ICS 13.310
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1480—2018

法庭科学计算机操作系统仿真检验技术规范

Technical specifications for computer operating system emulation examination in Forensics

2018-04-17 发布　　2018-04-17 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)提出并归口。

本标准起草单位:公安部网络侦察技术研发中心、盘石软件(上海)有限公司、厦门美亚柏科信息股份有限公司、上海弘连网络科技有限公司。

本标准主要起草人:刘晓宇、翟晓飞、宋庆飞、李毅、陆道宏、赵庸。

法庭科学计算机操作系统仿真检验技术规范

1 范围

本标准规定了 Windows、Linux 以及 MacOS 操作系统仿真检验的技术方法。

本标准适用于法庭科学领域电子物证检验中的计算机操作系统仿真检验。

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 5271.1—2000 信息技术 词汇 第1部分：基本术语

GA/T 755—2008 电子数据存储介质写保护设备要求及检测方法

GA/T 756—2008 数字化设备证据数据发现提取固定方法

GA/T 976—2012 电子数据法庭科学鉴定通用方法

3 术语和定义

GB/T 5271.1—2000、GA/T 755—2008、GA/T 756—2008 和 GA/T 976—2012 界定的以及下列术语和定义适用于本文件。

3.1

系统仿真 system emulation

利用虚拟化技术、重新定向技术对计算机操作系统的内核、硬件设备、用户环境、各种网络协议、应用程序、数据记录等信息进行动态模拟。

3.2

仿真对象 emulation object

用于系统仿真的存储介质、镜像文件及虚拟机文件等。

4 仿真检验步骤

4.1 检验准备

4.1.1 检材编号

对送检的检材进行唯一性编号。

4.1.2 检材拍照

对送检的检材加上唯一性编号并拍照。

4.1.3 检材保全备份

按照 GA/T 756—2008 的要求对具备保全条件的检材进行固定保全。