计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(1):10−16 [doi: 10.15888/j.cnki.csa.006707]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

电子取证应用研究综述①

蒲泓全[1,2,3], 郭艳芬[1,2], 卫邦国[3]

[1](中国科学院 成都计算机应用研究所, 成都 610041)
[2](广西混杂计算与集成电路设计分析重点实验室, 南宁 530006)
[3](成都市武侯区人民检察院, 成都 610041)
通讯作者: 蒲泓全, E-mail: 774149765@qq.com

摘　要: 近年来, 电子数据取证对案件侦破起着重要的作用, 由于电子数据具有易失性、易破坏性等特点, 需要取证人员具备专业的电子取证技术和方法, 才能最后分析出有用的证据, 保证案件的真实性和客观性, 详细分析三种取证技术和方法: 基于 Windows 的电子取证、基于智能手机的电子取证, 基于网络的电子取证, 其中基于智能手机的电子取证包括 Android 手机和 iPhone 手机, 并提出电子取证技术未来的发展方向.

关键词: 电子取证; Windows; 智能手机; 网络取证

引用格式: 蒲泓全,郭艳芬,卫邦国.电子取证应用研究综述.计算机系统应用,2019,28(1):10–16. http://www.c-s-a.org.cn/1003-3254/6707.html

Survey on Electronic Forensics Research

PU Hong-Quan[1,2,3], GUO Yan-Fen[1,2], WEI Bang-Guo[3]

[1](Chengdu Institute of Computer Application, Chinese Academy of Sciences, Chengdu 610041, China)
[2](Guangxi Key Laboratory of Hybrid Computation and IC Design Analysis, Nanning 530006, China)
[3](The People's Procuratorate of Wuhou District of Chengdu, Chengdu 610041, China)

Abstract: In recent years, electronic data forensics has played an important role in the detection of cases. Because the electronic data have the characteristics of vulnerability, in order to finally analyze the useful evidence, it is necessary for the forensics personnel to have professional electronic forensics technology and methods to ensure the authenticity and objectivity of the cases. Three kinds of forensic techniques are analyzed in detail: electronic forensics based on Windows, electronic forensics based on smart phones, and electronic forensics based on network. Electronic forensics based on smart phones, include Android mobile phone and iPhone mobile phone. And the future development direction of electronic forensics technology is put forward as well.

Key words: electronic forensics; Windows; smart phone; network forensics

引言

近年来, 信息技术和智能手机普及率迅速增加, 为人们生活带来方便的同时, 也为违法犯罪分子提供了科技方法和手段, 因此电子数据的提取显得尤为重要, 由于电子数据具有易删除、易覆盖、易篡改、易灭失等特点, 影响到电子数据的真实性, 所以电子数据取证技术对固定电子数据、保持电子数据原始性提供了可能[1,2].

1991 年, 在美国召开第一届国际计算机调查专家会议, 首次提出"计算机证据"的概念, 此后电子取证技术得到快速的发展, 形成一门计算机学科、法学学科与侦查实践的交叉学科[3], 下面基于 Windows、Android 手机、iPhone 手机、网络的电子数据取证技术和方法进行深入分析, 并提出电子数据取证未来的发展方向.

① 基金项目: 广西混杂计算与集成电路设计分析重点实验室开放基金 (HCIC201701)
Foundation item: Open Fund of Guangxi Key Laboratory of Hybrid Computation and IC Design Analysis (HCIC201701)
收稿时间: 2018-05-26; 修改时间: 2018-06-19; 采用时间: 2018-07-10; csa 在线出版时间: 2018-12-07

1 Windows 电子取证

电子数据主要存储在计算机中, Windows 操作系统是计算机普及度最高、使用范围最广的操作系统. 因此针对 Windows 系统的电子数据取证始终是电子取证研究方向的主流[4–6], Windows 操作系统版本较多, 下面内容都是基于 Windows 7.

1.1 浏览器取证

浏览器是一种在万维网 (www) 中用于检索、展现及传输信息资源的应用客户端. 目前国内外主流的浏览器有: IE、Chrome、Firefox、Opera、QQ、搜狗、360、傲游等. 虽然浏览器种类繁多, 内核也有差异, 但用户在使用浏览器访问互联网上的资源后, 会在计算机的硬盘上留下痕迹, 其中包括: URL 访问控制列表、缓存 (Cache)、Cookies 等资源信息. IE 浏览器是目前使用最多最为广泛的浏览器, 不同的 IE 浏览器版本也会存在一些差异, IE5–IE9 采用了相同工作机制和数据存储方式, IE10 以上版本则采用了全新的方式, 下面对 IE10 版本进行深入分析. 从电子数据取证角度来看, 新版本浏览器 IE10 最大的变化是使用一个全新的 WebCacheV01.dat 的数据库文件代替传统的 index.dat, 该文件是一个可拓展存储引擎 (ESE) 的数据库, ESE 可扩展存储引擎是一种灵活度很高的数据库类型, 数据库大小可以是 1 MB, 也可以达到 1 TB. 最重要的是当某条记录被数据库移除后, 其占用的空间会被标记为删除但数据库并不会执行覆盖操作, 那么原始记录可能还存在未被分配的区域内, 这就为数据恢复提供了可能[4,5]. IE10 相关数据文件详细信息如表 1 所示.

表 1 IE10 相关数据文件

文件类型	文件名
检查点文件	WebCacheV01.dat
事务日志文件	V01.chk
预留事务日志文件	V01.log
事务日志文件	V01#####.log

在 WebCacheV01.dat 数据库查询“Name”字段中名为 History、Content、Cookies 类别对应的 ContainerID, 然后再分别查询其对应的 Container_##表即可获得对应的 URL 访问控制列表、缓存和 Cookies 资源信息.

1.2 电子邮件取证

电子邮件是互联网中运用最为广泛的应用之一, 很多针对计算机的电子取证都涉及到对电子邮件的取证, 电子邮件可以通过客户端, 使用 POP3/IMAP、SMTP 协议收发电子邮件, 也可以通过网页方式在线使用, 使用 HTTP 协议收发电子邮件, 目前来说, 使用 HTTP 在线收发电子邮件因为本地不留存全部数据, 取证相对困难, 基于电子邮件取证步骤如下[6]:

(1) 查看电子邮件存储位置, 不同电子邮件存储位置不同, 可通过默认安装路径进行寻找.

(2) 查看邮件头, 邮件头作为电子邮件最重要的部分, 存储了电子邮件传输过程的重要信息, 取证人员可利用邮件头定位发送者的 IP 地址. 部分在线收发邮箱不允许直接查看邮件头, 需要经过其他方法操作方能查看, 例如 QQ 邮箱需要通过“显示邮件原文”来获取邮件头信息. 图 1 是用显示邮件原文获取的 QQ 邮件头.

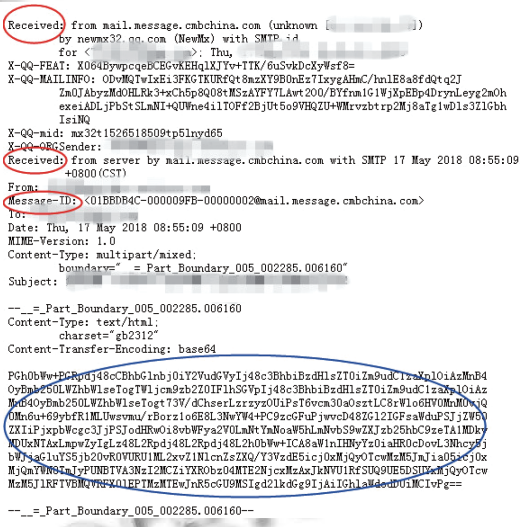

图 1 QQ 邮件头

(3) 分析邮件头, 只要不是用代理服务器和高级的密码学技术, 电子邮件中总会暴露发件人身份的有用信息. Received 和 MessageID 是追踪电子邮件最有用的两类电子邮件信息, 上图中用红色椭圆标记的部分. 因为 Received 信息是由服务器自动加上去的, 攻击者无法伪造, 除了包含发件人和收件人信息, 还包括 IP 地址, 这对于取证结果是不可抵赖的. Message-ID 是邮件系统在创建邮件时自动生成的唯一编号, 不可能两封邮件出现同一个编号, 同时不会被邮件系统回收, 当计算机上的邮件被删除之后, 可通过检查邮件服务代理 (MTA) 上的发送记录寻找 Message-ID, 然后通过 Message-ID 来确定发送主机的 IP 地址.

(4) 查看邮件内容

目前大多数邮件编码方式都是遵循 MIME 编码标

准, 邮件头中的内容不经过解码是无法查看的, 上图中用蓝色椭圆标记的即为邮件内容, 需要专门的解码器进行查看, 例如: Encase、乱码查看器等.

1.3 内存取证

计算机中运行的程序都存储在内存 (RAM) 中, 用于记录 CPU 运算的临时数据以, 因此 RAM 中存放了程序运行过程中最重要的状态信息. 例如: 运行的程序、打开文件的窗口函数等. 计算机木马可能处于某一目的, 在取证过程造假, 修改数据, 但是应用程序和数据在内存中却是真实存在的, 因此针对仅存于内存中, 关机就消失的木马程序, 内存取证是唯一的方式. 首先内存取证的前提是内存的获取, 而且必须在开机的状态下获取, 可以使用相关的工具进行获取, 例如: Winpmem、KnTTools 等. 内存获取之后进行内存分析, 2005 年电子取证研究工作组 (DFRWS) 首次提出针对内存取证的挑战, 之后对内存中保存的数据结构分析作为内存分析的重点, 也有相关的分析工具供取证人员使用, 例如: memparser、kntlist 等.

2 智能手机电子取证

目前智能手机使用率最高的是 Android 手机和 iPhone 手机, 针对这两类手机取证技术进行详细介绍和分析.

2.1 Android 手机取证

Android 是目前智能手机市场上最为流行的智能手机操作系统, 因此成为取证人员关注度最高的手机操作系统之一. 基于 Andorid 手机的取证技术包括物理取证和逻辑取证[7–9], 图 2 是 Android 手机取证的一般模型.

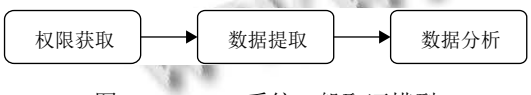

图 2 Android 系统一般取证模型

2.1.1 Andorid 系统

Android 系统是基于 Linux 内核完全开源的操作系统, 任何用户均可根据自己的需要修改源代码并设计自己的操作系统. Android 系统分为五个部分组成: 应用程序和插件、应用程序框架、库、Andorid 运行库、Linux 内核. Linux 内核提供了 Android 系统最底层的一些功能, 包括: 进程间通信驱动、Flash 驱动、USB 驱动、电源管理等等. 在 Linux 内核上的库是实现 Android 系统自带程序运行的基础, 这些库包括: SQLite、WebKit、SSL、Surface Manager, 所有的库运行在虚拟环境中, 这就构成了 Android 系统的应用程序运行环境.

2.1.2 Android Debug Bridge

Android Debug Bridge 又称为 ADB, 是取证人员针对 Android 手机取证经常接触到的一个工具, 属于 Android SDK, 包括服务器端和客户端, 其主要作用是在客户端建立和服务器端的通信, 提供通过客户端执行服务器端 Shell、上传/下载文件、建立各种连接并进行映射以及安装 apk 程序等功能. 默认情况下, Android 手机的 ADB 功能是关闭的, 需要手动进行开启 USB 调试模式, 并同时需获得手机的 root 权限.

2.1.3 逻辑取证

目前所有逻辑取证软件与手机端的通信均是同时 ADB 完成. 得到相应的系统文件后, 进行解析获得短信、通讯录、通话记录等一系列应用程序信息的过程.

Android 操作系统中大部分的数据使用 SQLite 数据库进行存储[7], 包括 SMS 短信、MMS 彩信、联系人、通话记录等常见的各种信息, 所以除了使用现成的手机取证工具外, 还需将对应的文件从 Android 手机中提取出来, 使用相应的软件进行分析, 从而实现对于 Android 手机的逻辑数据提取. 逻辑取证的前提是获取手机的 root 权限.

2.1.4 物理取证

通过 ADB 的逻辑数据取证针对的是手机中还存在的数据, 通常情况下, 手机中还存在被删除的信息, 这部分信息才可能是取证人员关心的数据, 这种被删除的数据无法通过逻辑取证获得, 这时就需要用到物理取证技术. 物理取证技术可分为软件取证模式和硬件取证模式.

(1) 软件取证模式

用软件的方法进行物理取证是 Android 手机物理取证的的首选[8], 简单快捷, 通过常用取证软件设备和命令即可获取 Android 手机的系统文件或者镜像. 软件物理取证目前有两种方法.

1) 使用专门修改的 loader 进行引导, 实现物理读取.

2) 通过软件对手机只能 dd 命令, 前提是获得 root 权限.

(2) 硬件取证模式

包括三种方式[9]: 拆解芯片、JTAG、微码读取. 拆解芯片可能会造成手机无法还原的后果, 风险较高. JTAG 是一个测试标准, 大部分电子设备均可使用 JTAG 方式进行测试或扫描, 同时 Android 手机一般具备 JTAG 端口, 可用于内存的读取与恢复. 微码读取是通过分析芯片上的物理电平门限值, 取证人员可以将 0 和 1 转换为 ASCII 字符, 目前微码读取仅作为一种取证方法存在, 运用到实际还有一定差距. 表 2 是对以上取证方法进行对比, 其中, Y 代表满足要求, N 代表不满足要求.

表 2 Android 手机取证方法对比

取证方式		提取简单	信息完整	数据损害
逻辑取证		Y	N	N
物理取证	软件取证	Y	Y	N
	硬件取证	N	Y	Y

逻辑取证技术应用广泛, 提取相对简单, 对原始数据的损害较小, 但提取信息的完整性较弱, 不能得到删除的数据. 物理取证中的软件取证提取较为简单, 对原始数据损害也较小, 能够恢复已经删除的数据, 而硬件取证技术操作难度较大, 损害数据的风险较高, 能得到完整的数据, 实践中难以应用.

2.2 iPhone 手机取证

iPhone 手机取证的前提是知道或能破解手机的密码, 随着苹果公司安全性的要求和用户自身安全意识的增强, 要想破解 iPhone 手机的密码是相当困难的, 因此取证人员在最初拿到 iPhone 手机时, 应立即通过手机所有人获取密码, 或者趁手机处于未锁定状态, 快速绕过密码修改设置.

iPhone 手机取证根据取证工具以及取证简易程度可划分为 5 类[10–13]: 人工提取、逻辑分析、十六进制转储、芯片拆解、微码读取, 图 3 是 5 类取证方法的分级, 从上到下, 方法和取证工具变得更加复杂和专业, 消耗时间更多, 成本更大, 更能获取取证手机的完整性数据.

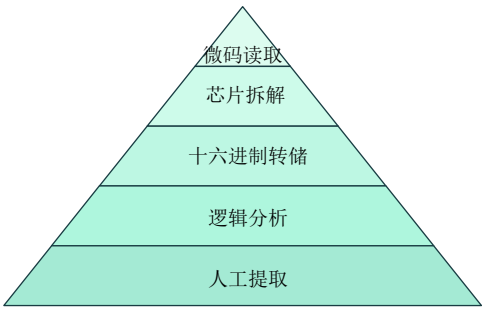

图 3 iPhone 取证方法分类

(1) 人工提取

人工提取是最简单的一种方法, 通过直接查看的方式提取信息, 不能获得已删除的记录, 但方便快捷, 对取证人员专业要求较低.

(2) 逻辑提取

该方法是将 iPhone 的文件系统备份出来, 通过这种方法, 能够恢复实际设备的已分配数据, 并随后对其进行分析[11]. 逻辑提取通常是取证人员的首选方法, 因为这种方法易于操作并能为后面的分析提供充足的数据来源, 操作步骤如下:

1) 打开并运行取证软件, 如 CelleBrite UFED、IXAM、Oxygen Forgensic Suite 2010 等.

2) 连接 iPhone 手机.

3) 开始数据备份, 使用 Apple 同步协议的设备备份中提取所有数据, 这种方法是从设备中直接提取数据.

4) 利用取证软件, 输出取证结果.

(3) 十六进制转储

十六进制转储一般是通过传输线将设备和取证工作站连接起来, 这种类型不再通过计算机启动命令, 而是将预先写好的代码植入到手机内存中, 执行代码命令手机将用户数据复制到计算机上. 这样用户的数据被复制、传输, 同时作为原始映像保存[12].

该取证方法是直接把物理存储介质作为目标, 而不依赖于文件系统访问数据. 这个方法最重要的一点是有可能恢复已删除的数据.

(4) 芯片拆解

芯片拆解是指从设备的 RAM 芯片中用物理手段获取数据, 然后利用芯片读取器提取存储的数据. 这种方法比前面几种方法都具有挑战性, 芯片拆解对取证人员专业技术更高, 取证时间更长, 因为取证过程中会存在大量原始的二进制数据格式的转换, 并且芯片损坏的风险较高, 在实践中不常使用[13].

(5) 微码读取

该方法需需要解释内存芯片上的临时数据. 通过分析芯片上的电平门限值[12], 将二进制数据翻译为 ASCII 字符. 该方法需要花费大量的时间和成本, 并对取证分析人员专业性程度高, 实践中应用较少.

表 3 是对以上 5 种取证方法进行对比, 其中, Y 代表满足要求, N 代表不满足要求.

以上几种取证方法各有利弊, 人工提取和逻辑提取操作简单, 易于获取, 但对取证信息的完整性较弱,

十六进制转储较前两种方法更复杂, 但提取的数据更完整, 更有意义; 芯片拆解和微码读取可能去目标设备有损害, 同时取证过程复杂, 但获取的信息也最为有效和完整.

表 3 iPhone 5 种取证方法对比

取证方法	提取简单	成本小	信息完整	数据损害
人工提取	Y	Y	N	N
逻辑提取	Y	Y	N	N
十六进制	Y	Y	Y	N
芯片拆解	N	N	Y	Y
微码读取	N	N	Y	Y

3 网络电子取证

电子取证对象除了计算机和智能手机之外, 还包括数据源最广的网络取证, 网络电子数据类型复杂, 并处于动态可变化状态. 该取证方法与前两类方法截然不同, 网络电子取证包括: 网站服务器取证、路由器取证、数据流信息取证等[4,14–20].

3.1 网络服务器取证

网站服务器取证流程[21–25]如下:

(1) 分析目标客户端的配置文件, 找到对应网站文件存储的目录和全部代码, 导出网站应用的所有代码文件.

(2) 分析网站服务器文件的配置, 找出网站服务器所使用的数据库类型、IP 地址以及访问数据库的登录名和密码, 导出数据库中所有数据.

(3) 使用提取的网站代码和数据库构建模拟网站服务器, 注意需要设置同样的主机名、数据库连接方式等.

(4) 使用同样的方法搭建模拟网站.

(5) 通过模拟网站登录, 模拟用户操作行为, 确定与之相关的网站程序和模块.

(6) 登录模拟服务器界面, 确定并分析服务器管理数据.

3.2 路由器取证

路由器作为连接网络节点的关键设备, 不仅会记录一般数据传输的路由信息, 同时也会记录一些关键的 IP 地址或 MAC 地址的访问信息, 因此在取证过程中, 路由器显得较为重要[26–28].

企业级路由器一般带有日志功能, 只需要提取日志即可, 一般家庭型路由器均不带有日志功能, 这就需要在路由器断电之前进行取证, 否则断电或重启路由器后, 一些重要的数据就会丢失, 达不到取证效果.

3.3 数据流信息取证

取证人员在经过相关法律机关授权后, 可利用网络嗅探的方式截获网络中传输的数据信息, 并通过对不同协议的解析, 从而达到取证的目的. 最常用的是 ARP 欺骗嗅探[29,30].

(1) 网卡设置为混杂模式, 使得在这种模式下工作的网卡能够接收到一切通过它的数据, 而不管实际的目的地址.

(2) 利用 ARP 欺骗目标主机, 目标主机认为欺骗主机是正确的交流方, 在传输与过程中交换机和计算机需要查询 ARP 表, 因此取证人员只需修改 ARP 表就行实现数据的获取, 把监控数据引导到自己的主机上.

(3) 分析数据.

4 电子数据取证技术的发展方向

随着科技的进步和发展, 传统取证技术和方法需要改进才能满足电子取证的要求, 下面就电子数据取证技术未来可能的发展趋势进行分析[31–37].

(1) 基于密码学的取证

对个人信息安全逐渐重视, 许多个人信息存储都使用较强的密码学技术, 例如: 同态加密、数字签名、比特承诺等方法, 这就需要取证人员具备密码学相关技术, 传统的取证工具需要具备最前沿的解密方法, 才能够获得电子数据内容, 为后面分析做准备.

(2) 基于区块链的取证

随着比特币的出现, 而区块链是比特币的技术基层, 由于区块链去中心化和匿名性的思想, 成为很多犯罪分子进行各类犯罪的工具, 然后针对区块链的取证目前来说还相当困难, 还没有有效的方法获取区块链中有用信息, 因此基于区块链的取证技术将是一个重要的研究方向.

(3) 基于云计算的取证

近年来, 云计算技术得到快速发展, 给社会带来便利的同事, 云安全技术却处于滞后状态, 出现了许多以云端为目标的违法犯罪, 传统的网络取证方法无法满足云计算取证的特点, 要比传统取证方法难度大很多, 这对电子取证技术来说是亟待解决的问题.

(4) 基于大数据的取证

随着信息社会数据凉的急剧增加, 互联网给人们

带来丰富信息的同时, 互联网海量数据给电子取证带来严峻的挑战, 因此传统的取证设备和分析方法不能满足大规模数据的要求, 需要建立大数据取证平台, 这将是电子数据取证发展的趋势.

5 结束语

详细分析了几类电子取证方法, 基于 Windows 电子取证、基于 Android 手机的电子取证、基于 iPhone 手机的电子取证、基于网络电子取证, 并对电子取证未来的发展方向进行展望.

参考文献

1 刘建军, 陈光宣. 电子取证技术体系研究. 网络安全技术与应用, 2013, (5): 8–10, 13. [doi: 10.3969/j.issn.1009-6833.2013.05.004]

2 刘尊. 网络电子取证技术研究[硕士学位论文]. 西安: 西北工业大学, 2005.

3 Jahankhani H, Watson DL, Me G, *et al*. Handbook of electronic security and digital forensics. Singapore: World Scientific Publishing Company, 2010.

4 刘浩阳, 李锦, 刘晓宇, 等. 电子数据取证. 北京: 清华大学出版社, 2015.

5 艾绍新. Windows 数据恢复技术在电子取证中的应用研究[硕士学位论文]. 大庆: 东北石油大学, 2013.

6 Kaplan RE. Computer forensics —what is it good for? Journal of Digital Forensic Practice, 2008, 2(2): 57–61. [doi: 10.1080/15567280801958464]

7 方冬蓉. 基于 Android 手机的数据恢复方法研究及应用[硕士学位论文]. 兰州: 兰州理工大学, 2014.

8 卿斯汉. Android 安全研究进展. 软件学报, 2016, 27(1): 45–71. [doi: 10.13328/j.cnki.jos.004914]

9 杜周. Android 应用取证分析研究[硕士学位论文]. 南京: 东南大学, 2016.

10 陈光宣, 丁丽萍, 杜锦. iOS 手机取证概述. 计算机科学, 2016, 43(12): 1–6. [doi: 10.11896/j.issn.1002-137X.2016.12.001]

11 贺滢睿, 陆道宏, 李建新, 等. 面向 iPhone 手机的电子数据取证分析. 第 28 次全国计算机安全学术交流会论文集. 贵阳, 中国. 2013. 87–90.

12 Hoog A, Strzempka K. iOS 取证实战: 调查、分析与移动安全. 彭莉娟, 刘琛梅, 赵剑, 译. 北京: 机械工业出版社, 2013.

13 秦玉海, 孙奕. 智能手机取证. 北京: 清华大学出版社, 2014.

14 Wang DG, Li T, Liu SJ, *et al*. Dynamical network forensics based on immune agent. Proceedings of the 3rd International Conference on Natural Computation. Haikou, China. 2007. 651–656.

15 林立友, 齐战胜, 黄超. 网络取证的发展现状及发展趋势. 保密科学技术, 2013, (1): 26–30.

16 黄晓芳, 徐蕾, 杨茜. 一种区块链的云计算电子取证模型. 北京邮电大学学报, 2017, 40(6): 120–124.

17 Birk D, Wegener C. Technical issues of forensic investigations in cloud computing environments. Proceedings of the 6th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. Oakland, CA, USA. 2011. 1–10.

18 Garfinkel SL. Digital forensics research: The next 10 years. Digital Investigation, 2010, 7(S1): S64–S73.

19 张昆. 云计算环境中电子取证技术研究与实现[硕士学位论文]. 成都: 电子科技大学, 2014.

20 Sekie AM, Yoo H, Shon T. Next generation electronic record management system based on digital forensics. International Journal of Security and Its Application, 2013, 7(1): 576–599.

21 Sylve J, Case A, Marziale L, *et al*. Acquisition and analysis of volatile memory from Android devices. Digital Investigation, 2012, 8(3-4): 175–184. [doi: 10.1016/j.diin.2011.10.003]

22 Case A, Marziale L, Neckar C, *et al*. Treasure and tragedy in kmem_cache mining for live forensics investigation. Digital Investigation, 2010, 7(S1): S41–S47.

23 Pereira MT. Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records. Digital Investigation, 2009, 5(3-4): 93–103. [doi: 10.1016/j.diin.2009.01.003]

24 Zawoad S, Hasan R. Trustworthy digital forensics in the cloud. Computer, 2016, 49(3): 78–81. [doi: 10.1109/MC.2016.89]

25 Kebande VR, Ray I. A generic digital forensic investigation framework for Internet of Things (IoT). Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud. Vienna, Austria. 2016. 356–362.

26 Spafford E. Some challenges in digital forensics. IFIP International Conference on Digital Forensics Advances in Digital Forensics II. Orlando, FL, USA. 2006. 3–9.

27 Luoma VM. Computer forensics and electronic discovery: The new management challenge. Computers & Security, 2006, 25(2): 91–96.

28 Yao W, Sha J, Yang T. Research on network multiple hard disk duplicator for electronic forensics. Computer Engineering, 2012, 38(5): 262–265.

29 Martini B, Choo KKR. An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 2012, 9(2): 71–80. [doi: 10.1016/j.diin.2012.07.001]

30 Beebe N. Digital forensic research: The good, the bad and the unaddressed. Proceedings of the 5th IFIP WG 11.9 International Conference on Digital Forensics Advances in Digital Forensics V. Orlando, FL, USA. 2009. 17–36.

31 Garfinkel S. Digital forensics XML and the DFXML toolset. Digital Investigation, 2012, 8(3-4): 161–174. [doi: 10.1016/j.diin.2011.11.002]

32 Shaw A, Browne A. A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. Digital Investigation, 2013, 10(2): 116–128. [doi: 10.1016/j.diin.2013.04.003]

33 McDonald JT, Kim YC, Yasinsac A. A yasinsac software issues in digital forensics. ACM Sigops Operating Systems Review, 2008, 42(3): 29–40. [doi: 10.1145/1368506]

34 Shin YD. New digital forensics investigation procedure model. Proceedings of 2008 4th International Conference on Networked Computing and Advanced Information Management. Gyeongju, South Korea. 2008. 528–531.

35 Vijayalakshmi VS, Shwetha B, Sathyanarayana SV. Image classifier based digital image forensic detection-a review and simulations. Proceedings of 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology. Mandya, India. 2015. 23–28.

36 Xu P, Cumanan K, Ding ZG, *et al*. Group secret key generation in wireless networks: Algorithms and rate optimization. IEEE Transactions on Information Forensics and Security, 2016, 11(8): 1831–1846. [doi: 10.1109/TIFS.2016.2553643]

37 Grajeda C, Breitinger F, Baggili I. Availability of datasets for digital forensics-and what is missing. Digital Investigation, 2017, 22(S1): S94–S105.