DOI:10.3969/j.issn.1009-6868.2016.01.008
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.TN.20151117.1459.002.html

计算机网络取证和调查的科学研究

Computer Network Forensics and Investigation

邹锦沛/KP CHOW[1]
陈航/CHEN Hang[2]
徐菲/XU Fei[3]

(1.香港大学 计算机科学系,香港 999077;
2. 南京理工大学 计算机学院,江苏 南京,210094;
3. 中国人民大学 法学院,北京 100872)
(1. Department of Computer Sciences, Hong Kong University, Hong Kong 99077, China;
2. Department of Computer Sciences, Nanjing University of Science and Technology, Nanjing 210094, China;
3. Law School, Renmin University of China, Beijing 100872, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2016) 01-0030-004

摘要: 认为针对计算机犯罪,现代的调查是对电子证据进行智能相关性分析,并发掘同一事件不同证据之间的联系;而证据分析又包括电子数据证据的分析、对收集的数据和备份进行查找、分析、归类,以及犯罪现场重建等。提出犯罪现场重建是计算机网络犯罪调查的重要部分。通过理论和实验分析,将取证科学应用到网络犯罪调查上,并以P2P网络调查作为例子,分析如何通过调查取证来寻找数据的第一个上传者。认为只有将恰当的法证科学适时应用到电子证据取证调查中,才能够更好地重构犯罪场景,还原案件真相并实现法律正义。

关键词: 电子证据;调查;法证科学;犯罪现场重构

Abstract: For computer related crimes, modern digital investigation emphasizes analysis of the relationship between different digital evidence with the goal of determining how different pieces of digital evidence appear in a single event. Digital evidence analysis includes searching, classification, analysis, and event reconstruction. Event reconstruction is the most important part of cybercrime investigation. By theoretical and experimental analysis, one can apply forensic science to cybercrime scene reconstruction. We demonstrate how to apply forensic science in cybercrime investigation involving the peer-to-peer network, with the objective of identifying the first uploader in the peer-to-peer network. By applying forensic science to cybercrime investigation, the digital investigator should be able to reconstruct the crime scene more efficiently.

Key words: digital evidence; investigation; forensic science; crime scene reconstruction

1 计算机法证的概况

1.1 电子证据与取证调查

人们常把由计算机制作的文件和计算机活动日志当作电子证据。根据香港特别行政区的《证据条例》第22A条[1],一项由计算机制作的文件的陈述,由在有关计算机的运作或有关活动的管理方面身居要职的人,依法签署的证明书依法证明后,则可在任何刑事法律程序中,接纳为该陈述内所述任何事实的表面证据。该证明书对由计算机制作的文件的制作方式予以描述,并在有关法律程序关系的范围内,说明该文件的性质及内容。

现代的计算机网络罪行更为复杂[2-4]。犯罪分子不仅窜改计算机记录,还用计算机来存储他们的数据,例如:非法金融交易和地址簿。此外,犯罪分子还利用互联网作为犯罪平台,例如分布式拒绝服务攻击、网络拍卖诈欺、分享受版权保护的作品等。现代计算机网络犯罪的主要特点是专业性强、有组织、并利用网络。

传统的计算机法证取证技术,已无法应对当今的计算机网络犯罪。现代的调查是对电子证据进行智能相关性分析,并发掘同一事件不同证据之间的联系。现代的分析证据是指对电子数据证据的分析,对收集的数据和备份进行查找、分析、归类等。

1.2 计算机法证的发展

计算机法证成立于20世纪70年代,其发展阶段可分为:婴儿期、儿童期和青春期。婴儿期为1985—1995年,儿童期为1995—2005年,青春期为2005—2010年[6-9]。计算机法证的研究重点是资料恢复,其中最主要是数据恢复、密码恢复和文件恢复[10]技术。数据恢复指恢复已被移走或删除的电子逻辑或物理数据,例如一个破碎的硬盘;密码恢复指处理受密码保护的原始数据,如密码加密的文件;文件恢复则尝试从硬盘内的数据块的片段恢复删除的文件。目前,文件恢复技术在计算机法证工作中,是一个主要的工作内容,例如手机的数

收稿日期:2015-11-08
网络出版日期:2015-11-17

D:\MAG\2016-02-126/VOL22\F3.VFT——4PPS/P1

据恢复[11]。

传统的法证主要集中在识别和重建。识别包括指纹、DNA 和毒品。指纹和 DNA 被用来识别特定的人，而毒品分析用于确定毒品的化学成分。识别的目的是用来判断样品是否来自一个特定的对象，诸如人或毒品。重建[12]则包括犯罪现场重建与弹道重建。犯罪现场重建指试图重建在犯罪现场所发生的事件，例如重现一宗谋杀案如何发生；而弹道的重建被用来重建从枪炮发射的子弹的轨迹。

计算机法证与传统法证相似，它们都试图解答一些问题，如：发生了什么事情？当事人是谁？什么时间、什么地点、如何发生的？这件事情发生的动机是什么？

2 计算机法证犯罪现场重建

在香港特别行政区及世界各地，藏有儿童色情物品是一种犯罪行为。香港地区某犯罪嫌疑人被指控藏有儿童色情物品，警方查获计算机一台。

2.1 犯罪现场重建过程

为了进行计算机法证分析，警方按标准的程序检查检获的计算机。这些标准程序基于确立的计算机采证程序，并产生法证克隆、计算哈希算法值、扫描计算机病毒等等。在标准的计算机采证过程后，计算机法证鉴定人将会分析检获的计算机硬盘驱动器，并收集电子证据。对于儿童色情物品的案件，电子证据便是儿童色情图片和动态影像。所以第一步是寻找在计算机内储存的儿童色情图片和动态影像，这些会包括：现存的儿童色情图片和动态影像、恢复删除的儿童色情图片和动态影像。图 1 显示了恢复删除的文件。

执法人员已为儿童色情图片和动态影像建立哈希值数据库，计算机法证鉴定人便不需要阅览个别的儿童色情图片和动态影像。相反，计算机法证鉴定人只需要把计算机里面的文件的哈希值与数据库比较。图 2 显示出根据该文件的创建时间和最后写入的时间的事件恢复过程。根据这两个时间戳，文件在 2005 年 2 月 22 日上午 12 时 37 分 09 秒被复制到当前位置。

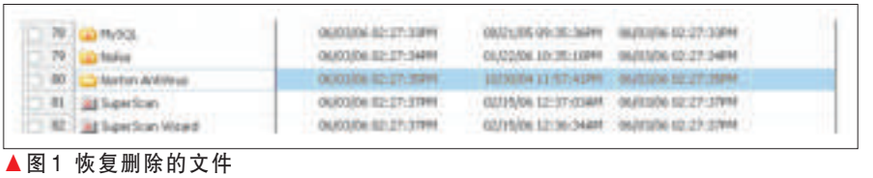
计算机法证鉴定人试图从文件中包含的关于文档的信息，例如创建者、修改的日期和其他细节，和其他计算机活动日志和电子证据，去重建产生该儿童色情图片和动态影像的经过。例如 2004 年 1 月 4 日，疑犯从互联网下载童色情图片和动态影像，并使用信用卡号码 0000-1111-2222-3333 在网上支付，然后在 2009 年 8 月 5 日备份到外部媒体。

图 3 显示了犯罪现场重建，犯罪嫌疑人在 2004 年 1 月 2 日使用他的信用卡购买在互联网上的儿童色情物品，然后在 2009 年 8 月 4 日做一个备份到外部硬盘上。

2.2 犯罪现场重建的法证科学

犯罪现场重建之所以重要，是因为在法庭上，计算机法证鉴定人需要给非技术人员（法官和陪审团）解释“技术细节”，让他们做出裁决。法律可能有特定的要求，例如控方需要证明犯罪嫌疑人知悉儿童色情图片和动态影像储存在计算机里。许多时候，犯罪嫌疑人的辩解是，儿童色情裸照是被木马下载的，他并不知道它们为什么在计算机里。辩方可以聘请专家质疑检察官的说法，或混淆法官和陪审团对“技术细节”的了解。计算机法证鉴定人的证言不仅受到辩方的质疑，还受到法庭的监察。

美国最高法院在 Daubert 一案裁定，主审法官必须确保接纳的科学证言或证据，不但全部切题并且全部可靠。所提出的科学证言须以恰当的



▲图 1 恢复删除的文件

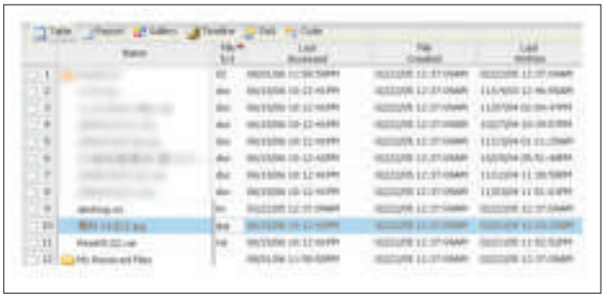


图 2▶ 事件重建

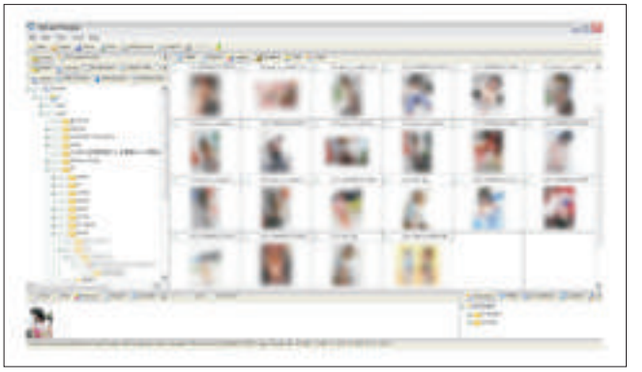


图 3▶ 犯罪现场重建

D:\MAG\2016-02-126/VOL22\F3.VFT——4PPS/P2

验证方法，获科学上已知的有力理据支持，具体包括：

（1）通过可靠性测试。

（2）通过同行评审。

（3）提供方法或理论的错误率，并在一定范围之内。

（4）符合标准和控制。

（5）得到普遍接受。

有关的法律也规定专家的科学证言须结合“科学知识”，并就证据的可靠性及可信性立下标准。证据的可靠程度取决于科学上能否验证。

现代的电子调查是对电子证据进行智能相关性分析并重建犯罪过程，例如通过计算机的所有者、电子签名、密码、交易纪录、邮件、发送服务器的日志、上网IP等计算机特有信息识别体，同其他证据互相印证、相互关联，然后进行综合分析。

同时，很多时候电子证据还需要传统的调查手法相辅助。调查人员在重建罪行时，需要适当考虑其他可能存在的解释，并在解释与证据之间进行相互印证。可能在某种假设情况下，需要查找更多的证据；又可能在新的证据下，得出新的假设和解释。调查人员要把证据互相印证，相互关联起来进行综合分析。调查人员要找出与理论假设与证据之间如何构成证实的关系，才能准确地重构犯罪过程。构建假设并验证就是可以采用的科学方法。

3 P2P网络中发布者取证调查

我们以Foxy软件为例，介绍在一个点对点分享（P2P）网络中，如何通过调查取证找到数据的上传者，以及何时调查能够找到数据的最先上传者。2008年香港艳照门事件中，嫌疑人就是利用Foxy对艳照进行共享，使得艺人的裸照在Foxy网络中迅速传播。想要抓捕嫌疑人，需要通过对Foxy进行分析，找到物理世界中的人。

Foxy是一个繁体中文P2P软件，发行者为一家已于2010年关闭的台湾公司。该软件只有正体中文版，没有英文等其他语言的版本，因此主要流行在台湾、香港及澳门等使用繁体中文的地区。它利用强制上传增加分享速度，但用户无法停止上传。它没有路由机制，源头的私隐（例如IP位址，所在地点）不受保障。它没有连接加密，连接容易被监视。它容易让使用者误设为全机分享，分享用户所有档案，每次下载完成后会自动重新分享用户的所有档案，并且用户无法停止。

当Foxy客户端试图连接到Foxy网络，会执行以下任务，如图4所示。

（1）用户连接到Foxy的服务器，以获得一个对等端列表。

（2）服务器回答一个对等的用户列表。

（3）用户发送一个PING请求到各个对端。

（4）各个对等端回答一个PING请求到用户。

（5）用户现在在Foxy网络上。

在Foxy网络中，每个共享文件都使用它的名字。当一个用户要寻找一个文件，他输入了一个搜索查询的文件名（或只是其中的一部分）。查询信息发送到所有对等端，然后传递给其他相邻对等端。当一个对等端拥有一个文件名和查询信息字符串相匹配，就回答一个QueryHit消息给发出请求的用户。QueryHit消息中包含的信息包括IP地址和端口号，共享文件和文件本身的信息。这使用户能够建立一个连接到该对等端，并启动下载。

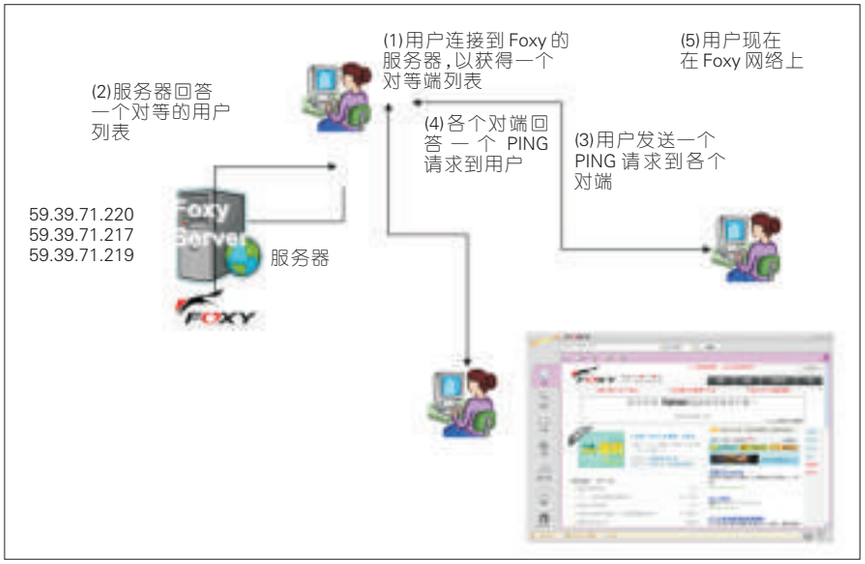
在接收QueryHit信息以及有关的连接信息，用户需要先选择一个文件，并发送一个TCP HTTP GET至承载该文件的等端，请求下载。承载该文件的等端然后回应，并开始发送所请求的数据。

与所有对等网络的文件共享，所有等端在Foxy网络中都是同等级的。所有拥有与“Query”请求匹配的副本的等端都回复它的IP地址给请求者。图5显示了在P2P网络中文件的分发种子数据增长曲线。当一个文件被广泛地分布后想要确认哪个等端是发起者多是不可能的。也许可以在下列情形中找到：

（1）在peer缓慢的增长期。

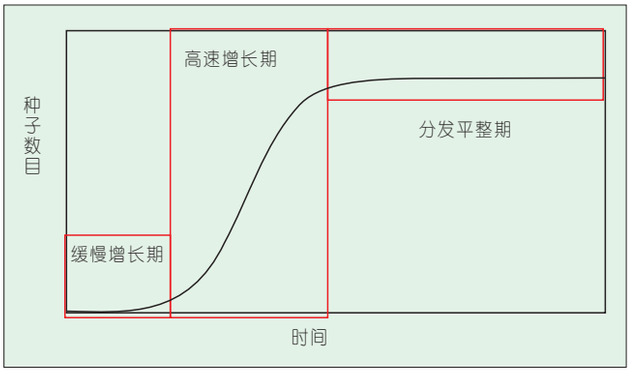
（2）分享文件非常大。

在缓慢增长期后找到谁是发起者也是不可能的。在连续监察下，我们认为如果识别到大量关于特定名字的查询，并且发现大量查询命中来自同一个IP地址，则很有可能该IP

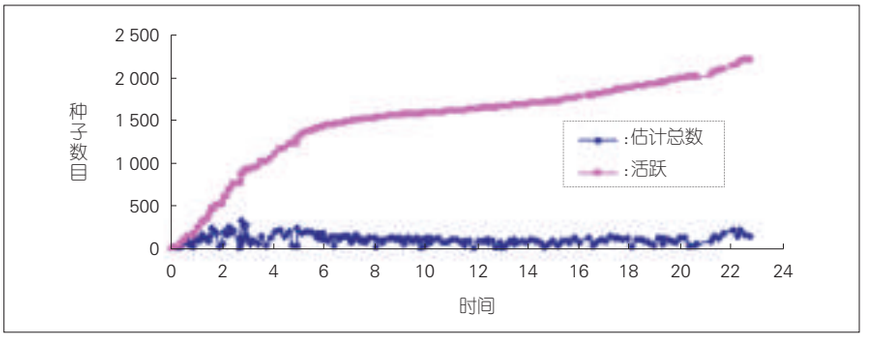


▲图4 Foxy客户端连接到Foxy网络

D:\MAG\2016-02-126/VOL22\F3.VFT——4PPS/P3



◀图5
在P2P网络中的文件分发



▲图6 实验确认缓慢上升期的存在

地址就是第1个上传者。我们进行了一系列相关的实验，实验结果验证了缓慢增长期的存在。实验结果如图6所示。

对于网络上数据的上传者，需要进行如下的科学分析：

（1）查清网络物品的来源。

（2）查清“虚拟嫌疑人”。通过上传人IP地址（包括静态IP、动态IP）、上网账号、密码及其相关登记资料、通过关联点分析网上活动轨迹及对资讯内容的分析，判断行为人的网络行为、个性特征，锁定虚拟嫌疑人。

（3）确认“现实嫌疑人”。这一般属于通常所说的落地调查，即通过询问嫌疑人，并通过现场搜查、勘验、检查及电子数据鉴定确定现实嫌疑人，其中硬盘、手机、日志、光盘的电子数据的固定和提取尤为重要。

4 结束语

现代计算机网络犯罪调查的重要部分是犯罪现场重建。在计算机网络取证中，电子证据在犯罪现场重建中往往能够起到关键作用。运用各种科学手段、方法和技术，分析电子证据中隐含的信息及线索，能够更好地重新构建或模拟一个犯罪现场。我们相信计算机网络犯罪调查既是一门技术，更是一门科学，只有将恰当的法证科学适时应用到电子证据取证调查中，才能够更好地重构犯罪场景，还原案件真相并实现法律正义。

参考文献

[1] KWAN M, OVERILL R E, CHOW K P, et al. Sensitivity Analysis of Digital Forensic Reasoning in Bayesian Network Models [C]// Proceeding of 7th Annual IFIP WG 11.9 International Conference on Digital Forensics, Orlano, Florida, USA, 2011
[2] 钟琳, 黎家盈, 邹锦沛, 等. 基于多视图分析的复杂网络犯罪现场重构[J]. 电信科学, 2010, (S2):165–170
[3] LAW F, LAI P, CHOW K P, et al. Memory Acquisition: A 2–Take Approach [C]//The 2009 International Workshop on Forensics for Future Generation Communication environments (F2GC–09), Jeju Island, Korea, Dec 10 – 12, 2009
[4] FRANK Y W, LAW, CHOW K P, et al. A Host–Based Approach to BotNet Investigation [C]// Proceeding of the 1st International Conference on Digital Forensics and Cyber Crime, Albany, NY, Sept 30–Oct 2, 2009
[5] HE Y, ZHANG P, HUI C K, et al. Cloud Forensics Investigation: Tracing Infringing Sharing of Copyrighted Files in Cloud [C]// Proceeding of 2012 ADFSL Conference on Digital Forensics, Security and Law (ADFSL’12), 30–31 May 2012
[6] XU F, CHOW K P, He J, et al. Privacy Reference Monitor–A Computer Model for Law Compliant Privacy Protection [C]//2009 IEEE International Conference on Parallel and Distributed Systems, Shenzhen, China, 2009
[7] PUN K H, HUI L C K, CHOW K P, et al. Review of the Electronic Transaction Ordiance, Can the Personal Identification Number Replace the Digital Signature [J]. Hong Kong Law Journal, 2002, 32(2):241–257
[8] IEONG S C R, CHOW K P. Enhanced Monitoring Rule Through Direct Node Query for Foxy Network Investigation[C]// The First International Conference on Digital Forensics and Investigation (ICDFI), Beijing, China, 2012
[9] YE Y, WU Q, LI Y, CHOW K P, et al. Unknown Chinese Word Extraction Based on Variety of Overlapping Strings [J]. Information Processing and Management, 2013, 49(2) : 497–512
[10] CASEY E. Digitla Evidence and Computer Crime: Forensic Science, Computers and the Internet [J].Jurimetrics, 2011, 11(3): 373
[11] 戴士剑. 电子证据调查指南[M]. 北京: 中国检察出版社, 2014
[12] LAI P K Y, CHOW K P, HUI L, et al. Modelling the Initial Stage of a File Sharing Process on a BitTorrent Network [J]. Peer–to–Peer Networking and Applications, 2014, 7(4): 311–319

作者简介

邹锦沛，香港大学副教授；主要研究领域为网络安全与电子取证；先后主持和参加项目20余项，获得多项科研成果奖；出版专著、已发表国际会议、期刊论文50余篇，其中被SCI/EI检索40余篇。

陈航，南京理工大学硕士；主要研究领域为内部威胁分析与电子取证技术；参加项目2项，获得了多项研究成果。

徐菲，中国人民大学博士后；主要研究领域为网络安全、隐私保护与电子取证；先后主持和参加项目10余项；已申请发明专利、软件著作权10余项，发表国际会议、期刊论文30余篇，其中被SCI/EI检索20余篇。

D:\MAG\2016-02-126/VOL22\F3.VFT——4PPS/P4