电子数据取证研究概述*)

孙 波 孙玉芳 张相锋 梁 彬
(中国科学院软件研究所 北京100080)

摘 要 随着计算机技术的飞速发展,人类社会对数字信息的依赖已达到前所未有的程度。与此同时,计算机犯罪率也以惊人的速度增长(2003 CSI/FBI 计算机犯罪调查报告)。由于计算机犯罪是刑事犯罪中一种新兴的高科技犯罪,政法机关在如何利用高技术手段对付这种高技术犯罪方面缺乏必要的技术保障和支持,为了保障和促进计算机信息网络健康有序发展,提高政法机关打击计算机犯罪的能力,需要对电子数据取证(数字取证、计算机取证)领域进行深入的研究,这不但需要开发切实有效的取证工具,更需要对电子数据取证领域的取证定义、取证标准、取证程序等理论基础的研究。本文正是在这种需求下,对电子数据取证领域的研究工作进行了分析,首先对电子数据取证的相关概念进行总结,然后对国内外电子数据取证的基础研究工作进行了概要性的描述,并对目前较为典型的取证工具作以介绍。本文对取证领域,尤其是对电子数据取证领域的基本理论和基本方法进行深入分析的基础上,结合其上层典型应用的行为方式为前提,力求为开发出适合我国国情的电子数据取证系统建立良好的基础。

关键词 电子数据取证,数字取证过程模型,计算机取证过程模型,有效性,真实性

Research of Requirement Based Computer Forensics Process

SUN Bo SUN Yu-Fang ZHANG Xiang-Feng LIANG Bin
(Institute of Software, Chinese Academy of Sciences, Beijing 100080)

Abstract Research regarding digital forensic technologies has become more active with the recent increases in illegal accesses to computer system. Many researchers only focus on the techniques or tools for evidence detecting and evidence analyzing, overlooking key fundamentals. And the important part in digital forensic key fundamentals includes the development of standards, definitions and methodologies. This paper explores the development of the digital forensics, compares and contrasts several forensics periods, and specially explores the development of the digital forensics process. Based on them, trying to develop sound digital forensics system which fits for our contry.

Keywords Digital forensics, Digital forensics process, Computer forensics process, Validity, Fidelity

1 引言

阻止计算机攻击的最好方法就是预先防止攻击的发生。清晰的安全策略可以帮助系统管理员消除工作中的歧义;一致的软件维护和用户管理执行规范,合理配置的授权机制及访问控制机制都可防止误用的发生;日志机制可帮助管理人员审查在计算机系统中曾经发生过的用户行为,以便查找事故发生的原因和影响;重要数据的定期备份可防止数据的丢失和损坏。然而,以上这些步骤在计算机系统的日常维护管理中却很少用,再加上软硬件设计中难以避免的不合理性,操作人员相关知识的局限性等等,使得我们无法保证系统的绝对安全。

如果在可预见的将来中计算机系统的绝对安全性无法保障,计算机犯罪将无法避免,那么如何从计算机犯罪现场挖掘犯罪方法、犯罪动机、犯罪工具、确定犯罪责任和评估损失?这就是计算机取证(Computer Forensics)领域要解决的问题。

当人们谈起取证(Forensics)时,总会与侦察犯罪现场的侦探们联系在一起,他们搜集证据,确定嫌疑人,构建充分的起诉材料体系。尽管计算机犯罪看起来非常新奇,然而与传统取证相比较,其特性是相同的,尽管其犯罪手法的不同,但是犯罪动机基本类似。

1.1 计算机取证技术的相关概念

由于计算机取证技术目前在国内甚至国外只是刚刚兴起,很多人对此领域还比较陌生,因此有必要首先对其基本概念作以简单描述:

1)电子数据证据 其概念涵盖所有与证据有关的电子数据,如文档文件、图像文件、音频及视频文件等。

2)取证科学 即使用科学原则及方法在犯罪侦察过程中去识别、发现、重构和分析犯罪证据的科学。

3)计算机取证 在业界对计算机取证基本概念的讨论是很丰富的,现列举几个已提出的、较具代表性的概念:

·作为计算机取证方面的资深人士—Judd Robbins 先生对此给出了如下的定义:计算机取证法不过是将计算机调查和分析技术应用于对潜在的、有法律效力的证据的确定与获取。

·计算机紧急事件响应和取证咨询公司 New Technologies 进一步扩展了该定义即计算机取证包括了对以磁介质编码信息方式存储的计算机证据的保护、确认、提取和归档。

·SANS 的一篇综述文章给出如下定义:计算机取证是使用软件和工具,按照一些预先定义的程序,全面地检查计算

*)本文研究得到国家自然科学基金(No. 60073022)、国家 863 高科技项目基金(No. 863-306-ZD12-14-2)、中国科学院知识创新工程基金(No. KGCX 1-09)资助。

机系统以提取和保护有关计算机犯罪的证据。

归纳以上的论述，我们认为计算机取证是对计算机入侵、破坏、欺诈、攻击等犯罪行为，利用计算机软硬件技术，按照符合法律规范的方式，进行识别、保存、分析和提交数字证据的过程。取证的目的是找出入侵者，并解释入侵过程。

4)计算机取证的三个重要知识体系

·计算机科学。其应用范围主要集中于提供用于分析电子数据证据的相关技术细节。

·取证科学。其应用范围主要集中于提供一套适当的方法用于分析任何形式的电子数据。

·行为证据分析。通过综合相关的技术知识和适当的科学方法来较完善地分析犯罪行为和犯罪动机。

1.2 计算机取证的基本原则

根据电子证据易破坏性的特点，确保电子证据可信、准确、完整并符合相关的法律法规，计算机取证主要遵循以下几点原则：

1)尽早收集电子证据，并保证其没有受到任何破坏；

2)必须确保“证据链(chain of custody)”的完整性，也称为证据保全，即在证据被正式提交给法庭时，必须能够说明在证据从最初的获取状态到在法庭上出现状态之间的任何变化；

3)不要直接对原始数据进行分析，分析数据的计算机系统和辅助软件必须安全、可信；

4)整个检查、取证过程必须是受到监督的。

1.3 计算机取证技术的实施步骤及实现方法

随着计算机技术的迅猛发展以及黑客技术的不断提高，再加上执法部门还没有形成统一标准的程序来进行计算机取证工作，使得计算机取证过程和技术越发复杂。尽管如此，计算机系统基本组成部分及其运行方式的变化不大，黑客攻击的基本方式也比较固定[3]。因此，取证的基本分析方法也是相对稳定的，现将其基本步骤及方法表述如下：

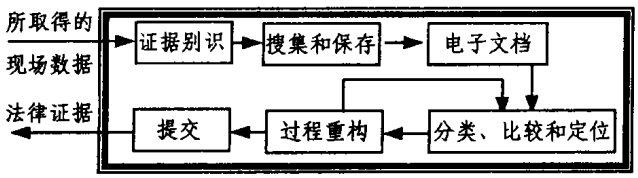

图1 计算机取证基本步骤

(1)证据识别 对所取得的现场数据依据软硬件特征正确识别取证信息所处范围，过程大体分为识别信息载体和通过区分取证信息和无关信息来确定取证信息所处范围两个步骤。

(2)搜集及保存电子数据证据 一旦确定了可作为证据的电子数据的范围，应在其原始状态下将其再次保存。保存过程中应保证备份信息的完整性，避免遗漏。

(3)对搜集及保存的硬件和电子数据证据建立电子文档 通过使用数字签名等技术保证备份数据的真实性、完整性和证据连续性，并且自动记录电子数据证据收集的所有细节(如位置、时间等)以便为以后的虚拟运行提供依据。

(4)电子数据证据的分类、比较和定位 对收集的数据进行分析和整理，这是电子数据鉴定系统的核心部分。大概过程为：

1)对电子数据证据进行特征分类并逐步建立起相应的特征类库，这不但有利于发现更多细节、精确已发现的证据而且也为今后的取证工作奠定了基础。

2)在分类的基础上将电子数据证据与类库中的样本进行内容、功能及特征上的比较找出其与同类中的差别并进行定位。其技术主要包括：依据对程序作者所习惯的程序布局、编程风格和编程的经验及能力来推断其作者的技术；文件的数字摘要分析技术；日志分析技术；发现同一事件中的不同证据间的联系；解密及密码破译技术；考虑到以上过程中数据之间所具有的关联性，可采用神经网络、数据挖掘、智能推理以及知识发现等方法对关联数据进行处理。

(5)犯罪过程重构 此模块最终目标是重构发生了什么及何时发生的经过，其目的是辨别作案的实际意图及发现新的漏洞以便取得更多的证据。通过重构再现，不但可发现很多遗漏的细节，还可搞清犯罪意图及损失程度。另外，通过与分析模块的不断反馈，使得重构再现更加接近真实情况，从而使得证据更具说服力。

(6)提交 此模块主要用于接收最终的电子数据证据的分析结果，并以可向法院提交的格式形成报表。

1.4 计算机取证技术的相关技术

正如上节所述，计算机取证过程充满了复杂性和多样性，这使得相关技术也显得复杂和多样。依据计算机取证的过程，涉及到的相关技术大体如下[15]：

(1)电子证据监测技术 随着计算机犯罪案件的日益增多，计算机取证面临着越来越多的困难，其中最为严重的就是证据问题，对于计算机犯罪的取证，就是对计算机数据的取证。电子数据的监测技术就是要监测各类系统设备以及存储介质中的电子数据，分析是否存在可作为证据的电子数据，涉及到的技术大体有事件/犯罪监测、犯罪简档监测(Profile Detection)、异常监测(Anomalous Detection)、审计日志分析等。

(2)物理证据获取技术 依据电子证据监测技术，当计算机取证系统监测到有入侵时，应当立即获取物理证据，它是全部取证工作的基础，在获取物理证据时最重要的工作是保证所保存的原始证据不受任何破坏[30]。在调查中应保证[16]：不要改变原始记录；不要在作为证据的计算机上执行无关的程序；不要给犯罪者销毁证据的机会；详细记录所有的取证活动；妥善保存得到的物证。

物理证据的获取是比较困难的工作，这是由于证据存在的范围很广，而且很不稳定：电子数据证据可能存在于系统日志、数据文件、寄存器、交换区、隐藏文件、空闲的磁盘空间、打印机缓存、网络数据区、记数器、用户进程存储区、堆栈、文件缓冲区和文件系统本身等不同位置[16]。涉及到的技术大体有：镜像技术、事件管理技术(Case Management)、时间同步技术(Time Synch.)等。

(3)电子证据收集技术 是指遵照授权的方法，使用授权的软硬件设备，将已收集的数据进行保全，并对数据进行一些预处理，然后完整安全地将数据从目标机器转移到取证设备上。这需要安全的传输技术(目前主要采用的是加密技术)、无遗失的压缩技术、数据裁减和恢复技术等。

(4)电子证据保存技术 在取证过程中，应对电子证据及整套的取证机制进行保护。只有这样，才能保证电子证据的真实性、完整性和安全性[25]。使用的技术主要有对取证服务器的网络进行物理隔离、加密技术、访问控制技术等。

(5)电子证据处理及鉴定技术 电子证据处理指对已收集的电子数据证据进行过滤、模式匹配、隐藏数据挖掘等的预处理工作。在预处理的基础上，对处理过的数据进行数据统计、数据挖掘等分析工作，试图对攻击者的攻击时间、攻击目

标、攻击者身份、攻击意图、攻击手段以及造成的后果给出明确并且符合法律规范的说明。

(6)电子证据提交技术　依据法律程序,以法庭可接受的证据形式提交电子证据及相应的文档说明。

综上所述,计算机取证技术是由多种科技范畴组合而成的边缘科学。在此,我们将涉及计算机领域的相关技术总结如表1所示。

表1　计算机取证涉及到的相关技术

证据监测	证据保存	证据收集	证据鉴定	证据分析	证据提交
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation
Resolve Signature	Imaging Technologies	Approved methods	Preservation	Traceability	Expert Testimony
Profile Detection	Chain of Custody	Approved Software	Validation Technology	Statistical	Clarification
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement
System Monitoring		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure
Audit Analysis		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation
Etc		Sampling	Hidden Data Extraction	Link	
		Data Reduction		Spacial	
		Recovery Techniques			

注:表中所提"证据"均指"电子证据"

1.5　计算机取证技术的应用领域

(1)司法系统　随着信息技术的不断发展,在人们的日常工作及生活中对它的依赖也越来越强,与此同时计算机犯罪也逐步显露出其对社会的极大危害。因此,作为此类犯罪侦查的最主要技术之一—计算机取证技术显得尤为重要,作为这种技术的一个组成部分—电子数字证据分析技术也体现出其重要的价值。

(2)学术界　在学术界时常会发生软件代码的偷盗行为,使用电子数据证据分析技术可有效地发现某段代码的真实作者。

(3)工业界　在工业界,常存在已运行了数年的大型软件产品,这些软件代码可达到百万甚至千万行,有关某个软件甚至某段代码的作者信息很可能已不存在或不准确了。然而,当某个模块或某段代码需要重写时,其作者信息就尤为重要了,当我们弄清模块或代码的作者时,就可以借助其力量较方便地对代码进行升级等工作。

(4)实时入侵检测系统　电子数据证据分析技术也可有效地强化实时入侵检测系统。

2　计算机取证技术研究的发展

计算机取证技术是打击当前不断增长的计算机犯罪的主要手段[31],要切实有效地打击日益广泛的计算机犯罪问题,必须建立牢固的计算机取证理论基础和基本方法,以及建立于它们之上的计算机取证应用工具[31]。早在20世纪80年代,计算机取证的研究就引起了研究机构(尤其是美国军方)的重视[13],至今,人们已在这个领域付出了十几年的努力,开展了大量的工作,也取得了一些瞩目的成果。今天,要确定正确的计算机取证方法,应该对其发展历史有一个比较全面的了解。善于从前人建立的科研宝库中吸取有益的养分,有助于把握正确的发展方向,在计算机取证的研究与开发中少走弯路、错路。

对计算机取证技术研究的发展历史进行全面的概括总结,是一项比较艰巨的工作,在本文的工作之前,这方面已有信息是零碎的、不全面的[12]。本文通过对计算机取证研究与开发方面十几年来比较有代表性的工作的深入考察,根据这些研究与开发工作及其相应的技术成果的特点,提出了三阶段划分的思想,给出了奠基期、初步发展期、理论完善期的定义,并以此为基础,归纳和描绘了计算机取证研究的发展演化历程,力求为确定正确的计算机取证技术研究开发方法建立良好的基础。

2.1　发展阶段划分方法

本文以时间为线索,根据计算机取证技术研究与开发工作的特点,进行阶段划分。考察的对象是从第一个计算机取证项目起至本文写作之时止计算机取证技术研究与开发中的典型工作。作者把计算机取证技术研究的历程划分为奠基期、初步发展期、理论完善期等三个发展阶段。奠基时期始于1984年FBI的计算机分析响应组(CART)的成立之时,在这个时期,计算机取证技术的研究经历了从无到有的探索过程,计算机取证技术的基本思想、理论、技术和方法逐步建立。初步发展期始于20世纪90年代中期,这个时期的特点是数字取证(digital forensic)特别是计算机取证(computer forensic)技术及产品的快速发展[19],同时却忽略了计算机取证基本理论和基本方法的研究。理论完善期始于2000年左右,这个时期的特点是计算机取证领域开始关注取证基本理论和基本方法的研究,到这个阶段计算机取证研究的发展经历了由理论到实践,再由实践回归理论的科学发展过程。三个时期的划分主要目的在于刻画计算机取证研究演化的主流特点,力图反映技术进步的特征,虽然以时间为线索,但并不意味着以时间为绝对界限。

2.2　奠基期

计算机取证科学(computer forensic science)主要是在司法机关的需求中应运而生的。早在1984年,FBI的实验室就开始对计算机取证进行研发。为了有组织有计划地解决刑侦人员不断增长的需求,FBI成立了计算机分析响应组

(CART)。尽管CART仅存在于FBI,但其功能和基本组织结构被世界上许多国家的执法机构所效仿[13]。计算机取证技术研究工作作为一门新兴的学科,开始蹒跚起步了。

2.2.1 "计算机取证(computer forensics)"概念的发展 自从20世纪90年代初,美国联邦犯罪调查实验室的主任们每年都会在华盛顿举行两次研讨会,就共同关心的问题进行讨论。他们共同创建了目前数字取证领域中享有盛誉的"数字取证科学工作组(SWGDE)"。这个工作组创先提出了"计算机潜在证据(latent evidence on a computer)"的概念,这个概念就是现在"计算机取证"(本文中所讨论的取证仅限于与计算机系统相关的证据,因此在本文中的数字取证、电子数据证据取证等概念范畴与计算机取证概念范畴等同)概念的雏形。1991年,由于计算机专家国际联盟(International Association of Computer Specialists,IACIS)在美国俄勒冈州波特兰市举行的第一次培训会中正式提出了计算机取证(Computer Forensics)的概念[10]。

20世纪90年代中期,音频及视频技术不断从模拟方式向数字方式转变[3],这使得"计算机取证"概念在数字犯罪侦察领域中显露出了它的局限性。包含数字视频和音频证据,更为广泛的新概念—"数字取证(digital evidence)"产生了,1998年3月2日在维吉尼亚州举行的美国联邦犯罪调查实验室研讨会上正式被提出。首次关于"数字取证"的讨论主要包括数字计算机证据(digital computer evidenc)、数字视频音频证据(digital audio and video evidence)等。同年5月,又举行了本年度的第二次会议,此次会议不但有各实验室的主任参加,而且他们还邀请来许多在本领域中著名的专家参与,并且这些专家在此会议中扮演了主要的角色。在这次会议中,又产生了另一个针对"数字取证"进行研究的工作组—"数字取证技术工作组(TWGDE)"。他们更多在技术层面上对"数字取证"技术进行研究。

2.2.2 计算机取证团体组织的发展 在取证科学中,不同取证学科中的专家组已逐步发展成为各种团体,它们有的开发标准、有的进行最佳的实践工作、有的探索适时可行的协议。这些团体均起始于90年代初期成立的"技术工作组(TWGs)"。在1999年,由于与FBI的一个工作组重名,而改为"科学工作组(SWGs)"。SWGs是由各种相关团体组成的一个规模较大的组织,它始终在不断的发展中。SWGs每年至少组织一次年会,其成员由50多个联邦、州的司法机关以及地方团体组成。

首次SWG年会主要处理新的取证技术—DNA的相关问题。此次会议被称为"Scientific Working Group for DNA Analysis Methods(SWGDAM)"。在1998年,FBI实验室对所有SWGs进行了一次调查[1]。其结果显示,SWGs的各种规章制度架构正在不断完善。在科学合理的制度下,SWGs具有良好的吸收优秀新成员的机制。在1999年,TWGDE转变成SWGDE。起源于SWGDE的现今SWGs的成员之一—镜像技术科学工作组(SWG-IT)加盟SWGs[1]。

2.2.3 定义数字取证"概念、标准及原则 从20世纪90年代初开始,有关制定"数字取证"标准以及提供"数字取证"检验框架的工作一直没有停止。在1993年FBI主持举行了名为"关于计算机取证的国际司法会议",来自美国各联邦、州及地方司法机构的70多位代表参加了会议,与会代表一致感到计算机取证标准的匮乏和迫切的需要[13]。在这种需求下,SWGDE在1998年8月的年会中发表了"数字取证"中相关概念的最新定义以及标准,这些定义和标准最终于1999年10月发表在"国际高技术犯罪与取证会议"上[26]。

2.2.4 数字证据的鉴定 只有采取了被取证科学界认可的"数字取证"方法,取证结果才有意义。ASCLD/LAB(The American Society of Crime Laboratory Directors/Laboratory Accreditation Board)制定了鉴定过程,清楚地说明了在取证实验操作中必须遵循的标准。SWGDE也公开表示其标准的撰写遵循ASCLD/LAB鉴定指南的要求。指南主要分为原则、标准和讨论等几类,涉及到实验管理及操作、人员资格和物理仪器等方面。

2.2.5 计算机取证实验室的建立 早期司法机关主要通过调用本单位内部一切可使用的资源来鉴别取证。这些可利用的资源通常是分散在本单位的各个部门。随着人们对计算机取证认识的不断提高,构建一个整合的实验环境,用于计算机的调查取证已成为一种趋势。美国国家保密局曾在1995年对计算机取证做过的一项调查表明,在美国有48%的司法机关已建立起了自己的计算机取证实验室,并有68%被成功捕获的计算机证据是在这些实验中完成的。这种有计划、有组织的计算机取证环境大大提高了办案的效率和准确度[13]。

在这个时期,计算机取证技术的研究经历了从无到有的探索过程,计算机取证技术的基本思想、理论、技术和方法逐步建立。

2.3 初步发展期

20世纪90年代中期,司法机关对数字证据的收集技术以及工具的需求越发强烈,这导致了数字取证(digital forensic)科学特别是计算机取证(computer forensic)科学的快速发展[19]。在此期间,信息安全领域对数字取证技术进行了较为热烈的讨论,先后出现了一些相关产品,并结合了神经网络、数据挖掘、智能推理以及知识发现等方法对关联数据进行处理。现将比较典型的几种产品介绍如下:

· Encase 由美国GUIDANCE软件公司开发,基于Windows、Linux和MAC OS等多种平台,用于法庭数据收集和分析系统,可将正在运行的系统在不停机的情况下,把系统的全部运行环境及数据生成一个镜像文件,再对该文件进行分析从而发现犯罪证据。此外它还可以记录谁在何时对证据进行了操作[8]。

· DIBS 由美国计算机取证公司开发,对数据进行镜像的备份系统。使用独特的数据镜像查证和鉴定技术,确保了单独复制的安全性和完整性[4]。

· Flight Server 由英国Vogon公司开发基于PC、Mac和Unix等系统的数据收集和分析系统。它可以将计算机犯罪现场中的计算机硬盘逐个扇区(包括环扇区)进行拷贝、复制,并生成一个物理镜像文件,然后对该镜像文件进行分析,从而帮助办案人员发现证据[29]。

· 其它产品 除了以上这些专用产品,还有一些工具也被用于计算机取证,以下列举其中几个较为常用的工具:

1. 各种密码破解程序;

2. LISTDRV:用于列出设备上的所有分区;

3. DISKIMAG:将软盘镜像备份到硬盘上,以便于进一步的分析;

4. FREESECS:用于在特定的逻辑分区上搜索未分配的或者空闲的空间,并将此间的信息保存到指定的文件中。

对计算机取证的研究中,对工具的开发与使用一直是此领域的焦点所在。尤其在这个阶段,计算机取证技术主要被商家和所应用的技术所驱动,而忽视了基本理论及基本方法的研究[2,19]。在计算机取证发展的最初阶段中,理论基础研究(如标准的取证过程和取证方法)的匮乏并不会对刚刚出现的计算机取证技术产生太大的影响,但在以后阶段中,却显得十

分突出。这种趋势导致很多针对这些工具的可靠性和有效性的攻击，其中很多攻击是无法防御的[2]。

整个计算机取证领域都对这样一个问题表示担忧—当前还没有一部国家级的计算机取证标准用于专业认证[20]。至今为止，许多认证是与某些商家的特定产品或与特定的操作系统绑定在一起，使得人们认为计算机取证领域根本就不存在通用标准。然而，取证科学的其它领域已充分显示建立本领域的统一标准是可行的，也是必须的。文[21]对此观点进行了详细的论述。

司法机关及各种社会团体对标准的缺乏，甚至对计算机取证培训课程的设置及内容都十分担忧。数字犯罪(cyber crime)的出现，使得国际上的许多司法机构已经对先前很多司法程序及司法手段的"科学"合理性产生了置疑，迫切需要对一些理论基础及科学的严密性进行证明[22,23]。美国最高法院在"Daubert v Merrell"裁定书中对下级法院提供了有关科技证据的认可标准：

- 是否所依赖的理论或技术已被测试；
- 是否所依赖的理论或技术已经过公开发表和审查；
- 所使用方法的已知或潜在的出错几率；
- 是否所依赖的理论或方法已被大多数科技组织所接受。

这些标准明显体现出司法机关对此领域基本理论与基本方法进行进一步研究的渴望，从而使得取证科学更加成熟[9,14,26]。

2.4 理论完善期

20世纪90年代后期，数字取证发展中隐含的问题越发突出，即过分关注应用产品的开发而忽视了基本理论及基本方法的研究，导致了在许多数字犯罪的侦破中的取证过程既没有一致性也没有可依据的标准。由此，业内许多专家开始对取证程序及取证标准等数字取证中的基本问题进行研究，本文在此列举此阶段较为典型的五类计算机取证过程模型进行分析，这五类模型是：基本过程模型(Basic Process Model)、事件响应过程模型(Incident Response Process Model)、法律执行过程模型(Law Enforcement Process Model)、过程抽象模型(An Abstract Process Model)和其它过程模型。

2.4.1 *基本过程模型*(Basic Process Model) 此阶段最早开始对数字取证的程序和标准等基本理论问题进行研究的是Farmer和Venema。1999年在他们主办的计算机取证分析培训班上提出了一些基本的取证过程[6]。提出的取证过程包含了一些基本的取证步骤："保证安全并进行隔离(secure and isolate)，对现场信息进行记录(record the scene)，全面查找证据(conduct a systematic search for evidence)，对证据进行提取和打包(collect and package evidence)，维护监督链(maintain chain of custody)[6]"。他们以UNIX取证过程为例，对整个取证过程进行了界定，并提出了每个步骤的操作中应遵循的基本原则，其主要思想适用于大多数的计算机系统。为了验证其理论的合理性，Farmer和Venema开发了计算机取证领域中著名的取证工具"The Coroner's Toolkit(TCT)"此工具运行于UNIX平台，主要用于数据收集。Farmer和Venema对计算机取证基本问题的研究为这个时期的数字取证发展起到了领航和奠基的作用。

尽管他们朝着正确的方向迈进了一步，但是提出的取证过程粒度较粗，也没有把在事件发生前的取证准备作为取证过程的一个阶段，他们提出的取证过程还处于初级阶段；再者，他们在TCT上的实践工作主要集中在UNIX平台。也就是说，其研究理论在其它平台上并没有实践性的工作，也没有提出切实可行的应用方法。

2.4.2 *事件响应过程模型*(Incident Response Process Model) 2001年，Chris Prosise和Kevin Mandia在"Incident Response：Investigating Computer Crime"一书中提出了事件响应过程模型的概念[11]，Mandia和Prosise所提出的事件响应过程模型是计算机取证过程中一项卓有成效的工作，他们提出的数字取证过程模型考虑得比较全面、具体，明确地提出了"攻击预防(pre-incident prepartion)"的概念，并将其作为取证程序的一个基本步骤，将取证过程延长到攻击发生之前，他们的理论较之Farmer和Venema的工作又前进了一步。Mandia和Prosise对各类典型平台(如Windows2000/NT、UNIX、Cisco路由器等)都提供了详细的使用原则和应用方法。他们对于数字取证基本方法的研究，为计算机犯罪调查的广度和深度都打下了良好的基础。尤其是"攻击预防"概念的提出，成为专业取证方法区别于非专业的关键步骤[2]。他们提出的过程模型大体分以下几个阶段：

1. 攻击预防阶段(Pre-incident Preparation)：事先进行相关培训，并准备好所需的数字取证设备。
2. 事件侦测阶段(Detection of the Incident)：识别可疑事件。
3. 初始响应阶段(Initial Response)：证实攻击事件已经发生，须尽快收集易丢失的证据(Volatile evidence)。
4. 响应策略匹配(Response Strategy Formulation)：依据现有的经验确定响应策略。
5. 备份(Duplication)：产生系统备份。
6. 调查(Investigation)：调查系统以便识别攻击者身份、攻击手段及攻击过程。
7. 安全方案实施(Secure Measure Implementation)：对被侦察的系统进行安全隔离。
8. 网络监控(Network Monitoring)：监视网络以便识别攻击。
9. 恢复(Recovery)：将系统恢复到初始状态，并合理设置安全设施。
10. 报告(Reporting)：记录相应的步骤及补救的方法。
11. 补充(Follow-up)：对响应过程及方法进行回顾审查，并进行适当的调整。

Mandia和Prosise的计算机取证步骤从整个取证分析过程来看，主要集中于证明正在运行的系统是否被攻击，以及被攻击后系统原始状态的恢复。一般来说对于整个取证过程，系统分析所占粒度应该最大，然而，在它们设计的模型中，系统分析仅占了1/11。对于一般的取证过程来说，分析阶段应分散于许多阶段中(如攻击预防阶段)。

"攻击预防阶段(Pre-incident Preparation)"概念的提出成为专业取证方法区别于非专业的关键步骤[2]，但是在这个阶段中，仅提到了"事先准备取证工具及设备，熟练取证技能，不断学习新的技术以便应对突发事件"等攻击预防中的"操作准备阶段"，而并没有从系统基本构架的角度，在敏感主机中预先安装证据收集系统，以便在攻击发生的同时对系统环境进行记录。

2.4.3 *法律执行过程模型*(Law Enforcement Process Model) 2001年美国司法部(DOJ)在"电子犯罪现场调查指南"中提出了一个计算机取证程序调查模型[28]。这个指南对不同类型的电子证据以及对其安全处理的不同方法都进行了说明。指南面向的对象是一直从事物理犯罪取证(非数字取证)的司法人员，因此重点在于满足他们的需要。而对于系统的分析涉及较少。DOJ的法律执行过程模型基本步骤为：

1. 准备阶段(Preparation):在调查前,准备好所需设备和工具。

2. 收集阶段(Collection):搜索和定位电子证据。

·保护与评估现场(Secure and Evaluate the Scene):保护现场人员的安全以及保证证据的完整性,并识别潜在的证据。

·对现场记录、归档(Document the Scene):记录包括现场的计算机照片等物证。

·证据提取(Evidence Collection):提取计算机系统中的证据,或对计算机系统全部拷贝。

3. 检验(Examination):对可能存在于系统中的证据进行校验与分析。

4. 分析(Analysis):对检验分析的结果进行复审和再分析,提取与对案件侦破有价值的信息。

5. 报告(Reporting):对案件的分析检验结果汇总提交。

此过程模型基于标准的物理犯罪(Physical Crime)现场调查过程模型。作为事件响应模型,它对于检验和分析过程没有给予较多的关注,然而在数字取证过程中,这两步占了相当大的比重[31]。

另外,此模型将硬盘作为电子证据收集的对象之一,这容易引起概念上的混淆。在调查中,办案人员不知道是否硬盘中存有案件相关的电子证据。在一般概念上,首先应确定电子证据的存储位置,然后进行提取,但在这个模型中在确定电子证据的存储位置之前就对所谓的电子证据进行提取了。因此,收集阶段更准确地说是对物理证据的收集,当对被收集的物理证据进行检验分析时才对电子证据定位和提取。

2.4.4 过程抽象模型(An Abstract Processs Model)

在数字取证基本理论和基本方法研究中,过程抽象模型(An Abstract Process Model)的研究被认为具有里程碑的作用[28]。本小节将对两项较具代表性的研究成果进行分析。

2.4.4.1 AIRFORCE 过程抽象模型

美国空军研究院在计算机取证的基本方法和基础理论方面也进行了进一步的研究工作。通过对以前方法的总结,他们敏锐地意识到在特定技术及特定方法细节上的研究无法总结出普遍的取证方法,同时发现各种不同的取证过程模型都存在共同的特性,因此可将这些模型抽象为一个通用的模型。由此,他们对特定方法的取证过程进行抽象。抽象的结果产生了具有普遍意义的数字取证程序,这种研究的意义十分明显:

·使得传统的物理取证知识应用于数字子取证中;

·使得数字取证程序的研究真正由计算机取证扩展到数字取证。

这种开创性的工作,为数字取证技术基本方法和基本原理的进一步研究奠定了良好的基础,使得数字取证的研究又迈上了一个新台阶。对此模型的简要介绍如下,此模型分为以下几个阶段:

1. 识别(Identification):侦测事件及犯罪。

2. 准备(Preparation):准备工具、技术及所需的许可。

3. 策略制定(Approach Strategy):制定策略来最大限度地收集证据和减小对受害者的影响。

4. 保存(Preservation):隔离并保护物理和数字证据。

5. 收集(Collection):记录物理犯罪现场并复制数字证据。

6. 检验(Examination):查找犯罪相关证据。

7. 分析(Analysis):对检验结果进行再分析,给出分析结果。并重复检验过程,直到分析结果有充分的证据及理论的支持。

8. 提交(Presentation):总结并对结论及所用理论提供合理的解释。

在实际中,"准备"阶段应放在"识别"阶段之前,以便在攻击发生之前提早做好人员及设备的预备工作。此模型与第一届数字取证工作组(DFRWS)年会[5]中提出的模型有许多相同的地方,所不同的是对每一阶段进行了详细的描述。

尽管此模型的提出意义重大,但也有一些问题存在:

此模型使用了"检验(Examination)"和"分析(Analysis)"阶段来识别和提取数字证据。由于其含义仅存在细微的不同,因此这两个阶段常被混淆。检验(Examination)的定义是"研究或分析(study or analysis)",分析(Analysis)的定义是"一种系统的检验,也就是说通过将对象拆分成多个不同的部分,研究其相互之间的关联"。很显然这两个阶段的含义是不同的,但其名称上的近似常常会引起混淆。

2.4.4.2 DOJ 过程抽象模型

与此同时,美国司法部(The U. S. Department of Justice, DOJ)也提出了类似的过程抽象模型的思想:不同的取证过程模型都存在共同的特性,因此可将这些模型抽象为一个通用的模型。由此,他们对特定方法的取证过程进行抽象,抽象过程包含收集(collection)、检验(examination)、分析(analysis)、报告(reporting)等过程[28]。

不仅如此,DOJ 对各种电子设备中可能存在的证据类型、潜在的存储位置和犯罪类型进行了分类整理。这种在不同电子设备上,对各种类型的潜在证据的识别和定位的研究是数字取证科学基本理论的又一次发展,它为进一步开发具有普遍意义的数字取证程序及标准奠定了良好的基础,使得侦案人员遵照数字取证标准,采用普遍的数字取证方法,采取由一般到特殊的科学过程对具体案件进行侦察成为可能。尽管 DOJ 在这方面的研究工作刚刚开始,但真正触及到了数字取证研究的核心部分。数字取证基础理论和基本方法研究的序幕拉开了。

遗憾的是,此模型以及前面提到的 AIRFORCE 过程抽象模型都使用了"检验(Examination)"和"分析(Analysis)"这两个常被混淆的阶段来识别和提取数字证据。

2.4.5 其它过程模型 由美国空军研究院、美国信息战督导/防御局共同资助的计算机取证组织—数字取证研究组(Digital Forensics Research Workshop, DFRW)对于数字取证领域的基本方法和基本理论的研究也是十分明显的。其独特之处在于它是由学术界领导的第一个较大规模的、致力于数字取证基本理论及方法研究的联盟组织。

目前在学术界存在的最大问题是在其研究过程中即没有标准的数字取证分析过程及协议,也没有标准的术语[5]。在 2001 年召开的 DFRW 的一届年会上,这个工作组提出了此组织近期将要解决的问题:

·定义计算机取证科学的基本框架;

·探讨如何确定数字证据的真实性及可靠性;

·探讨发现及恢复隐藏数据;

·探讨网络取证的基本理论及方法。

并提出了一个初步的计算机取证科学的基本框架,框架包括"证据识别、证据保存、证据收集、证据检验、证据分析、证据保存和提交"[5]。基于这个框架,科技界可以对数字取证基本理论和基本方法进一步的发展和完善。

DFRW 的创立对于学术界在数字取证领域中的发展方向的定位,凝聚发展力量起到了推动作用。

2.5 国内计算机取证研究概况

在我国计算机证据出现在法庭上也只是近几年的事情,

有关计算机取证的研究与实践尚在起步阶段，只有一些法律法规涉及到了一些计算机证据，如《关于审理科技纠纷案件的若干问题的规定》、《计算机软机保护条例》等。目前我国法庭案件中出现的电子证据还比较简单，如电子邮件、程序源代码等，不需要使用特殊的工具就能得到。我国计算机取证工作无论是在技术、人们的意识形态，还是在法律执行部门与发达国家都存在一定差距：

·首先，技术上还缺乏自主知识产权的优秀计算机取证工具，许多企业和政府部门的网络甚至金融系统受到攻击造成重大损失时没法收集证据，使犯罪者逍遥法外；

·其次，在人们的意识当中信息安全仅仅停留在被动防护的概念，只是尽量将自己的网络和数据保护好，殊不知再好的安全防范措施也会随着技术的发展或人员的误操作而变得不安全；

·最后，由于计算机取证的高科技性，需要有专门的司法机构，同时还需颁布相关的法律法规，规范计算机取证。

目前，国家有关部门非常重视对打击计算机犯罪的研究，组织相关单位开展了相关课题的研究，目前在研究的课题有：

·2000年5月，公安部制定了《打击计算机犯罪攻关思路》，确立了以办理计算机犯罪为主线，以电子数据证据为核心，以计算机犯罪侦察为主要内容的技术攻关思路。北大、同济、复旦等高校，金诺网安、启明星辰等企业参与了相关的研发工作；

·国家863计划之子课题—电子物证保护与分析技术；

·公安部Internet侦控管理系统；

·国家"十五"重点攻关项目—打击计算机犯罪侦查技术研究；

·中国科学知识创新工程重大项目之子项目，由中国科技大学和中科院高能物理所共同承担。

目前国内出现的计算机取证产品：

·中科院高能物理所计算机中心他们推出一部称为"取证机"的机器，据介绍，这部机器可以侦探黑客的入侵手段，向人们提交分析报告，并将成为法庭上合法的呈堂证供；

·厦门美雅博科技有限公司主持开发的计算机证据侦察箱，具有证据的提取、破解、分析和恢复等功能。

由于计算机犯罪侦察技术专业性很强，从国外引进的打击计算机犯罪技术和设备的速度远远滞后于计算机技术的发展，导致了目前政法机关在打击计算机犯罪方面的技术落后，设备老化，难以适应实战的需要。因此，急需有效组织社会资源，着手防范和打击计算机犯罪的技术研究。高校和科研单位应在理论上和实践中探讨计算机取证技术，并开发有自主知识产权的计算机取证工具，为政法机关打击计算机犯罪提供技术依据和理论的支持。

总结 电子数据取证是一门近几年来兴起的集取证科学、计算机科学和行为证据分析等学科为一体的边缘科学。本文从技术原则和法律原则两方面对电子数据取证领域的基本状况进行了描述。从技术原则的角度来看，有关电子数据取证的概念、标准、基本开发方法等基础知识比较零碎，相关的取证工具也十分繁杂且不规范。本文对已有的电子数据取证的概念进行了分析和总结，系统地描述了电子数据取证领域的相关概念；以此领域较为突出的事件为线索，对电子数据取证研究的产生、发展进行了描述，并以此为基础，总结了此研究领域存在的不足。从法律原则方面，以现存的法律法规为基础，对电子数据证据的法定形式，证据力及证明能力进行了讨论，明确了电子数据证据作为呈堂证供应满足的条件。

参考文献

1 Adams D E, Lothridge K L. Scientific Working Groups. Forensic Science Communications, 2000, 2(3)

2 Carrier B, Spafford E. Getting physical with the digital forensics investigation. International Journal of Digital Evidence, Winter 2003

3 Casey E. Digital Evidence and Computer Crime. Academic Press, 2001

4 Computer Forensics, et al. http://www.computer-forensics.com

5 Digital Forensics Research Workshop. A Road Map for Digital Forensics Research. www.dfrws.org, 2001

6 Farmer D, Venema W. Computer Forensics Analysis Class Handouts. http://www.fish.com/forensics/class.html, 1999

7 Fisch E A, White G B, et al. The Design of An Audit Trail Analysis Tool. IEEE, 1994

8 Guidance Software. inc. http://www.encase.com

9 International Organization on Computer Evidence. Digital evidence. standards and principles. http://www.fbi.gov, May 2003

10 Isner J D. Computer Forensics: An Emerging Practice in the Battle Against Cyber Crime. SANS Institute. 2003

11 Mandia K, Prosise C. Incident Response. Osborne/McGraw-Hill, 2001

12 Rogers M K, Seigfried K. The Future of Computer Forensics: Needs Analysis Survey: [CERIAS Tech Report]. 2003

13 Noblett M G, Pollitt M M, Presley L A. Recovering and Examining Computer Forensic Evidence. Forensic Science Communications, 2000, 2(4)

14 New Technolgoies Inc. Junk sicence legal challenge explained. http://www.forensics-intl.com/def14.html, June 2003

15 Palmer G. A Road Map for Digital Forensic Research. Digital Forensic Research Workshop(DFRWS), Aug. 2001

16 Parra M. Computer forensics. 2002. http://www.giac.org/practical/Moroni_Parra_GSEC.doc

17 Reith M, Carr C, Gunsch G. An examination of digital forensic models. International Journal of Digital Evidence, Spring 2002

18 Richardson R. CSI/FBI 2003 computer crime survey. http://www.gocsi.com. June 2003

19 Rogers M. The role of criminal profiling in computer forensic investigations. Computers and Security, 2003(4)

20 Rogers M. Computer forensics: Science or fad. Security Wire Digest, July 24, 55(5)

21 Saferstein R. Criminalistics: An introduction to forensic science. New York: Prentice Hall, 2001

22 Smith F, Bace R. A guide to forensic testimony: The art and practice of presenting testimony as an expert technical witness. Boston, MA: Addison Wesley

23 Sommer P. Computer Forensics: An Introduction. http://www.virtualcity.co.uk/vcaforens.htm, 1997

24 Sommer P. Digital Footprints: Assessing Computer Evidence. Criminal Law Review Special Edition, Dec. 1998. 61～78

25 孙波，孙玉芳，等. 电子数据证据收集系统保护机制的研究与实现. 电子学报，2004

26 Scientific Working Group on Digital Evidence and International Organization on Digital Evidence. Digital Evidence: Standards and Principles. Forensic Science Communications, 2002, 2(2)

26 Scientific Working Group on Digital Evidence. SWGDE draft best practices. http://ncfs.ucf.edu/digital_evd.html, June 2003

28 Technical Working Group for Electric Crime Scene Investigation. Electronic Crime Scene Investigation: A Guide for First Responders. 2001

29 Vogon International Limited. http://vogon-data-recovey.com

30 王玲，钱华林. 计算机取证技术及其发展趋势. 软件学报，2003, 14(9)

31 Alec Yasinsac. Policies to Enhance Computer and Network Forensics. In: Proc. of the 2001 IEEE Workshop on Information Assurance and Security, June 2001