文章编号：2095-2163(2020)02-0151-03 中图分类号：TP309 文献标志码：A

网络犯罪下电子取证技术研究与探索

李玲俐
（广东司法警官职业学院，广州 510520）

摘 要：针对网络犯罪下的电子取证技术进行了研究和探索。分析当前网络犯罪的特点，提出网络取证研究的重要性，为能有效提高网络犯罪下的办案效率，概述了电子取证的定义和特点，阐述了目前电子取证的关键技术，以及中国电子取证在技术和法律层面面临的挑战，最后对网络犯罪下电子取证技术做了总结，并提出今后的研究重点。

关键词：网络犯罪；电子取证；电子证据；反取证；云取证

Research and exploration of cyber-crime electronic forensics technology

LI Lingli
（Guangdong Justice Police Vocational College, Guangzhou 510520, China）

【Abstract】 The paper studies and explores the electronic forensics technology under the network crime, analyzes the characteristics of the current Internet crime, and puts forward the importance of network forensics research. In order to effectively improve the processing efficiency of the case under the network crime, the paper correspondingly introduces the definition and characteristics of electronic evidence, expounds the key technology of the electronic forensics, and the technical and legal challenge of the electronic forensics in China. Finally, the paper summarizes the technology of electronic forensics under the network crime, and points out the research emphasis in the future.

【Key words】 cyber-crime; electronic forensics; electric evidence; anti-forensic; cloud forensics

0 引 言

大数据、云计算等现代科技发展迅猛，电子取证结合现代侦查技术成为网络犯罪涉案中非常关键的取证方式，大量从事计算机技术和法律范畴的学者们对电子取证进行了深入的研究。文献[1]分别对基于 Windows、基于智能手机、基于网络的电子取证方法和技术进行了综述；文献[2]通过分析网络犯罪中电子证据的特殊性、电子取证技术的意义，提出电子取证的收集和保全方法；文献[3]提出一种网络犯罪案件中能提高电子取证分析效率的溯源策略。由于网络犯罪分子的犯案手段日渐灵活，电子取证在技术和法律层面都有其优缺点，本文分析网络犯罪的特点，详细探讨了网络犯罪中电子取证的关键技术，继而阐述了中国电子取证的技术和法律两个方面都有待完善，最后提出未来的研究方向。

1 网络犯罪的特点

在全球信息化的今天，计算机网络的普及和飞速发展，云计算、大数据、人工智能等广泛应用，为人们的工作和生活带来很大的便利，数据共享、即时聊天、语音视频、网络会议、电子商务、电子政务等都成为不可或缺的一部分。这样的社会背景下，网络安全事件已然引起各界的关注与重视，网络钓鱼、病毒、木马、黑客攻击、网络诈骗、新 APT(高级持续性威胁，Advanced Persistent Threat)组织、数据隐私、勒索软件等凡是能获取经济利益的行为，时刻威胁着电子商务的安全运行，犯罪分子的目标是网银中的钱、虚拟货币和有价值的资料信息等，逐步形成一条环环紧扣的灰色产业链[4]。

网络犯罪利用互联网的便捷实施犯罪行为[5]，从事网络犯罪活动的大部分是高智能的专业犯罪人员，有其特殊的犯罪手段。个人做案，反侦察能力不强，但隐匿性高；团体做案，分工明确，有较高的反侦察能力和流窜性。部分犯罪分子具备一定的网络技术和信息安全知识，能通过一些手段将证据隐藏或者瞬间销毁，使取证调查难以发现其犯罪行为，这就使得取证技术在不断进步的同时，反取证技术也在悄然地发展着。反取证技术一般有数据加密、数据隐藏和数据清除三种[3]，给取证工作增加了很大难度。网络犯罪的危害不容忽视，电子取证的研究显得重要和紧迫。

2 网络犯罪中的电子取证研究

2.1 电子取证概述

2.1.1 电子取证的定义

1991 年，美国举行第一届计算机调查专家国际

作者简介：李玲俐(1977-)，女，教授，主要研究方向：数据挖掘、模式识别、网络安全。

收稿日期：2019-10-24

会议 IACIS(International Association of Computer Investigative Specialists),首次提出计算机取证(Computer Forensics)(也称为电子取证)的概念。2012 年,中国修改的《刑事诉讼法》中,“电子数据”被正式归为法定证据的种类之一。电子数据是指能证明案件事实的电子信息和数据资料,即电子证据(Digital Evidence)。电子取证是指对计算机系统以及网络中相关的电子证据进行获取、保存、辨析和提交的过程。随后,电子取证技术快速发展,逐渐成为一门融合计算机科学、法学、心理学、侦查学等在内综合性、交叉性的学科。

2.1.2 电子证据的特点

网络犯罪案件侦查过程中,通常要用到的电子证据,其目的是为了调查、分析和恢复从各种电子设备中采集到的数据信息[6-7]。电子证据易于存储、传送方便快捷、便于操作[8]、可以多次被复制,有以下特点。

(1)无形性。调查取证过程中,通常要用到的电子证据是以数字化形式存在的载体,用硬盘、磁盘、U 盘和智能卡等磁性物理介质保存。

(2)多样性。电子证据的内容有文本、图像、音频、视频和计算机编码等多种数据信息。

(3)消失性。计算机故障、病毒、误操作、恶意删除等都有可能使电子证据消失。

(4)动态性。网络犯罪案件中,除了用静态存储设备储存的数据,更多的电子数据是网络数据,动态电子证据涉及到对象、时间、地点、技术等方面,对电子取证的技术设备和取证人员的专业素质都提出了更高要求。

(5)实时性。电子数据在网络中传输时会自动生成日志记录,包括数据生成的时间、大小、属性等。日志是侦查取证过程中非常重要的电子证据来源,在某种程度上,电子数据的实时性为取证人员侦查取证提供了很大的帮助,但是由于大部分网络数据存储在云端服务器,有时间和空间的限制,不同的服务器提供商支持的数据格式可能不一样,为取证工作增加了准确、及时的客观要求[5]。

(6)分散性。电子数据在生成、传输、存储等过程中,分散在网络的各个部分,有些犯罪分子会清除犯罪痕迹,加大了各项数据的取证工作的难度。

网络犯罪下的电子取证技术和过程是传统取证的发展和延伸,电子证据的生成、传输、接收、存储、收集等每一个步骤都要求电子取证必须全面、及时、真实、合法,才能保证电子取证工作的顺利进行[8]。

2.2 网络犯罪下电子取证的关键技术

网络犯罪的技术和手段越来越高级,电子取证所需要的技术也越全面,涉及到法律、网络信息安全、数据挖掘、人工智能等各个领域,目前主要有下面几种常用的关键技术。

(1)数据备份。也叫数据复制,是指将全部或部分数据集合、数据库从原主机的硬盘或阵列复制到其它存储介质的过程。包括拷贝、拍照、摄像、镜像等方法,保证备份数据和原数据的一致性和完整性。

(2)数据恢复。网络犯罪分子通常将与犯罪事实有关的电子证据篡改、删除或破坏,为取得有效证据,专业人员需要在存储介质的存储区域没有严重受损的情况下,通过各种数据恢复工具把修改、遭到破坏、甚至丢失的数据还原为原始数据。

(3)数据加解密。数据加密是信息保护的主要方法之一,将密钥和加密算法加密后的密文在公网中传递,以保证数据的机密性、完整性和可用性。如果犯罪嫌疑人不愿意提供密码,侦查人员必须通过各种手段获得,除了嫌疑人的计算机、智能卡等存储设备,也可能利用暴力破解等方式获得其口令或密钥,再采用解密技术将密文恢复为明文。

(4)数字签名和时间戳。数字签名用于鉴别数字信息,证明消息发布者的身份;时间戳提供一份电子证据,证明数据生成时间[9]。数字签名和时间戳的抗抵赖性能证明数据的完整性和有效性。侦查人员通常要对有时间的信息内容进行标记。

(5)入侵检测系统(Intrusion Detection System,IDS)取证。IDS 是一种能够通过分析系统安全相关数据来检测入侵活动的系统,依照一定的安全策略,对系统和网络的运行状况进行监控,尽可能识别各种非法攻击[10],同时收集相关的电子证据,包括日志记录、攻击的行为结果、网络流量的变化,并进行分析[11]。

(6)数据挖掘。数据挖掘是从海量数据中获得有价值信息,在大数据时代,这是不可或缺的取证技术。在动态地址取证阶段,数据挖掘技术中的基于关联规则的分类方法可以对犯罪嫌疑人的非法行为进行对比判断,挖掘出对破案有利的证据。

除了以上关键技术,还有数据抓取、安全扫描、日志分析、蜜罐技术、恶意代码、网络监听等电子取证技术,取证人员通过对数据的分析和比对,将有效的数据串联起来,作为判案所需的电子证据。

2.3　中国电子取证的挑战

电子取证对犯罪案件的调查和侦破起着非常重要的作用，是传统取证技术的重要补充。当前形势下，网络犯罪下的电子取证工作面临的挑战主要体现在如下 3 个方面。

(1)电子取证相关法律程序不完善。目前，中国现有法律制度对电子取证的程序的规定还在完善之中，实践应用中电子证据的合法性、有效性有待明确。例如，侦查员具有很强的法律意识、隐私权和人权保护意识，但很多时候隐私数据和非隐私数据没有严格的界定，导致在取证过程中往往无法确定哪些是法律范畴内能获得的电子证据。

(2)电子证据取证难、认证难[12]。其一，侦查员很难将嫌疑人或者其设备扣押而进行取证，即使可以，由于嫌疑人经常更换设备，比如计算机网卡、手机等，或者直接破坏硬件、覆盖原始数据。其二，取证时间越长，犯罪痕迹可能被海量数据淹没，例如有些嫌疑人在网上租用的云储存服务器，租约到期云服务器中的数据被释放，或者云服务器失效导致数据不可恢复；又例如嫌疑人在取证前删改、伪造原始数据，侦查员无法判断其完整性和真实性，更不能作为判案的依据。

(3)电子取证人员需要具备行业领先的高素质。互联网时代的犯罪分子通常具备高科技设备和技术，电子证据易篡改、易受破坏性、易实时变更，搜集和司法鉴定变得复杂，取证人员必须拥有专业过硬的取证技术[1]，进行全面的分析，提取有价值的证据。目前，中国的电子取证高素质专业人员的相对匮乏，使得很多取证工作不够全面、不够合理、不够及时，达不到预期的效果。

3　结束语

本文阐述了网络犯罪的特点，对电子取证现状和关键技术进行分析，提出目前中国电子取证所面临的挑战。随着新时代电子技术、信息安全、智能手机的高速发展，网络犯罪下电子取证的难点是如何在虚拟网络世界中拿捏好侦查权，如何获得并确保取证人员获得的电子数据能够作为对判案有效的电子证据，如何在整个取证过程中保障人权和隐私权[13]。未来研究方向除了将上述关键技术继续发展和提升外，还有 2 点可做阐释分述如下。

(1)基于区块链的电子取证技术。区块链是中心化、去信任化的数据库，涉及密码学、数字签名、时间戳、分布式数据存储、共识机制等计算机及网络安全技术，能够安全存储比特币及其交易，也可以存储其它数字资产，网络犯罪分子将无法篡改和伪造区块链中的电子证据[14]。

(2)云取证技术。云时代，各种云服务为人们带来便利，大量与人们工作生活相关的数据信息储存在云端，这些电子资料成为犯罪分子的主要目标。云取证是云计算和电子取证相结合的产物，传统的电子取证工具、技术和框架得到变更[15]，取证人员在云取证过程中涉及到的调查范围更大、技术性更强、用法更全面。到目前为止，云取证发展时间比较短，面临数据分散、技术和法律问题，但也会带来新的机遇，云取证势必会在将来云计算犯罪调查方面有着重要的应用前景。

参考文献

[1] 蒲泓全，郭艳芬，卫邦国. 电子取证应用研究综述[J]. 计算机系统应用，2019,28(1):10.

[2] 李小良. 网络犯罪中电子证据的收集及保全分析[J]. 法制与社会，2016(32):258.

[3] 李志刚，朱巨军. 一种计算机网络犯罪案件电子取证的溯源策略研究与实践[J]. 网络安全技术与应用，2017(1):137.

[4] 刘建军，陈光宣，秦子惠. 浅析当前网络犯罪特点及取证对策[J]. 网络安全技术与应用，2012(6):4.

[5] 王玉龙. 网络犯罪电子取证的程序规范[J].公安学刊(浙江警察学院学报)，2015(2):32.

[6] REITH M，CARR C，GUNSCH G. An examination of digital forensic models[J]. International Journal of Digital Evidence，2002，1(3):1.

[7] CARRIER B. Defining digital forensic examination and analysis tools using abstraction layers[J]. International Journal of Digital Evidence，2003，1(4)：5.

[8] 百度文库. 电子取证特性及电子取证方法[EB/OL].(2018-06-30)[2019-08-18]. https://wenku.baidu.com/view/de1737c40066f5335b8121be.html

[9] 百度百科. 时间戳[EB/OL].[2019-08-18]. https://baike.baidu.com/item/时间戳/6439235?fr=aladdin.

[10] 吴疆. 刑事案件网络电子取证研究[D]. 杭州：浙江大学，2019.

[11] 吴绍兵. 云计算环境下的电子证据取证关键技术研究[J]. 计算机科学，2012,39(S3):139.

[12] 邓强，李军辉，李金月.电子证据取证存在的问题与对策探析[J]. 电脑知识与技术，2015,11(20):14.

[13] 季晨. 论网络诈骗案件中的电子取证[D]. 杭州：浙江大学，2018.

[14] 徐蕾. 基于区块链的云取证系统研究与实现[D]. 绵阳：西南科技大学，2017.

[15] RUAN K,CARTHY J,KECHADI T,et al. Cloud forensics[M]// PETERSON C，SHENOI S. Advances in Digital Forensics VII. Berlin：Springer，2011：35.