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 Linux 操作系统日志检验技术规范

Forensic sciences—Technical specifications for examination of Linux operating system 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：罗文华、汤艳君、秦玉海、徐国天、高扬、马贺男、楚川红。

法庭科学 Linux 操作系统日志检验技术规范

1 范围

本标准规定了Linux操作系统日志检验的方法。

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

GA/T 1071-2013 法庭科学电子物证Windows操作系统检验技术规范

3 术语和定义

GB/T 29360-2012、GA/T 1071-2013界定的以及下列术语和定义适用于本文件。

3.1

Linux操作系统日志 Linux operating system log

由Linux操作系统进程syslog记录的事件信息。

3.2

日志配置文件 log configuration file

用于记录日志信息来源、信息级别及存储位置的文件。

3.3

日志管理文件 log management file

用于说明系统管理日志文件方式的文件。

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、Linux 等。

4.2.2 软件工具：电子数据取证综合分析软件、Linux 操作系统命令行。

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 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 对检材（若已保全，使用保全的存储设备）通过只读接口接到电子数据检验工作站。

5.4.3 对 Linux 操作系统中的日志配置文件进行检验，确定该系统记录的系统事件信息以及事件信息存放位置。

5.4.4 对 Linux 操作系统中的日志管理文件进行检验，确定系统管理日志文件的方式。依据日志管理文件中的内容，确定现有日志与周期备份日志的时间关系。结合检验要求，选择相应日志文件予以分析。

5.4.5 根据步骤 5.4.3、5.4.4 的检验结果，确定检材中需要检验的 Linux 操作系统日志文件，使用电子数据检验综合分析软件或 Linux 操作系统命令对其进行检验。对于明文格式日志，可直接查看；对于二进制格式日志，使用相应的工具或命令予以解析查看。

5.4.6 解码后包含有时间信息的日志文件，需结合操作系统所属时区进行时间转换。

5.4.7 对于已被删除的日志文件，依据 GB/T 29360-2012 进行数据恢复后，再按步骤 5.4.5、5.4.6 进行检验。

5.4.8 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 应对送检的检验对象做好防水、防磁、防静电和防震保护。