ICS 13.310
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1663—2019

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

2019-10-14 发布　　2019-12-01 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。