司　法　鉴　定　技　术　规　范

SF/Z JD0402004——2018

电子文档真实性鉴定技术规范

Guideline for forensic authentication of digital document

2018-11-08 发布　　2019-01-01 实施

中华人民共和国司法部公共法律服务管理局　发布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　鉴定步骤 1
5　记录要求 2
6　鉴定意见 2

前　言

本技术规范按照GB/T 1.1-2009给出的规则起草。

本技术规范由司法鉴定科学研究院提出。

本技术规范由司法部公共法律服务管理局归口。

本技术规范起草单位：司法鉴定科学研究院和上海交通大学。

本技术规范主要起草人：施少培、杨旭、李岩、卢启萌、曾锦华、郭弘、陈晓红、卞新伟、邱卫东、黄征。

本技术规范为首次发布。

电子文档真实性鉴定技术规范

1 范围

本技术规范规定了电子文档真实性鉴定的鉴定步骤、记录要求及鉴定意见。

本技术规范适用于司法鉴定/法庭科学领域中的电子文档真实性鉴定。

2 规范性引用文件

下列文件对于本文件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文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 29360 电子物证数据恢复检验规程

GB/T 29362 电子物证数据搜索检验规程

SF/Z JD0400001-2014 电子数据司法鉴定通用实施规范

SF/Z JD0403003-2015 计算机系统用户操作行为检验规范

3 术语和定义

SF/Z JD0400001-2014界定的以及下列术语和定义适用于本文件。

3.1

电子文档 digital document

文字处理软件生成的以数字形式存在的文件。

3.2

电子文档真实性鉴定 forensic authentication of digital document

对电子文档的形成过程进行分析，判断其修改情况。

4 鉴定步骤

4.1 准备

了解检材文档形成过程，并收集生成、存储、编辑、浏览、打印检材文档的电子设备或其存储介质。

4.2 固定和保全

4.2.1 对检材文档的物理载体进行唯一性标识并拍照。

4.2.2 当能够获得生成检材文档的存储介质时，制作其电子数据副本并计算哈希值。

4.2.3 当无法获得生成检材文档的存储介质时，对检材文档进行提取并计算哈希值。

4.3 搜索和恢复

对获取的存储介质电子数据副本，按照GB/T 29360及GB/T 29362的要求搜索、恢复其中的检材文档及与检材文档相关的数据。

4.4 检验和分析

根据检材文档具体情况，视需要对下列全部或部分内容进行检验和分析：

a) 对检材的操作系统进行检验，分析时间基准是否经过修改；
b) 对检材的文件系统进行检验，分析针对检材文档及相关文档的操作记录，包括但不限于 NTFS 日志、页面文件、休眠文件、卷影副本、交换数据流等；
c) 对与检材文档相关的应用程序进行检验，可按照 SF/Z JD0403003-2015 章节 4.4.5 的要求分析软件使用记录等信息；
d) 对检材中的打印记录进行检验，可按照按照 SF/Z JD0403003-2015 章节 4.4.4 的要求分析检材文档的打印记录等信息；
e) 对检材文档的数字签名情况进行检验，分析数字签名的完整性，解析并呈现数字签名所含信息；
f) 对检材文档的存储位置进行检验，包括目录结构及存储介质中的物理位置；
g) 对检材文档的文件属性及元数据信息进行检验，分析其中的创建时间、最后修改时间、访问时间、MFT 更新时间、最后打印时间、作者、最后保存者、编辑次数等信息；
h) 对检材文档的内容数据进行检验，分析其正常状态下未显示的内容；
i) 对与检材文档相关的临时文件进行检验，分析相互之间的关系；
j) 对系统注册表进行检验，分析文件访问记录等信息；
k) 对与检材文档相关的其它文件或数据进行检验，分析相互之间的关系。如包含相同或相似关键词的文件、创建或修改时间相同或相近的文件等。

4.5 综合分析

根据上述检验结果，对检材文档进行综合分析，应注意以下内容：

a) 尽可能多角度对检材文档及相关数据进行分析，以形成相互之间的印证关系；
b) 有些异常情况可能是软件缺陷等原因造成，应对其成因进行分析；
c) 必要时通过模拟实验，对检材文档的存疑特性进行分析；
d) 对检材文档数据与其形成过程陈述是否存在矛盾进行分析。

5 记录要求

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性。检验记录应反映出检验人、检验时间、审核人等信息。

6 鉴定意见

根据综合分析结果，对检材文档的形成过程及修改情况进行客观描述。信息不充分的，可出具无法判断的鉴定意见。