司　法　鉴　定　技　术　规　范

SF/Z JD0403003——2015

计算机系统用户操作行为检验规范

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

本技术规范旨在确立电子数据司法鉴定实验室进行计算机系统用户操作行为检验应当遵循的技术方法和步骤等方面的要求，确保相关鉴定活动的规范有序。

本技术规范按照 GB/T 1.1-2009 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。

本技术规范由司法部司法鉴定科学技术研究所负责起草。

本技术规范主要起草人：施少培、杨旭、李岩、卢启萌、卞新伟、陈晓红、奚建华、孙维龙、曾锦华。

计算机系统用户操作行为检验规范

1 范围

本技术规范规定了计算机系统用户操作行为检验的技术方法和步骤。

本技术规范适用于电子数据鉴定中的计算机系统用户操作行为检验。

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 JD0400001－2014 电子数据司法鉴定通用实施规范

SF/Z JD0402001－2014 电子邮件鉴定实施规范

3 术语和定义

SF/Z JD0400001－2014 电子数据司法鉴定通用实施规范所确立的以及下列术语和定义适用于本技术规范。

3.1

用户操作行为 User Behavior

用户使用计算机系统的特定行为，如登录/登出、接入外部设备、文件操作、打印、软件使用、浏览网页、即时通讯、收发电子邮件等。用户操作行为分为正在进行的行为和已经发生的行为。

3.2

操作痕迹 Operation Trace

存在于日志、注册表、临时文件、配置文件、数据库等区域，可以全部或部分反映用户操作行为过程的数据。

4 检验步骤

4.1 了解相关情况

4.1.1 了解检材的使用情况，如用户信息、系统状态、可能的操作行为等。

4.1.2 如检材有登录口令或加密密钥保护，了解口令或密钥信息，并获得使用授权。

4.2 固定保全

4.2.1 对检材进行惟一性标识。

4.2.2 对检材进行拍照或录像，记录其特征。

4.2.3 当检材为开机状态时：

a) 对检材屏幕的显示内容进行拍照或录像；

b) 必要时提取检材内存数据并计算哈希值；

c） 必要时对检材存储介质中需要的数据进行备份，并计算哈希值；
d） 采用适当工具和方法对检材进行在线分析，并对检材中运行的程序及进程/线程进行分析和保全。

4.2.4 当检材为关机状态时：

a） 对具备条件的检材进行完整备份，并进行校验，之后使用备份数据进行检验；
b） 对于无法进行完整备份的检材，采用适当的工具和方法启动计算机系统，对需要的数据进行备份，并计算哈希值；
c） 必要时在只读条件下进行开机检验，并做好相关记录。

4.3 搜索和恢复

根据检验需要，搜索、恢复保存在检材中的相关文件和数据。

4.4 检验和分析

根据检材具体情况，视检验需要对下列全部或部分内容进行检验和分析。

4.4.1 登录/登出行为检验

a） 分析系统日志、应用程序日志及系统安全日志等日志文件中与用户登录/登出相关的记录；
b） 分析注册表中用户键值中的信息，如用户最后一次登录时间、最后一次登录失败时间等；
c） 在系统中其它位置查找与登录/登出相关的信息，如系统中文件的修改时间、防病毒软件的启动/关闭记录等。

4.4.2 接入外部设备行为检验

a） 分析系统驱动安装日志中与设备相关的数据；
b） 分析注册表中与设备相关的数据；
c） 分析系统中的文件与外部设备中的文件的相似性及复制关系；
d） 对于存在自动备份机制的外部设备（如手机），分析备份在计算机系统中的数据。

4.4.3 文件操作行为检验

a） 分析文件的属性信息；
b） 分析文件的元数据信息；
c） 分析文件操作形成的临时文件、备份文件、快捷方式等；
d） 分析文件在相关软件及系统中的最近打开记录；
e） 对于被删除的文件，分析其状态、位置及内容。

4.4.4 打印行为检验

a） 分析系统中安装的打印机驱动程序；
b） 恢复并分析打印临时文件，如 SHD、SPL 及 TMP 文件；
c） 查找打印源文件，针对特定类型的源文件（如 Word 文档），分析其中的打印时间。

4.4.5 软件使用行为检验

a） 分析系统中软件文件的属性信息；
b） 分析软件运行时生成的配置文件、临时文件及其属性信息；
c） 分析软件的日志信息；

d) 分析软件在系统中其它位置（如注册表、系统还原点、系统镜像、最近打开文档等）留下的信息；
e) 对于含有数据库的软件，对数据库中的数据进行分析。

4.4.6 浏览网页行为检验

a) 根据网页浏览器类型和版本，查找其历史数据保存位置；
b) 分析网页浏览历史数据，如地址栏网址输入记录、网址重定向记录、网页浏览历史记录等；
c) 分析与被浏览网页相关的图片、文档、压缩包、Cookies、脚本等信息；
d) 查找并分析系统中与被浏览网页相关的其它文件，如收藏夹、保存的网页、下载的文件等；
e) 条件允许的情况下获取并分析位于服务器上的相关记录。

4.4.7 即时通讯行为检验

a) 查找系统中安装的即时通讯软件及其数据文件；
b) 分析客户端软件版本、用户账号等信息及数据文件的属性信息；
c) 分析数据文件中的聊天记录等信息；
d) 查找并分析通过即时通讯传输的图片、文档、多媒体文件等信息；
e) 条件允许的情况下获取并分析即时通讯交互中另一方的数据；
f) 条件允许的情况下获取并分析位于服务器上的相关记录。

4.4.8 电子邮件收发行为检验

a) 查找系统中安装的电子邮件客户端软件及其数据文件；
b) 根据客户端类型分析数据文件中的电子邮件及其相互之间的关联；
c) 在系统中搜索其它与需检电子邮件相关的信息；
d) 对于通过网页电子邮件服务收发的电子邮件，按照浏览网页行为进行检验；如能获得授权，参照SF/Z JD0402001－2014电子邮件鉴定实施规范保全并分析；
e) 条件允许的情况下获取并分析电子邮件往来中另一方或其他收件（抄送）方的电子邮件；
f) 条件允许的情况下获取并分析位于服务器上的相关记录。

4.5 注意事项

4.5.1 计算机系统中的时间信息与真实时间并非完全一致，检验中应注意系统时间与实际时间的差值，并分析人为修改、失电等原因造成的系统时间改变。
4.5.2 对于加密的数据，检验前应先对其进行解密。
4.5.3 在查找操作痕迹时，应注意搜索、恢复的全面性。
4.5.4 注意查找并分析检材中多处可以互相印证的操作痕迹。
4.5.5 注意查找并分析与操作行为相关的存在于第三方的数据。
4.5.6 对于检验中发现的一些存疑现象，可以搭建类似的环境进行实验重现，判断其性质。

5 检验记录

与鉴定活动有关的情况应及时、客观、全面地记录，保证鉴定过程和结果的可追溯。检验记录应反映出检验人、检验时间、审核人等信息。检验记录的主要内容有：

a) 有关合同评审、变更及与委托方的沟通等情况；
b) 检材固定保全情况，包括检材照片或录像、检材的哈希值等；
c) 检验设备和工具情况；

d) 检验过程和发现；
e) 对检验发现的分析和说明；
f) 其他相关情况。

6 检验结果

6.1 计算机系统用户操作行为检验结果应根据检验要求对检验对象、检验范围、检验所得进行客观、概括的描述。

6.2 对于尚不能明确计算机系统用户操作行为的，可出具无法判断结论并说明原因。