ICS 13.310
A 92

GA

中华人民共和国公共安全行业标准

GA/T ××××—××××

法庭科学 MS SQL Server 数据库日志检验技术规范

Forensic sciences—Technical specifications for examination of MS SQL Server database logs

××××-××-××发布　　××××-××-××实施

中华人民共和国公安部 发布

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

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这些专利的责任。

本标准由全国刑事技术标准化技术委员会电子物证检验分技术委员会（SAC/TC 179/SC 7）提出。

本标准由全国刑事技术标准化技术委员会（SAC/TC 179）归口。

本标准起草单位：中国刑事警察学院物证鉴定中心、公安部物证鉴定中心。

本标准主要起草人：赵广晔、刘奇志、秦玉海、汤艳君、马贺男、高洪涛、徐国天、楚川红。

法庭科学 MS SQL Server 数据库日志检验技术规范

1 范围

本标准规定了MS SQL Server数据库日志检验方法。

本标准适用于法庭科学领域中的电子物证检验。

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 29360-2012 电子物证数据恢复检验规程

GB/T 29362-2012 电子物证数据搜索检验规程

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据库日志 database log

记录对数据库进行的增加、删除、修改、查看等操作以及操作结果消息的文件，包括事务日志、错误日志等。

3.2

错误日志 error log

记录数据库启动、运行或停止过程中产生的各类信息的文件。

3.3

事务日志 transaction log

记录所有事务以及每个事务对数据库所做修改的事件信息的文件。

3.4

数据库管理系统 database management system

一种操纵和管理数据库的大型软件，用于建立、使用和维护数据库。

4 仪器设备

4.1 硬件

存储介质、保全备份设备、电子物证检验工作站。

4.2 软件

4.2.1 操作系统：Windows 等。

4.2.2 软件工具：数据库管理系统软件、数据库日志分析软件。

5 操作步骤

5.1 检材编号

对送检的检材进行唯一性编号。

5.2 检材拍照

对送检的检材加上唯一性编号进行拍照。

5.3 检材保全备份

对具备保全条件的检材进行保全备份。

5.4 检验

5.4.1 病毒查杀

启动杀毒软件对电子物证检验工作站系统进行杀毒。

5.4.2 数据库日志提取

提取数据库日志时应提取包括事务日志和错误日志在内的全部数据库日志，提取过程应按照以下步骤进行：

a) 将检材（若已保全，使用保全的存储设备）通过只读方式接到电子物证检验工作站；
b) 在数据库系统规定的默认路径下提取数据库日志文件；或仿真运行检材中的操作系统，使用数据库管理系统提取数据库日志；
c) 对于已被删除的日志文件，依据GB/T 29360-2012、GB/T 29362-2012进行数据恢复、搜索检验。

5.4.3 数据库日志检验

使用数据库日志分析软件对提取出的数据库日志进行查看、分析，得出检验结果。

5.4.4 结果保存

将检出数据存储在专用存储介质中并计算哈希值。

6 检验结果的表述

检验结果表述符合以下规定：

a) 检验结果分为检出、未检出、不具备检验条件三种；
b) 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、有针对性的描述；
c) 结果表述应包含检材编号、检出情况、检出数据文件或保存检出数据介质哈希值、保存检出数据介质编号等必要信息。

7 附则

7.1 在检验过程中应做检验记录。

7.2 在检验过程中，不应改变检材中的数据。

7.3 应对送检的检材做好防水、防磁、防静电和防震保护。