司　法　鉴　定　技　术　规　范

SF/Z JD0400002——2015

电子数据证据现场获取通用规范

2015-11-20 发布　　2015-11-20 实施

中华人民共和国司法部司法鉴定管理局　发布

目　　次

前　言

本技术规范按照 GB/T 1.1-2009 给出的规则起草。

本技术规范由司法部司法鉴定科学技术研究所提出。

本技术规范由司法部司法鉴定管理局归口。

本技术规范起草单位：上海辰星电子数据司法鉴定中心。

本技术规范主要起草人：雷云婷、崔宇寅、张颖、郭弘、黄道丽。

本技术规范为首次发布。

电子数据证据现场获取通用规范

1 范围

本技术规范规定了电子数据鉴定中电子数据证据现场识别、收集、获取和保存的通用方法。

本技术规范适用于电子数据鉴定中电子数据证据现场识别、收集、获取和保存。

2 规范性引用文件

下列文件对于本技术规范的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本技术规范。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本技术规范。

SF/Z JD0100000－2012 电子数据司法鉴定通用实施规范

3 术语和定义

SF/Z JD0100000－2012 电子数据司法鉴定通用实施规范中界定的以及下列术语和定义适用于本技术规范。

3.1

随机存取内存转储 Random Access Memory dump (RAM dump)

将随机存取内存（RAM）中的部分或者全部数据转存到某种类型的存储介质中。

3.2

逻辑文件 Logical files

用户所观察到的文件组织形式，是可以直接处理的数据及结构。

3.3

潜在电子证据 Potential Digital Evidence

所有与案件相关的电子数据证据。

3.4

易失性数据 Volatile Data

容易改变或消失的数据，如内存数据。

4 原则

SF/Z JD0100000－2012 电子数据司法鉴定通用实施规范所确立的原则适用于本技术规范。

5 步骤

5.1 制定方案

在进行电子数据证据现场获取之前，需分析案情并根据具体情况制定详细的方案，包括：

a) 明确现场获取的目的和范围；

b) 明确参加现场获取的人员，需明确分工，落实责任；

c） 明确进行现场获取需携带的移动仪器设备；
d） 明确现场获取采用的方法和步骤；
e） 明确现场获取的顺序；
f） 明确现场获取操作可能造成的影响。

5.2 记录现场

现场取证人员应在到达现场后，立即对现场状况通过拍照或录像等的方式进行记录并予以编号保存，以便需要时可以进行验证或重建系统。

5.3 现场静态获取

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获取（封存），方法如下：

a） 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电子设备；
b） 封存前后应当拍摄或者录像被封存电子设备和存储介质并进行记录，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；
c） 对系统附带的电子设备和存储介质也应实施封存。

5.4 现场动态获取

对于运行中的系统，应进行电子数据证据的动态获取，其中又具体分为易丢失数据的提取和固定、在线获取以及电子设备和存储介质的封存三个部分。

5.4.1 易丢失数据的提取和固定

易丢失数据的提取和固定应遵照以下步骤：

a） 固定保全内存数据，特别是以下数据：
   1） 打开并未保存的文档；
   2） 最近的聊天记录；
   3） 用户名及密码；
   4） 其他取证活动相关的文件信息。
b） 获取系统中相关电子数据证据的信息，包括：
   1） 存储介质的状态，确认是否存在异常状况等；
   2） 正在运行的进程；
   3） 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 信息，防火墙配置等）；
   4） 尚未存储的数据；
   5） 共享的网络驱动和文件夹；
   6） 连接的网络用户；
   7） 其他取证活动相关的电子数据信息。
c） 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。

5.4.2 在线获取

在线获取应在现场不关闭电子设备的情况下直接分析和提取电子系统中的数据，包括：

a） 打开的聊天工具中的聊天记录；

b) 打开的网页；
c) 打开的邮件客户端中的邮件；
d) 其他取证活动相关的电子数据信息。

5.4.3 电子设备和存储介质的封存

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，对系统是否需关闭作出判断并采取相应的措施。其中，对于已经关闭的系统的处理方式参照 5.3。

对于不能关闭的电子设备和存储介质，应遵循以下几点：

a) 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；
b) 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；
c) 封存前后应当拍摄或者录像被封存电子设备和存储介质并进行记录，照片或者录像应当从各个
d) 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。

5.5 电子数据证据的固定保全

从现场获取的上述所有电子数据证据需遵照以下几个方式进行固定保全：

a) 完整性校验方式：计算电子数据和存储介质的完整性校验值，并进行记录；
b) 备份方式：复制、制作原始存储介质的备份，并依照 5.3 规定的方法封存原始存储介质；
c) 封存方式：对于无法计算存储介质完整性校验值或制作备份的情形，应当依照 5.4.4 规定的方法封存原始存储介质，并记录不计算完整性校验值或制作备份的理由；
d) 保密方式：潜在电子数据证据的保密是一个要求，无论是业务要求或法律要求（如隐私）。潜在电子数据证据应以确保数据机密性的方式保存。

6 记录

电子数据证据现场获取的过程中，记录应贯穿整个过程:

a) 记录可以用摄像、截屏、拍照、编写文档等方式存放于任何一种存储介质中；
b) 对可能存在证据数据的电子数据存储介质进行拍照，编号并贴上标签标识；
   1) 对现场状况以及提取数据、保存数据的关键步骤进行录像；
   2) 对电子数据证据信息的属性、状态以及其他信息进行详细记录。
c) 从现场获取的电子数据证据，应记录该电子数据的来源和提取方法；

现场获取检查结束后，应当及时记录整个工作过程。

7 注意事项

在电子数据证据现场获取中，应注意以下事项：

a) 不得将生成、提取的数据存储在原始存储介质中；
b) 不得在目标系统中安装新的应用程序。如果因为特殊原因，需在目标系统中安装新的应用程序的，应当记录所安装的程序及其目的；
c) 应当详细、准确记录实施的操作以及对目标系统可能造成的影响。