计算机工程与应用 2009 45 (18): 74-77 ISSN: 1002-8331 CN: 11-2127/TP

研发、设计、测试

基于KPCR结构的Windows物理内存分析方法

郭 牧, 王连海

山东省计算中心，济南 250014

收稿日期 2008-7-25 修回日期 2008-9-10 网络版发布日期 2009-6-17 接受日期

摘要 介绍了计算机在线取证方式的优势，总结了目前国外在计算机物理内存分析的研究现状及其存在的不足，在此基础上提出了一种新的Windows物理内存分析方法——基于KPCR结构的物理内存分析方法。与传统的物理内存方法相比，这种方法更为可靠，适用范围更广，具有很高的实用价值。

关键词 计算机取证 计算机在线取证 物理内存分析 数字取证

分类号

Windows physical memory analysis method based on KPCR structure

GUO Mu,WANG Lian-hai

Shandong Computer Science Center，Jinan 250014，China

Abstract

This paper describes the function of computer live forensics，and sums up the researches on computer physical memory forensics analysis.Then a new method of Windows memory forensics analysis is proposed，which is much reliable than other methods.This method is very useful in computer live forensics.

Key words computer forensics computer live forensics physical memory analysis digital forensics

DOI: 10.3778/j.issn.1002-8331.2009.18.024

通讯作者 郭 牧 wanglh@keylab.net

扩展功能

本文信息

Supporting info

PDF(732KB)

[HTML全文](0KB)

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

复制索引

Email Alert

文章反馈

浏览反馈信息

相关信息

本刊中 包含“计算机取证”的相关文章

本文作者相关文章

· 郭 牧

· 王连海