

软件技术与数据库

虚拟机文件取证分析

钟琳1, 许榕生2

(1. 福州大学数学与计算机学院, 福州 350000; 2. 中国科学院高能物理研究所计算中心, 北京 100049)

收稿日期 修回日期 网络版发布日期 接受日期

**摘要** 介绍VMware Workstation软件常见的虚拟机磁盘文件结构及其含义, 提出一种符合司法要求的虚拟机文件取证方法。通过直接扫描虚拟机文件, 依据虚拟硬盘分区文件类型的存储结构定位虚拟机磁盘文件的虚拟主机的相应扇区, 获取证据。以虚拟硬盘分区文件系统NTFS为例进行说明, 探讨在虚拟机下进行计算机取证的策略。

**关键词** [虚拟机; VMware Workstation软件; 取证](#)

**分类号** [TP391](#)

**DOI:**

通讯作者:

作者个人主页: 钟琳1; 许榕生2

#### 扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF \(109KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [参考文献\[PDF\]](#)

▶ [参考文献](#)

服务与反馈

▶ [把本文推荐给朋友](#)

▶ [加入我的书架](#)

▶ [加入引用管理器](#)

▶ [引用本文](#)

▶ [Email Alert](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ [本刊中 包含“虚拟机; VMware Workstation软件; 取证”的 相关文章](#)

▶ [本文作者相关文章](#)