

司法鉴定技术规范

SF/Z JD0402002—2015

数据库数据真实性鉴定规范

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.....	I
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：司法部司法鉴定科学技术研究所、上海交通大学和贵州天剑司法鉴定中心。

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

数据库数据真实性鉴定规范

1 范围

本技术规范规定了数据库数据真实性鉴定的步骤和方法。
本技术规范适用于电子数据鉴定中数据库数据的真实性鉴定。

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。

GB/T 5271.17—2010 信息技术词汇第 17 部分:数据库
SF/Z JD0400001—2014 电子数据司法鉴定通用实施规范

3 术语和定义

下列术语和定义适用于本技术规范。

3.1

数据库 **database**

支持一个或多个应用领域，按概念结构组织的数据集合，其概念结构描述这些数据的特征及其对应实体间的联系。

3.2

数据库管理系统 **database management system (DBMS)**

基于硬件与软件，用于定义、建立、操纵、控制、管理和使用数据库的系统。

3.3

数据库应用系统 **database application system (DBAS)**

在数据库管理系统的支持下建立的计算机及其他应用系统。

3.4

数据库数据文件 **database file**

与数据库数据相关的文件，包含数据库数据表文件、数据库配置文件及数据库日志文件等，如 SQL Server 的.mdf 和.ldf 文件、Oracle 的.ora 文件等。

4 鉴定步骤

4.1 准备

- 4.1.1 了解待检数据库的开发、使用和维护等情况。
- 4.1.2 了解待检数据库的安全管理、权限配置等相关情况。
- 4.1.3 了解待检数据库的版本更新、升级等情况。
- 4.1.4 了解待检数据库备份情况，如备份的频次、备份文件的存放位置、最后一次备份时间等。

4.2 固定和保全

- 4.2.1 条件允许情况下，对运行待检数据库的系统进行拍照或录像。
- 4.2.2 条件允许情况下，对待检数据库所在的存储介质进行完整性备份。
- 4.2.3 无法进行完整性备份的，可直接对数据库系统中的所需文件或数据进行提取。

注1：提取过程应注意保持数据库数据的完整性，避免改变数据库结构及添加、修改、删除数据库数据。

注2：无法进行完整性备份的，提取过程应进行全程录像。

4.3 搜索和恢复

搜索、恢复与待检数据库相关的存储介质中的数据库数据文件及数据。

4.4 检验和分析

- 4.4.1 对数据库数据文件、备份文件、日志文件及其它相关文件的属性进行检验。
- 4.4.2 通过数据库管理系统分析数据库中数据表、数据字段与数据库应用系统所显示数据的对应关系。
- 4.4.3 分析数据库数据结构及数据是否存在异常。
- 4.4.5 分析数据库数据的时间顺序是否存在矛盾，重点关注含有时间信息的数据表。
- 4.4.6 分析数据库日志内容及与数据库数据是否存在矛盾。
- 4.4.7 分析数据库备份与数据库数据是否存在矛盾。
- 4.4.8 分析数据库数据的硬拷贝（如从数据库应用系统获得的纸质打印件）与数据库数据是否存在矛盾。
- 4.4.9 分析数据库的用户权限授予及变更情况。
- 4.4.10 分析其它可能与检材数据库形成印证关系的数据。

4.5 注意事项

- 4.5.1 应尽可能多角度对数据库数据进行检验，以形成相互之间的印证关系。
- 4.5.2 有些异常情况可能是数据库应用系统的缺陷、版本升级或者数据库使用者误操作等原因造成，应对其成因进行综合分析。
- 4.5.3 对于检验发现的存疑情况可通过实验进行分析。
- 4.5.4 注意分析数据库数据与其形成过程陈述是否存在矛盾。

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。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，包括照片、录像及备份数据和提取数据的哈希值等；
- c) 检验设备和工具使用情况；
- 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 鉴定意见

根据检验发现，对待检数据库中的数据是否经过修改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。
