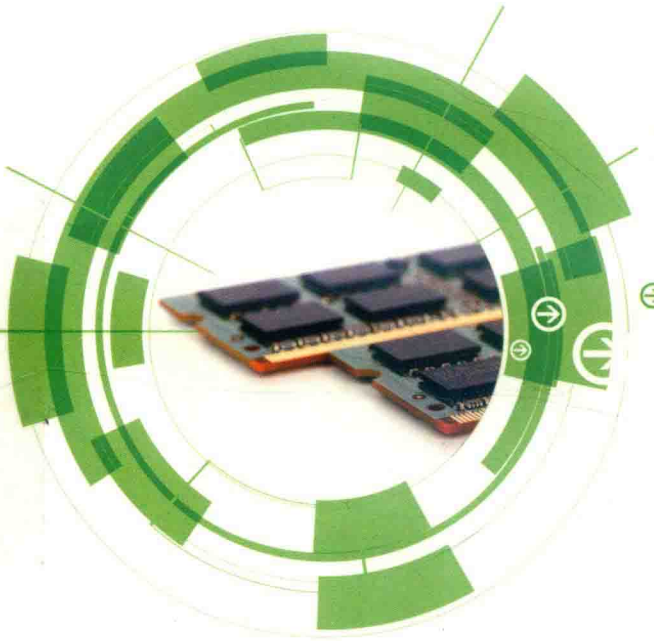
内存取证原理与实践

Theory and Practice of Memory Forensics

王连海　张睿超　徐丽娟　张淑慧◎编著



中国工信出版集团　人民邮电出版社
POSTS & TELECOM PRESS

内存取证原理与实践

Theory and Practice of Memory Forensics

王连海　张睿超　徐丽娟　张淑慧◎编著

人民邮电出版社

北　京

图书在版编目（CIP）数据

内存取证原理与实践 / 王连海等编著. -- 北京 : 人民邮电出版社, 2018.11
ISBN 978-7-115-48787-2

Ⅰ. ①内… Ⅱ. ①王… Ⅲ. ①计算机犯罪－证据－数据收集 Ⅳ. ①D918

中国版本图书馆CIP数据核字(2018)第224635号

内 容 提 要

本书详细讨论了近年来计算机取证技术中最热门并极富挑战性的内存取证技术，共 15 章。第 1~4 章首先对内存取证的发展和意义进行概述式的描述，然后对涉及的现代计算机软硬件技术基础进行简要介绍，最后介绍内存获取和分析需要的方法、工具等。第 5~10 章根据几个主要的操作系统（Windows、Linux 和 Mac）对内存分析进行更加深入的介绍。第 11~15 章介绍内存分析技术在最新计算环境下的一些相关进展和技术，如移动设备的内存分析、云计算环境（虚拟机）下的内存分析应用。

本书的读者对象为内存取证领域内本科生、研究生和科研人员，同时，对于具备计算机专业技术背景，并对计算机内存取证和分析技术感兴趣的信息安全相关领域的从业人员，本书同样是不可多得的重要参考资料。

◆ 编　　著　王连海　张睿超　徐丽娟　张淑慧
责任编辑　邢建春
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京市艺辉印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：22　　2018 年 11 月第 1 版
字数：536 千字　　2018 年 11 月北京第 1 次印刷

定价：138.00 元

读者服务热线：(010) 81055488　印装质量热线：(010) 81055316
反盗版热线：(010) 81055315

前 言

中国互联网信息中心最新发布的《中国互联网络发展统计报告》指出，截至2017年12月，我国网民规模达7.72亿，普及率达到55.8%；移动网络促进“万物互联”，移动支付使用不断深入，互联网理财用户规模增长明显；网络娱乐用户规模持续高速增长；六成网民使用线上政务服务；数字经济繁荣发展，电子商务持续快速增长。可以说，信息技术每天都在改变着我们的生活，人们对信息技术的依赖程度也越来越高。

现代信息技术给人们的工作和生活带来便利的同时，也不可避免地引发了各种负面问题，尤其是利用网络和信息而引发的各类犯罪行为呈现逐年增长的多发态势，如窃取国家机密、泄露个人隐私、盗窃网银密码、网络诈骗、黑客攻击之类的事件层出不穷，与之相关联的刑事、民事、行政案件或纠纷也大幅增长。为适应这类案件或纠纷的诉讼需要，计算机取证（数字取证、电子取证）应运而生。

计算机取证是用计算机、通信、电子等相关学科中的原理和方法，按照符合法律规范的方式识别、保存、分析和提交电子证据的过程。计算机取证在中国已有十几年的发展历史，在实际工作中已经被政府执法部门、法律界从业者和广大执法人员认可，积累了大量的经验并且取得了相当多的成就。目前，国内有很多学术团体从事这一方向的研究工作，许多公安、政法类院校也开设了计算机侦查和计算机取证专业；产品和技术方面，由最早主要使用国外技术和产品，逐渐涌现出一批符合国内取证调查实际的具备自主产权的产品；在商业领域，也有越来越多的企业开始重视应用计算机取证技术进行企业内部调查和IT审计。可以说，计算机取证技术是一个迅速发展的研究领域，有良好的应用前景。特别是在2012年新的刑事诉讼法对“电子数据”的法律地位加以独立规定后，计算机取证技术的重要性显得更为突出。

本书编者所在研究团队是国内较早进行计算机取证研究的学术团体之一，从事计算机取证方面的研究与实践工作已有十余年。特别是在内存取证方向上，突破了一些关键核心技术，取得了一些具有领先水平的科研成果，开发的多个软硬件产品在相关国家部门中得到配装，在维护国家安全、打击犯罪的实战中发挥了作用。本书详细讨论了近些年计算机取证技术中最热门并极富挑战性的一个方向：内存取证技术。通过本书，我们希望能够比较全面地介绍内存取证技术，并且与读者分享在内存取证实践上的经验和成果，以期读者对内存取证这一方向有所了解和启发，并且将其应用在自己的研究与工作中。

本书的研究对象是内存（RAM）中的数据。传统的计算机取证主要针对存储在各种介质中的静态数据，而内存取证研究的是内存中的动态信息。这些信息在系统运行时会经常产生

变化，在关机和重启机器后会丢失，因此也被称为易失数据。

为什么要做内存取证？因为在内存中，分析人员可以看到操作系统正在做的几乎所有事情。当内存块没有被覆盖时，很多曾经发生的事情的信息也同样被保留在内存中。内存中存在很丰富的信息，包括进程和线程、网络连接、打开的文件、剪贴板、用户生成的密码、硬件和软件的配置、操作系统日志和注册表等。而且，很多磁盘中没有的信息，在内存中都可以获取和分析出来，如恶意软件，加密、解密应用的密钥等。有了这些信息，就可以关联其他数据，得到更多有用的结果。

本书首先概述了内存取证的背景、起源、发展、作用和局限，随后简单介绍了 Intel 和 ARM 硬件架构、硬件内存管理（MMU, Memory Management Unit）、地址空间、地址转换等内存取证中需要了解的一些基础知识。

内存取证是从稳定和完整地获取 RAM 内存的镜像开始的。第 3 章给出了获取各种系统内存数据的软硬件方法，详细介绍了各方法的原理和实现，并对常用的一些工具做了简单介绍。物理内存镜像的获取是内存分析的前提和基础。

第 4 章探讨了一个经常被实际应用内存取证人员忽略的问题：获取到内存镜像，然后以此为基础分析得到的结果，能够多大程度上代表原来系统的运行状态？第 4 章中提出了基于内存镜像的在线取证模型，探讨了影响其获取信息可靠性的几个方面，最后提出基于测量理论的评估方法，在此基础上对此模型的可信性进行了评估。

获取的内存镜像文件是数十亿比特组成的数据，取证调查人员的职责是准确地描述从这些数据中识别、提取和分析出能够被法庭理解的电子证据的专业过程。有时，从内存镜像文件的比特演化成法庭能理解的文本并不需要很复杂的过程，如简单地针对一个字符串进行搜索就可以证明其在目标系统中存在。但更多时候，需要更复杂的技术，往往要依赖专业工具才能将比特数据转换为人们可以理解的文本。从专业角度说，取证人员仅依赖工具来获得答案，在法庭专业质询和激烈的辩论中，往往很被动，因此需要深入了解取证工具所使用的原理。

本书后面的章节针对 Windows、Linux、Mac 操作系统和安卓系统，分别论述了内存获取与分析的原理。这些章节回答了如下问题：从哪里开始寻找埋藏在内存镜像文件中的证据？在各个系统中的内存中可以获取哪些主要信息？如何使用特定知识对内存镜像文件中的相关证据进行识别、提取和分析？这些章节的内容可以帮助读者了解如何从内存镜像文件中获取进程、注册表、打开的文件、日志、网络等常见的数据，掌握内存分析和内存数据提取背后的原理和逻辑，在内存取证的实践中做到知其然，也知其所以然。

最后，本书用较多的篇幅论述了内存取证技术的实践应用，其中很多问题来源于我们的实际经验和研究工作，略述如下。

云计算一直是这几年的热点，本书探讨了内存分析在云安全中的应用。通过获取和分析宿主机物理内存，检测出宿主机中正在运行的虚拟机，实现了从宿主机物理内存中提取虚拟机物理内存信息，对虚拟机逃逸行为检测和基于旁路的云安全威胁监控技术进行了描述和讨论。

在实际取证工作中，经常碰到通过 uKey 的使用来限制特殊用户对机器访问权限的情况。本书论述了在未知 PIN 码、无法获取 uKey 硬件的情况下，利用内存分析技术绕过目标计算机对 uKey 的认证机制，并解除目标计算机上 USB 接口禁用的方法，以实现取证的目的。

恶意代码检测是网络空间安全研究中特别关心的问题。所有的恶意代码都会想尽办法在系统中隐藏自己，躲避各类工具的检测。但是，无论其如何隐藏自己，终究也要在内存中执行。本书探讨了使用内存分析技术进行恶意代码检测，着重介绍了 Windows、Linux 和 Mac 操作系统中基于内存分析的恶意代码检测方法。通过本书的学习，读者可以了解到：使用内存分析技术可以从系统正在运行的内存中识别被注入的代码，定位可疑动态链接库，从而达到检测木马的目的，并且能够从恶意代码遗留的各类痕迹中做更深入的分析工作。从这些探讨中可以看出，基于内存分析的检测方法与传统检测方式相比，有独特的优势。

登录密码的破解是内存分析技术中最为实用的应用之一。取证人员遇到处于屏保或待机状态的目标机时，不知道密码的情况下常处于束手无策的状态：一旦强制关闭目标计算机进行离线取证工作，嫌疑人的犯罪证据很有可能会丢失。此时，使用破解系统密码技术进行取证成为最佳选择。本书首先分析了 Windows、Linux、Mac 操作系统下密码认证的方式，然后详细介绍了利用内存取证技术对 Windows、Linux、Mac 等操作系统的登录密码进行破解的方法。

书中实例所用的内存镜像文件样本，以及我们自己开发的内存获取、分析等软件可通过 PC 端地址 box.ptpress.com.cn/y/48787 下载。

本书是山东省计算中心（国家超级计算济南中心）网络安全与取证团队长期研究成果的结晶。团队发展过程中，得到了齐鲁工业大学（山东省科学院）王英龙，青岛农业大学顾卫东，山东省计算中心杨美红、谭安辉、彭利民、李晔的大力支持。本书及相关研究工作离不开他们的热情帮助，在此特表感谢。

本书的编写工作得到了“山东省自然科学基金（No. ZR2014FM003）”的支持，内存取证的研究得到了“国家自然科学基金（No. 61070163、No. 61572297）”的支持，在此特表感谢。

当然，内存取证技术并不是万能灵药，其本身也存在各种局限，必须结合其他取证技术才能发挥出最大作用。相信读者在阅读过程中会发现和体会到这一点。

由于我们水平有限，编写时间紧张，书中难免存在疏漏和不当之处，敬请读者批评指正。

作者

2018 年 4 月

目 录

第1章 内存取证技术概述

1.1 计算机取证技术

现在，信息技术已经走进了人类社会生活的各个方面，计算机、互联网、智能手机、可穿戴设备等已经与人们的日常工作和生活密不可分。信息系统已经成为国家战略性的基础设施，经济、国防、能源、行政、通信、金融以及娱乐休闲等社会各行各业越来越重视和依赖信息系统。但是，同其他科学技术一样，信息技术在带给全社会巨大便利的同时，也带来一些问题。与信息系统相关的各类违法犯罪事件随着技术的发展也逐渐渗入社会生活的各个方面，涉及信息技术的法律纠纷更是层出不穷。因此，需要新的技术来帮助法庭和相关人员应对这些犯罪和纠纷。于是，计算机取证（Computer Forensic）技术慢慢发展起来。

Forensic 这个词在韦氏辞典是这样解释的：应用科学知识于法律问题，与应用科学知识到法律问题相关的。这个词语最初的翻译使用了“取证”这个词，而且最早的技术应用场景主要是围绕计算机及其周边设备的，因此约定俗成地就一直使用计算机取证这个术语概括这一法律与信息技术互相交叉的领域。有时也会使用计算机法证这个术语。随着模拟技术逐渐向数字技术转变，数字取证（Digital Forensic）这个词也越来越常用。有人认为计算机和数字等词不适于概括所有技术，使用了电子取证这个概念，这是国内公安部门一般使用的术语。我国 2012 年《刑事诉讼法》《民事诉讼法》以及 2014 年修改的《行政诉讼法》将电子数据作为一种新的证据种类纳入立法，使其得到了独立的证据地位。但是并没有明确电子证据的具体定义。

各种信息技术虽然日新月异，但都是人们获得信息、记录信息、处理和利用信息的手段。以上概念和术语本质上并没有不同，无论名称如何，其核心都是以某种信息技术作为载体保存证据的处理问题，即利用信息技术，按照法律规范允许的方式，对电子证据的识别、收集、固定、分析和呈现问题。因此，读者在碰到这些术语时，广义上可以看作是相同的概念。

计算机取证需要获取的对象是电子数据，其本身具备的一些特点直接影响到计算机取证的进行。电子证据的特点可以归纳为以下几点[1]。

（1）脆弱性

脆弱性主要表现在两个方面：一方面，由于电子数据都存储在磁介质或电子元器件中，而这些介质本身的一些特性使电子数据容易被人为地损坏，因而在计算机取证中对证据材料的保存有十分严格的约束；另一方面，电子数据可以很容易地被修改或删除，而这种操作往往是不可完全恢复的，即便可以恢复，也会对这些数据的证据有效性产生极大的影响。

（2）非直观性

电子数据存在于一个二进制的世界，因为信息系统的整体架构在不同的硬件和逻辑层次有各种各样的表现形式，所以很多时候无法直观识别证据材料的内容。

（3）隐蔽性

计算机系统中存在太多的随机性，很多数据只有在特殊的上下文环境中才有其特定的意义，所以无法判断电子证据中有效信息的位置，而且现在已经存在很多反取证的技术，这使有效证据信息的检索更加难以进行。

（4）多态性

电子数据的作用往往需要有一个上下文环境作为参考，不同环境下对电子数据分析产生的结果很可能是不同的。

（5）时效性

计算机系统中很多电子数据只有很短的生命周期，当系统运行一定时间后这些信息可能会被系统覆盖或清除。

电子证据的特点使它不像一般的民事或刑事案件相关的证据那样显见、直接，可以利用传统的搜集及分析方法粹选出供法庭上判决的直接证据，而是必须依赖特定的取证技术或方法加以搜集分析才能作为判决上参考的间接证据。只有通过使用取证工具，使用合法的程序（流程）获得，并且通过科学专业的知识进行分析、呈现和解释的电子证据才能被法院理解与认可。由于不同的国家在法律、道德和意识形态上存在差异，而取证原则又依赖于不同的证据使用原则，但大体都是为保证获取的证据的合法性、客观性和关联性，因此计算机取证的原则可归纳为以下几个方面[1,2]。

（1）依法取证原则

计算机取证不仅要保证取证实体合法，还要保证取证程序合法。任何证据的有效性和可采性都取决于证据的客观性、与案件事件的关联性和取证活动的合法性。取证活动的要件构成是指参与取证全过程、决定或影响取证与司法鉴定结果的各个方面或因素，包括取证的主体、对象、手段、过程和环境 5 个要素，只有保证取证“五要素”同时合法，才能保证获取的证据合法。

（2）无损取证原则

首先，由于电子数据自身的脆弱性以及证据的严格性（即证据材料能够客观地、真实地反映案件事实），所以取证人员在对电子数据进行采集时必须严格地遵循合法流程进行电子数据的获取。其次，对电子数据的保存应该做到多备份，一方面是为了克服电子数据脆弱性，另一方面是为了可以重现分析过程。

（3）全面取证原则

全面取证原则体现在调查机关在取证过程中应该尽可能地全面调查取证，使获取的证据之间相互印证，以真实地重现案件事实。但由于电子数据的隐蔽性，在海量数据面前，调查

人员往往容易忽视海量信息中一些细微的数据信息，因而在计算机取证过程中，一定要认真分析来源并进行全方位、多角度的取证，在确保证据与案件事实关联的基础上，将获取的所有电子证据与案件的其他类型证据相互例证，排除矛盾的电子证据，从而克服电子证据的多态性，最终组成完整的证据链。

（4）及时取证原则

由于有些电子数据的时效性很强，所以当确定取证对象后，应该尽早搜集证据，保证其没有受到任何形式的破坏和损失。

计算机取证涉及信息技术的方方面面，需要综合运用各种技术知识来解决问题，如操作系统、文件系统、网络协议、密码技术等。同时，计算机取证又是一个多门学科交叉的研究领域，与之相关的学科有计算机应用技术、信息安全、网络安全、法律与法学、刑事科学等。计算机取证研究的内容依据取证步骤的过程不同，分为证据的识别、获取、分析和呈现等；根据取证对象的不同，分为 Windows 取证、Linux 取证、网络取证、移动设备取证等。几十年来，国内外计算机取证的研究从无到有，从少数到具有一定规模，逐渐发展壮大成内容丰富、理论实践都较为成熟的研究领域。

1.2　计算机取证技术的发展

20 世纪 70 年代，美国立法机关对联邦民事诉讼程序规则第 34 条等法律条文进行了相应的修改，以应对电子证据带来的问题。这可以说是计算机取证技术的开端[3]。当时，因为信息技术的应用还极其有限，只有极少数人，如信息系统开发人员、管理人员、极少数执法人员在工作中碰到这方面的事件，采取一些临时的措施来应对。

随着个人计算机的出现和逐渐普及，涉及计算机的犯罪事件与法律纠纷大量涌现。1984 年，美国联邦调查局（FBI，Federal Bureau of Investigation）开始开发专门的计算机应用程序来检测计算机证据，随后，FBI 还成立了计算机分析响应组（CART，Computer Analysis Response Team），其功能和结构被许多国家和机构效仿。这一时期的操作系统大多是 Unix 和 DOS，Macintosh 的操作系统和早期的 Windows 操作系统处理的介质是容量较小的软盘和磁盘等，普通用户开始使用电话拨号接入互联网。计算机取证中主要的参与者已经开始意识到需要制订相应的取证规范，开始开发初步的专用软硬件产品，培养相关的专业人员，成立专业部门完成计算机取证的任务。

后来，互联网逐渐普及，个人计算机更加深入社会生活的各个方面。计算机取证的需求大大增加，计算机取证技术有了突飞猛进的发展。政府、军事和情报部门对计算机取证技术倍加关注，企业界的兴趣同时也大大提升，逐渐出现许多专门从事计算机取证软硬件工具开发和销售的企业，出现了许多大型的专门取证软硬件产品。

从计算机取证技术开始出现到逐步发展的过程来看，其主要目的是应对实际应用需求，因此，其早期的关注重点是工具开发和技术实现层面。但在计算机取证逐步发展过程中，学术界开始逐渐参与，计算机取证的专业学术会议开始出现。研究和关注的主体也从个体发展到企业、机构和学术团体，特别是政府资助和成立了许多专业机构，有了训练有素、配备相关装备的专业队伍从事实际的计算机取证工作。

经过多年实际需求的刺激和持续的进步，计算机取证已经发展到相当高的程度。目前，国内外已经有众多的规模企业，无论是综合性的面向系统平台的企业级通用取证工具，还是具体针对某个信息系统应用的专门电子取证工具，市场上都有相应的产品供选择。同时针对云环境等新技术、新的取证需求、新的思路和方法仍然层出不穷。在学术研究方面，国内外有许多高校研究团队、科研机构活跃在计算机取证研究的前沿，DFRWS（Digital Forensics Research Workshop）、IFIP WG11.9（International Federation for Information Processing Working Group 11.9 on Digital Forensics）以及 SADFE（Systematic Approaches to Digital Forensics Engineering）等学术组织，多年来也不断发展壮大，各种学术活动一直非常活跃。

计算机取证技术如今已经走过了几十年的发展历程，计算机取证技术理论研究发展迅速，实践内容日益丰富，其研究成果和独特的取证视角扩展了信息安全领域的研究方法，启发了研究与分析某些信息安全问题新的研究思路。计算机取证技术已经从一个局限于传统犯罪证据获取的领域，逐步发展成为信息安全中一个重要的实践与理论阵地。

1.3 计算机取证类型

计算机取证包括证据获取和证据分析等，需要获取的内容以电子数据的形式存在。计算机取证的主要对象和层次如图 1-1 所示。根据获取电子数据的时机，计算机取证一般分为离线方式和在线方式。

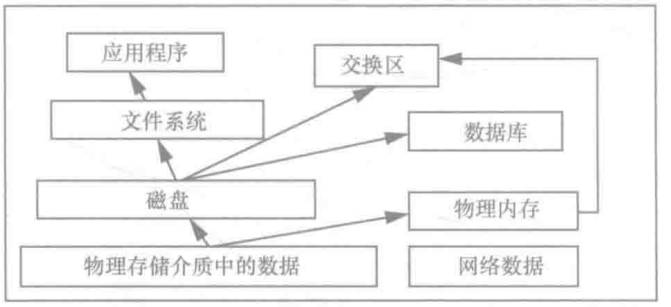


图 1-1 取证内容

1.3.1 离线取证

离线方式是指在关闭计算机或电子设备后，对相关数据进行取证，这是传统的取证方式。早期的取证流程和规范规定：首先，使用切断计算机电源的方式关闭计算机和电子设备，最大程度上保持电子数据的原始状态；其次，对存储介质进行比特对比特的镜像复制；然后，分析存储介质副本中的静态数据和文件系统中的数据，从中分析得到需要的电子证据。例如，可以通过恢复删除的数据或者文件碎片的方式，分析出文件的访问模式、浏览器的访问活动等。至今，这种方式仍然是应用最广泛的一种计算机取证技术，应用于打击计算机网络犯罪、反恐等重要领域。

单一的离线取证方式存在一些显而易见的不足。

首先，仅进行离线取证而没有获取易失性数据，会丢失案件关键信息。

当关闭计算机或电子设备时，当前系统的进程信息、当前登录的用户信息、网络连接状态、系统的内存信息等信息将丢失，而这些信息往往在调查网络犯罪的过程中有着不可替代的作用。

其次，在许多情况下，离线取证无法获取数据。

例如，现在 Windows 操作系统提供了 BitLocker 驱动器加密技术，加密整个 Windows 操作系统卷，用于保护用户的硬盘数据。取证时，硬盘被锁定且不知道密码的情况下，就很难获取数据。另外，很多硬盘也使用了 BIOS 加密，设置了硬盘的数据访问锁，必须在对应的主板且知道密码的情况下才能访问硬盘数据。这些加密保护的情况，必须对相应的加密系统进行破解，有时还需要针对硬盘的固件进行破解，才能最终访问硬盘数据，给取证工作带来很大的困难。

再次，很多应用场景中，如网吧等，用户可能会用预装操作系统的光盘（如 Windows 下定制的 Windows PE、Linux 下的 Knoppix 等）使用计算机，运行时候的数据并不保存在本地硬盘。

在云计算情况下，用户通过计算机、手机等方式接入数据中心，运算和存储大部分都在云端，本地硬盘中的有用数据极少，但由于受到国别、地域、法律、技术难度等种种限制，几乎不可能对云计算中心进行取证。

诸如此类的情况还可以列举出许多，这种情况下，在线取证就成为获取证据的唯一手段。

最后，磁盘镜像模式在很多情况下难以实施。

硬盘发展至今已经有几十年的历史，硬盘的体积越来越小而容量越来越大，从兆字节（MB）为单位到吉字节（GB），发展到现阶段的太字节（TB）阶段，可以预计在单个硬盘的容量扩充技术还会继续增长。目前的磁盘镜像技术，在复制速度上很难跟上存储容量的发展，往往需要花费大量的时间。在有时间要求的情况下，完全磁盘镜像模式难以实施。

现在，人类已经步入一个数字化的信息时代。IT 在各个领域中正处于前所未有的关键地位，各种业务数据的数据量呈几何级增加。为了长时间存储并确保这些数据的可访问性，设计了各种存储技术架构，如磁盘阵列、分布式存储等复杂的海量存储解决方案。随着云计算、移动计算等技术的发展，短信、电子邮件、文档、图片、视频、社交网络等数据更是急剧增长。云环境下，往往采用虚拟桌面技术，工作是在设备上进行，但是信息数据保存在云端，采用云存储服务等复杂的海量存储系统。这些系统的复杂程度和海量的存储量导致在取证时，完全进行镜像难以实施。

另外，在实际工作中，有些情况是无法静态进行磁盘镜像的。例如，对需要保障连续运行的系统，中断系统的代价十分昂贵，会造成巨大的声誉和金钱损失。

1.3.2 在线取证

在上述情况下，在线取证（Live Forensics）方式越来越受到人们的重视。在线取证是在不关闭目标计算机或电子设备的情况下，获得目标计算机内存、磁盘等存储介质中的电子数据，并进行分析呈现的取证方式。在线取证的核心任务是获取计算机上的系统进程信息、加载的驱动程序、网络连接状况、当前打开的文件等易失性数据（Volatile Data），这些信息是信息安全事件追查、入侵取证分析的关键要素，而这些信息都驻留在计算机物理内存中，随着宕机或系统重启，这些信息将丢失。

计算机在线取证一般需要获取以下几方面的信息。

（1）内存信息：整个物理内存；每个应用程序使用的内存。

（2）网络连接状态：包括打开的端口，与打开端口相对应应用程序、当前和最近的连接、共享目录、文件、网络配置信息、路由信息、netbios 信息等。

（3）进程信息：正在运行的进程信息；每个进程加载的动态链接库；进程打开的文件；线程信息。

（4）文件信息：所有文件的创建、修改和访问时间；隐藏文件；远程打开的文件。

（5）用户信息：当前登录到系统的用户，登录记录。

（6）系统信息：OS 版本、OS 序列号、OS 安装时间、系统时间、时区设置以及输入法设置；正在运行的服务；所有已安装的服务信息；历史开机时间、系统启动时间、环境变量；驱动程序信息；开机自动启动信息：包括 DOS 自动加载程序、Windows 启动加载选项；USB 等设备使用记录；硬盘信息。

（7）应用程序信息。

（8）应用程序的密码、登录系统的密码。

可以看出，计算机在线取证的任务是获取计算机内存和页面交换文件中存在的易失信息。早期的在线取证方式，很自然地采取一种直接方式，即针对需要获取的具体数据，分别开发相应的取证工具，直接在目标计算机系统中获取信息。在实际在线取证过程中，根据每次取证的需求，分析判断取证的步骤、采用的工具、保存的方法，制定具体的取证方案，实施在线取证。这种方式可以满足获取信息的需求，但是从计算机取证的角度看，存在一些不足。

（1）获取的在线证据的正确性难以保证。

进行在线取证过程中，一方面要根据每次在线取证的需要，分析系统，判断出需要提取的信息，然后运行相应工具获得证据，这个过程受到分析人员水平、工具本身以及反取证技术的影响，最后得到的结果正确性难以保证；另一方面，在线取证工具受到核心态木马和病毒的影响，得到的数据可能是已被恶意程序篡改过的数据。

（2）时间长，存在丢失内存中和硬盘上有用信息的风险。

由于目前的在线取证工具，如 Helix 等工具在获取证据时，需要持续的时间比较长，很可能覆盖内存中可疑的信息。同时，恶意攻击者也可能在这段时间删除或破坏硬盘上的有用信息。

（3）易引起数据混淆。

当多个在线取证工具运行在目标系统中时，将不可避免地改变系统的数据和状态，容易引起数据混淆，破坏了取证应尽量不影响原始现场的原则。

（4）方法不科学，依赖于一次过程，得到的证据结果难以质疑和检验。

在线证据获取的过程中，同时包含收集、保存和分析等步骤，取证的过程阶段难以划分。获取得到的证据，在法庭上往往会受到种种质疑。例如，如何证明在线取证时的分析判断过程是科学的，获取证据的工具是否是科学、可信的，获取到的结果是否与需要证明的结论是相关的，是否忽略了能提供相反意见的数据等。这些问题因取证的现场已经消失（当时正在运行的计算机系统），无法通过与其他技术专家的重新检测、分析进行质证，不能得到验证，证据的科学性和可信度会降低。

1.4　内存取证

直接在可疑或者目标系统中运行各种工具的在线取证方式，大大破坏了计算机取证的现场——内存。这种方式只保留了取证后得到的结果，却并没有保存证据原始的数据，如果有新的在线取证需求提出，会毫无办法；取证的结果受到质疑时，无法根据原始数据进行验证。因此，一种特殊的在线取证方式——内存取证（Memory Forensics）开始进入计算机取证研究者的视线。

内存取证先获取内存镜像文件，再通过分析镜像文件，提取在线取证所需的各种信息。

从内存镜像文件中获取信息，最简单和直接的方法就是使用 strings 和 grep 等工具或更为强大的应用软件（如 WinHex）进行明文字符串的查找、模式匹配。这种方法有时也被称为非结构化内存取证，因为它仅将内存镜像文件看作一个字节流的文件。这种简单的方法可以获取账户信息、文档数据等有用的信息，但是这种方法不能提供信息的上下文环境，无法知道匹配的字符串来自哪个进程的地址空间，无法得知这些信息是如何被系统使用的。而且，一些数据通过简单的编码或者加密，就可以使这种方法失效。因此，这种直接提取信息的内存取证方法，远远不能满足计算机取证的要求。

真正意义上的内存取证的研究工作始于 2005 年。数字取证研究组（DFRWS，Digital Forensic Research Workshop）推出了一项名为“内存分析挑战”（ Memory Analysis Challenge）的物理内存分析竞赛活动。该活动提供了 Windows 2000 操作系统的物理内存镜像文件，要求参赛者分析并且回答文件中所包含的隐匿进程及其隐匿方式、网络攻击者如何攻击以及何时、何处发起攻击等相关攻击时间轴信息。Betz 和 Garner 以及 Mora 给出了详细的解答，并最终获得优胜。Betz 通过逆向分析 Windows 2000 内核，获取其重要的内核数据结构，并研发了内存取证工具 MemParser，详细地提取了该内存转储文件中所蕴含的信息；Garner 和 Mora 开发了 kntlist 工具，通过进程链数据结构 PsActiveProcessList，顺序对比所给的有隐匿进程的镜像样本和另外一台可信的对比镜像样本的进程信息，也得到了最后的结果。自此，计算机取证领域开始了一波内存取证研究的热潮。各种内存取证方法和相应的内存取证工具不断出现，至今仍是计算机取证研究的热点之一。

内存取证的对象是存储系统运行时保存在线数据的文件，主要是指物理内存的镜像。通过内存镜像，将运行系统的物理内存中的所有数据以二进制文件的形式保存到固定的存储介质上（通常保存到硬盘上），将易失性的证据固化为非易失性的证据（数据），保留了取证原始现场。另外，内存取证的对象还包括一些操作系统中存储在磁盘中的文件，如虚拟机内存快照等静态的内存、操作系统进行内存管理产生的文件（如 Windows 操作系统的 pagefile.sys、hiberfil.sys 文件，Linux 系统的 swap 文件等）和其他内存转储文件。

内存取证的任务就是以操作系统内核数据结构为特征，通过结构化、逻辑化的分析，从这些文件中提取所需的信息，并对这些文件中保留的系统运行状态进行相应的描述，最大限度地构建电子证据以及其存在的状态。这种内存取证与分析使用一定的结构来解析内存镜像文件，也被称作结构化的内存取证。内存取证的主要研究内容可以用图 1-2 描述。