地址；

9.1.10　检查网络连通性：在命令窗口输入“ping 具体网站”；

9.1.11　检查网络路由：在命令窗口输入“tracert 具体网站”；

9.1.12　固定证据，登录网站后台对网站关键信息进行截图，有条件的可以进行全量数据导出包括网站文件夹、数据库、日志、输入输出产品存放的文件夹；

9.1.13　计算哈希值：将导出的文件打包成 zip 包，进行哈希值计算并保存值；

9.1.14　再次校对时间：浏览器搜索北京时间进行时间校准；

9.1.15　关闭录屏，计算录屏的哈希值并保存；

9.1.16　最后需要将提取的数据和哈希值一并填写到电子数据提取笔录中。

9.2　手机云端数据取证

9.2.1　将用于取证的手机卸载可能引起冲突的软件或者修改可能引起兼容问题的设置（有条件的可进行恢复出厂操作)，并查看手机 IMEI 值等：

9.2.2　打开手机录屏软件、浏览器百度北京时间进行时间校准，安装涉案 APP 客户端，登录之后对各页面点击查看，进行截图，导出能导出的数据，再次校对时间；

9.2.3　有条件的登录已付费的存证云平台，将取证截屏保存的文档、手机录屏文件、申请时间戳，并与源文件进行验证。

10　补充事项

10.1　在现在提取易失性数据之前不应关闭已经打开的电子设备，有屏保密码且无法解除的除外。

10.2　应立即终止操作系统正在进行的整理硬盘、格式化硬盘、删除文件、重装操作系统等操作。

10.3　所有扣押的电子设备必须统一编排唯一性标识，所有提取的电子数据必须计算哈希值。

10.4　对于操作难度大的可以使用专业的取证软件，或者聘请有专门知识的人员现场辅助执法人员进行收集、提取。

10.5　取证完成后按要求制作电子数据证据提取笔录（笔录包含执法现场情况的，可不单独制作现场检查笔录）、证据提取单，现场行政相对人签字确认。

10.6　不得将生成、提取的电子数据证据存储在原始存储介质中。

10.7　对于有屏保密码或者其他需要密码进入的情况，需要第一时间与行政相对人沟通，获取密码，然后清除或更改密码，并在电子数据证据提取笔录记录该操作。

10.8　对于结案后所有的电子数据取证证据，均应刻盘，并按照要求归档保存。

10.9　对于采取行政强制措施的设备，电子取证完成后，应及时解除行政强制措施，归还行政相对人。