基于证据链的电子证据可信性分析

赵志岩[1,2,3] 石文昌[2,3]

(中国人民公安大学网络安全保卫学院 北京 100038)[1]

(数据工程与知识工程教育部重点实验室 北京 100872)[2] (中国人民大学信息学院 北京 100872)[3]

摘 要 随着信息技术的普及与应用,计算机已经成为了人类生活的必需品,同样也成为了犯罪活动中必不可少的工具。计算机留下的电子证据通常会成为案件侦破或审判的核心证据。但是,由于电子证据的易失性和易篡改性,导致其经常在法庭上遭到质疑,因此证明电子证据的可信性是当前取证领域面临的一大挑战。提出的基于证据链的电子证据可信性分析模型通过构建证据链获取关联电子证据,并通过判断证据间一致性的方法,进行推理获得电子证据的可信性。

关键词 证据链,电子证据,分析模型,可信性

中图法分类号 DF794,TP29 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.7.023

Trustworthiness Analysis of Digital Evidences Based on Chain of Evidences

ZHAO Zhi-yan[1,2,3] SHI Wen-chang[2,3]

(Institute of Network Security Defense, People's Public Security University of China, Beijing 100038, China)[1]

(Key Laboratory of Data Engineering and Knowledge Engineering of Ministry of Education, Beijing 100872, China)[2]

(School of Information, Renmin University of China, Beijing 100872, China)[3]

Abstract Computers are necessary in our lives along with the popularization of information technology, and they are also important tools in criminal activities. Digital evidences often play a major role in the judicial case or trial, but digital evidences have usually been questioned in the courts because they are easy to forge. To prove the trustworthiness of digital evidences is a big challenge of forensic research. In this paper, we put forward a framework to analyze trustworthiness of digital evidences based on chain of evidences by means of building chain to access associated evidences and judging the consistency among evidences to deduce the their trustworthiness.

Keywords Chain of evidences, Digital evidences, Framework, Trustworthiness

1 引言

计算机和网络已经成为人类生活中必不可少的工具,也成为了犯罪实施过程中必需的一种手段,如嫌疑人可以利用email和即时通信软件进行团伙联络、搜索受害者、寻找买家、实施诈骗,也可以利用文字处理软件伪造合同、策划案件实施、记录账目等。这些软件实施的犯罪过程必然会在存储媒介、计算机系统中留下大量的记录痕迹,而这些痕迹也就成为了证明犯罪事实的证据。电子证据目前已经作为一种特殊类型的证据,在侦破案件及案件审理中起了很大的作用。

电子证据与传统证据相比有其独特的特点:1)易失性[1],即电子证据是存储在介质中的电磁信息,很容易受到电磁干扰或复写而消失,尤其对于RAM类介质,断电后证据就会消失;2)易篡改性[2],电子证据很容易被篡改和伪造,而且篡改后很难从证据本身观察出来;3)难理解性,电子证据的本质是二进制代码,经过不同软件的层层解析才能让人理解,其非直观性导致电子证据表现出来的含义并不一定代表底层的真实数据[3]。

电子证据的易失性和难理解性等特点导致其可信性较低,在法庭上经常遭到嫌疑人的抵赖,同时也经常会被嫌疑人恶意篡改和伪造,用来迷惑侦查人员或作为伪证。传统证据如笔迹、物证等,都有比较成熟的技术手段去验证其可信性,而电子证据伪造后特征并不明确,很难从证据本身去验证其可信性,因此如何使用技术手段证明电子证据的可信性是当前取证领域面临的一大挑战[4]。

事实上,电子证据作为科技的衍生物,它的产生和结果具有一定的科学规律,根据一定的推理规则,可以推导其可信性。

2 相关工作

电子证据从产生、收集、固定、分析、解释到呈堂,每一个步骤都可能引入导致其不可信的因素。文献[5]提出了电子证据领域的有效性问题,主要探讨取证过程中存在的问题,如获取证据工具的错误率、分析工具可能的错误率、推导结论过

到稿日期:2016-02-04 返修日期:2016-04-25 本文受国家自然科学基金项目(61472429),北京市自然科学基金项目(4122041)资助。

赵志岩(1980—),女,博士生,讲师,主要研究方向为网络犯罪侦查与取证,E-mail:zhaozy227@163.com;石文昌(1964—),男,博士,教授,主要研究方向为信息安全,E-mail:wenchangshi@139.com。

程可能存在的错误率等。

国内外对电子证据的可信性研究提出了很多方法，分别从不同的角度进行验证和分析，可以总结为以下几种。

(1)根据证据文件自身的属性特点进行分析，这类方法适用于特殊格式的文件，如图片、视频等，当图片进行拉伸、合成、柔化等操作后，可以根据图片的像素或色彩值等模式的变化来确定。

(2)证明电子证据从调查者获取电子证据的时间点开始，到分析鉴定过程结束，证据的二进制内容未被修改，并在法庭出示时能够证明其获取、保存、分析过程中始终保持完整和不变[6,7]。这种可信性一般采用加密算法对电子证据进行 MD5 或哈希计算，得到电子证据的特征值，然后通过特征值的比较来验证内容的完整性。

(3)使用审计方法，通过存储大量调查者在实际案例调查中使用的经验和方法，以此为基础评估当前调查过程的可信度，并对调查者得出的结论进行可信验证[8]。这种方法适用于提高调查者对电子证据形成的主观结论的可信性，确保其工作的质量，毕竟仅依赖某个调查者单独的经验和技术对所有电子证据进行正确的解释，是容易受到怀疑的[9]。

(4)验证取证工具的可信性，电子证据本质上是一些二进制代码，只有通过工具软件的解析才能被人理解。然而，任何工具软件都避免不了设计上的缺陷或代码中的漏洞，因此，电子证据的解析过程极大地依赖工具软件编写的可靠性，需要考虑取证工具对于取证结果的影响，取证工具的有效性能够间接确保电子证据的可信性。

本文通过将刑事案件中的证据链概念引入到电子证据领域，通过一定的规律构建电子证据链的证据链，然后推理判断证据链中所包含的电子证据之间的关联性和一致性，根据制定的规则判断电子证据的可信性，即电子证据没有被恶意篡改和伪造。本文第 3 节具体阐述基于证据链的电子证据分析推理模型，其中包含对证据链推理中涉及的形式化表述；第 4 节用具体案例说明推理模型适用的场景，并说明方法的有效性；最后对模型的细节实现提出思路。

3 电子证据可信性模型的构造

计算机和网络的普及，改变了传统的犯罪模式，很多网络犯罪类型中，仅依靠计算机网络就可以实现整个犯罪过程，这样的案件所涉及的关键证据均为电子证据，如制作并传播病毒案件，从制作病毒、贩卖病毒到转账获利等行为均可以用计算机实现，因此在主机系统中会留下完整的证据链。即便是以计算机为工具，只参与一部分犯罪过程的案件，由于软件的运行规律，也会表现出电子证据的完整行为过程，用以证明电子证据的可信性。

基于证据链的电子证据可信性推理模型的设计目标是构建电子证据链，然后根据证据链中相关电子证据之间的一致性推导其可信性。模型共包含 3 层，分别为证据表示层、证据链构建层和一致性推理层。模型在设计的过程中，需要对证据链及电子证据之间的关联关系等进行形式化定义，然后以形式化的方法描述模型，最后在模型形式化的基础上进行自动化推理，得出电子证据的可信性。

3.1 证据表示层

证据表示层是对调查过程中涉及的主机系统进行数据获取，主要功能是复制、解析和表示主机中的电子数据。复制就是位对位的二进制代码拷贝，然后对得到的二进制证据进行初步分析，将无意义的底层数据转换成独立的可识别的文件，最后以统一的特征结构表示不同类型的电子证据。

不同类型的文件格式通常是不同的，无法按照一定的标准进行关联和分组，所以无法对这些证据进行比较和推理分析，为了方便这些证据文件之间的统一处理，需要用形式化的方法表示它们。电子证据可以使用多种形式化表示方法，如采用结点结构用于案件重构[10]、采用论断形式进行推理[11]、采用集合形式体现调查过程等[12]。但现有的这些形式化方法并不适用于获取关联证据和一致性判断，因此采用了一种新的集合结构，从文件和系统中提取尽可能多的属性来表示证据，该结构如下所示：

$E_i\{T,A,Y,D,K\}$

其中，T 为时间属性，$T_i(tc,tm,ta)$，tc 是创建时间，tm 是修改时间，ta 是最后访问时间，A 为文件作者属性，Y 为文件类型，D 是存储目录，K 是文件中的关键词集合。

3.2 证据链构建层

证据学和法学认为，证据对于案件事实是否有证明力、是否具有可信性，取决于证据与案件事实是否有联系。为了提高证据的可信性和证明力，法庭审理的实践中主要通过构建证据链的方式说明。即单独的证据不能证明案件事实，只有当多个不同来源的关联证据共同指向同一个犯罪事实时，才能说明证据及其结论的可信性。

定义 1 电子证据链是指由两个或两个以上不同的电子证据所组成的、通过一定的关联关系连接起来、内容相互印证并体现或提高证明力的、用以证明案件事实性的证据集合[13]。

关联性是证据被法庭采纳的前提条件，其含义是证据所反映的事实与案件事实具有合理的联系。电子证据之间的关联关系有很多，不可能完全列举，如果花费太多的精力去挖掘所有的关联关系，不仅浪费时间，而且还会由于挖掘不重要的关联数据而导致忽略重点，因此本文采用两种关联关系，即案件关联关系和操作关联关系去证明可信性。

定义 2 设 C 为网络犯罪案件类型，$E(C)$ 为主机系统中包含的 C 类型案件产生的电子证据集合，$C_i(i=1,\cdots,x)$ 表示案件中连续的实施步骤，$E(C_i)$ 为每个步骤中产生的电子证据集合，若 $e_m\in E(C_i)\wedge e_n\in E(C_j)$，其中 $i\neq j$，则称电子证据 e_m 和 e_n 具有案件关联关系。

由案件关联关系组成的电子证据称之为案件链，数字空间的犯罪案件由于其特殊的环境，导致其具有相对独立的实施特性，尤其对于相同类型的网络犯罪行为来说，实施步骤的规律性更强[14]，使得产生的痕迹同样具有规律性，按照同类案件的实现步骤可以推出电子证据的案件链。例如，网络诈骗案件会遵循这样的规律：首先，通过电子邮件或即时通讯软件群发，引诱受害者上当，然后通过受害者点击链接或点击可执行程序植入木马，劫持受害者机器，最后获取账号信息或者引诱受害者转账。这些实施步骤中产生的电子证据之间就具有案件关联关系。

定义 3 设 S 为主机系统中的软件，$O(S)$ 表示软件 S 的操作，$E_i(O(S))(i=1,\cdots,x)$ 是软件 S 的 O 操作留下的电子证据集合，其中 i 代表由于操作产生的证据顺序，若 $\exists\{e_m,e_n\}\subseteq$

$E(O(S))$，则称电子证据 e_m 和 e_n 具有操作关联关系。

操作关联关系形成的电子证据链称为操作链，案件的每个实施步骤中至少要选择使用一种软件操作达到目的，也有可能选择多种软件操作，不同步骤还可能采用相同的软件操作实现。电子证据的操作关联关系依据系统和软件的运行规律进行构建，这些关联证据是系统自动生成的，用户很难更改。如执行用户的打开文件操作，根据系统运行规律，会产生临时文件、历史记录文件、快捷方式文件以及改变注册表的最近打开文档键等痕迹，表示这些痕迹的电子证据之间就具有操作关联关系。

如果这些相互关联的证据之间是一致的，则可以形成有效的证据链，而且这些证据之间可以互相证明并依据一定规则推断其相应的可信性。如何判断相关证据的一致性是比较困难的任务，本文定义了两种一致性（存在一致性和时间一致性来判断相关证据，如定义 4 和定义 5 所示。

定义 4（存在一致性） 具有案件关联关系或操作关联关系的电子证据 e_m，e_n，如果 e_n 产生的前提是 e_m 存在，记做 $e_m \rightarrow e_n$，则称 e_m 和 e_n 具有存在一致性。

e_m 和 e_n 的关联关系分为“与关系”（用 AND 表示）和“或关系”（用 OR 表示），如果 e_n 产生的前提是 e_{m1} 和 e_{m2} 同时存在，则为与关系；如果 e_n 产生的前提是 e_{m1} 和 e_{m2} 中任意一个存在，则为或关系。用图 1 来表示电子证据之间的与关系和或关系。

(a) AND 结构　　(b) OR 结构

图 1　关联电子证据之间的两种基本结构

定义 5（时间一致性） 实际获取到的案件关联证据 e_m，e_n，其中 $e_m \in E(C_i)$，$e_n \in E(C_j)$，若 $i<j$ 且 $e_m[T] < e_n[T]$，则 e_m，e_n 具有时间一致性。同理，若 $e_m \in E_i(O(S))$ 且 $e_n \in E_j(O(S))$，$i<j$ 且 $e_m[T] < e_n[T]$，则 e_m，e_n 也具有时间一致性。

根据电子证据的案件关联关系和操作关联关系所组成的案件链和操作链是相对独立的，其中案件链的主体是用户，存在的形式通常是程序文件或用户的数据文件。操作链的主体是系统或软件，存在的形式通常是临时文件、注册表、日志等文件。下面对电子证据的这两条证据链进行形式化。

定义 6　电子证据案件链 ECL 是一个有向图，可以表示为三元组 $ECL=\{N,L,R\}$。

(1) N 是电子证据链中的顶点集合，$N=\{e,C_i\}$，E 表示电子证据，C_i 表示案件的实施步骤。

(2) L 表示有向边的集合，由顶点的有序对唯一确定，如 $l=\{n_i,n_j\}$，其中 $n_i=\{e_m,C_i\}$，$n_j=\{e_n,C_j\}$，其中，$i=j-1$ 且 $e_m \rightarrow e_n$，表示结点 n_i 和结点 n_j 被有向边 l 连接，对于 $\forall n_i \in N$，定义 $IN(n_i)=\{l \mid l=(n_k,n_i), l\in L, n_k \in N\}$ 为指向顶点 n_i 的边集，定义 $OUT(n_i)=\{l \mid l=(n_i,n_k), l\in L, n_k \in N\}$ 为顶点 n_i 指向的边集。

(3) R 为逻辑表达式的集合，用来记录证据关联关系中的与或关系。R 与顶点集合中的元素一一对应，若 $IN(n_i)=\{l_1,l_2,l_3 \mid l_1=(n_1,n_i), l_2=(n_2,n_i), l_3=(n_3,n_i)\}$ 且 $R(n_i)=\{(l_1 \wedge l_2) \vee l_3\}$，则 n_1，n_2 表示的电子证据与 n_i 表示的电子证据是 AND 关系，而 n_3 与 n_i 则是 OR 关系。

由于软件运行过程是依据特定规律的固定过程，因此由软件操作导致的痕迹也具有相关的规律，不论是时间的先后顺序还是留下的电子证据种类与数量，都能够事先确定下来，而且这些证据之间都是并列关系。但由于软件产生的痕迹经常表现为临时文件，操作结束或较长时间后，临时文件也许会被删除覆盖，因此并不一定能够找到所有痕迹。

定义 7　电子证据操作链 EOL 是一个有向图，可以表示为二元组 $EOL=\{N,L\}$。

(1) N 是电子证据链中的顶点集合，$N=\{e,S\}$，e 表示电子证据，S 为产生、运行、编辑 e 的软件。

(2) L 表示有向边的集合，由顶点的有序对唯一确定，如 $l=\{n_i,n_j\}$，其中 $n_i=\{e_m,S\}$，$n_j=\{e_n,S\}$，且 $e_m \rightarrow e_n$，表示结点 n_i 和结点 n_j 被有向边 l 连接。

目前，在网络犯罪的侦查取证实践中，获取案件关联的电子证据主要靠人工完成[15]，即基于调查者的经验，根据案件类型进行总结，然后使用常用的取证工具进行浏览和自定义搜索。本文利用领域专家的经验，形成不同案件类型的电子证据案件链，以此来体现电子证据的案件关联关系。

案件链的构成是一个逐渐细化的过程，首先将案件大致分为“起因”、“开始”、“经过”、“结果”4 个阶段，不同的案件类型各阶段会有一些细微的变化。如制造并传播木马病毒案件类型，“起因”阶段指的是犯罪活动的准备步骤，“开始”指的是实施预备，“经过”指的是实施步骤，“结果”是犯罪活动的结束步骤。大致的关联关系如图 2 所示。

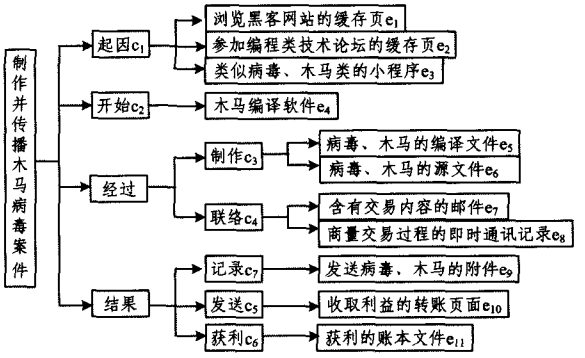

图 2　案件关联的电子证据

把图 2 中的电子证据按照与或关系连接起来，就形成了制造并传播木马病毒案件的案件链，如图 3 所示。

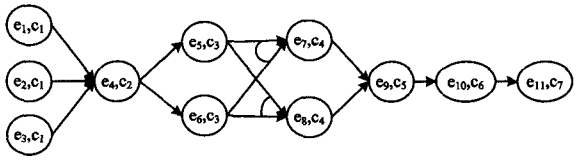

图 3　电子证据的案件链

图 3 形成的电子证据案件链仅仅是制作并传播木马病毒案件的初始模型，真正案件中涉及到的关联证据更多、更详细，因此该模型还需要进一步细化，包括犯罪步骤的细化以及每一步骤中涉及到的电子证据的细化。

电子证据操作链的构建，需要分析与电子证据操作相关的软件，包括与电子证据来源相关的软件、编辑过程相关的软件等。在实际的案件审判中，只有当嫌疑人对关键电子证据抵赖或提出质疑时，才需要根据电子证据的操作软件构建操作链，获取与电子证据操作相关联的痕迹，用来增强电子证据的可信性。

只要电子证据的类型确定，依据系统和软件的运行的规

律，这些相关操作所留下的痕迹就是固定的。可以采用监测软件运行的方式获得这些痕迹。目前，只针对案件中经常被质疑的电子证据，即用户的数据文件，如 office 文档、图片、音频、视频、邮件、聊天记录这几类证据进行可信性的分析，因此只需要对这些类型文件的操作进行监控即可。

以制作并传播木马病毒案件为例，案件链中的 e_{11} 为 office 文档，为了构建 e_{11} 的操作链，需要监控的软件操作有：下载工具从网络下载 office 文件的操作、office 软件从 USB 设备复制文件的操作，以及创建、打开、复制、移动、粘贴、删除、保存、关闭等操作；压缩软件对 office 文件的压缩、解压缩操作。

若 office 软件记做 s_1，$s_1 \in S$，监控 s_1 在执行创建、编辑等操作时得到的关联证据有：系统历史记录文件夹中的快捷方式文件 e_a，office 目录中的历史记录文件 e_b，在 temp 文件夹中留下的临时文件 e_c，在注册表中留下的最近访问记录键 e_d 等。这些都是监测得到的结果，把这些关联证据按照顺序连接起来就形成了电子证据的操作链，如图 4 所示。

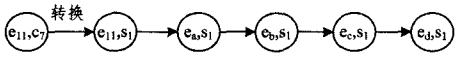

图 4　office 文档的 s_1 操作链

其中，(e_{11},c_7) 和 (e_{11},s_1) 是同一个电子证据在案件链和操作链中的不同表示。

同样，对于每一个操作 e_{11} 的软件，都分别有一条操作链，在案件的搜索过程中，如果能获取到这些痕迹信息，则可以极大程度地证明相关证据的可信性，并进一步证明目标证据的某些操作过程。

需要说明的是，案件链构建和操作链构建都是可扩展的，目前为了模型的实现，限定了一定范围的案件类型和证据文件。依据相同的设计思想和方法，模块可以进行扩展，增加更多的案件关联关系和操作关联关系，使模型能更灵活地适应信息技术的迅速发展。

3.3　一致性推理层

推理层主要是对关联电子证据进行存在一致性和时间一致性的判定，进而得到电子证据的可信性。一致性推理层完成两个功能，即关联证据搜集和一致性判断。

一致性推理层功能的实现依赖于证据链构建层的结果，即自动推理某电子证据的可信性，要求模型在构建层中存在该电子证据所属类型的网络犯罪案件的案件链，同时存在该类电子证据相关的操作链。只有在案件链和操作链都已知的前提下，才能按条件搜索相关电子证据并依据规则进行自动推理，因此模型实现的基础是对网络犯罪案件的总结和相关电子证据链的构建。

推理层实施的基本步骤可描述如下：

(1)将案件侦查中得到的目标电子证据形式化表示为 E：$\{T,A,Y,D,K\}$，根据属性匹配，映射到案件链中。

(2)根据证据链中的有向边分别向前和向后获取关联证据，以关联证据的属性为过滤条件，搜索主机系统，查找符合条件的关联电子证据，直到证据链顶点的 $IN(N)=0$ 或 $OUT(N)=0$，将搜索到的电子证据的形式化表示也分别映射到证据案件链中。

(3)对于有争议的目标电子证据，将其设为操作链的起点，匹配操作链中电子证据的属性集合，找出与目标证据操作关联的电子证据。

(4)根据证据的属性进行判断，案件链及操作链中的关联证据是否具有存在一致性和时间一致性。

4　实证分析

为说明提出方法的适用性，采用一个真实的制作并传播木马病毒的案件做验证，为保护嫌疑人的隐私，把电子证据中有关嫌疑人姓名和病毒名称的具体信息隐去，该案件最后依据模型提出的证据链信息顺利进行侦破和结案，这充分验证了模型的有效性。

4.1　案例背景

制作并传播木马病毒案件中，查获某嫌疑人电脑中有关病毒买家的基本情况的. doc 文档，文档中包含买家姓名、账号、购买金额等信息。但嫌疑人否认此文档的真实性，声称自己从未见过此文件。因此，调查者决定采用证据链的可信性模型进行测试，验证该 word 文档的可信性。

4.2　案例分析

首先，证据表示层处理嫌疑人的电脑，获取硬盘镜像、解析镜像的二进制代码，形成互相独立的文件，这部分功能对于取证工具来说比较普通，因此这里不再详细说明实现过程。

然后，将嫌疑人机器中的所有关键文件用特殊统一的集合形式表示，即使用属性集合的方式表示电子证据，包括所有用户数据文件，如 office 文档、邮件、图片、聊天文件、网页等；重要的系统文件，如注册表文件、日志文件等。这些属性应该包括文件类型、时间、作者信息、内容关键词等。

以. doc 文档为目标证据，依据证据链的主链和支链，以属性过滤的方式寻找相关的电子证据，包括案件关联关系和操作关联关系。关联证据及其对应的证据链如表 1 所列。

表 1　目标证据的关联电子证据

关联证据	对应链	映射顶点
黑客软件使用说明书	案件链	(e_1,c_1)
通用病毒木马源代码	案件链	(e_3,c_1)
Delphi7	案件链	(e_4,c_2)
*** 病毒可执行程序代码	案件链	(e_5,c_3)
功能不断完善的 *** 病毒源代码系列	案件链	(e_6,c_3)
询问价格、病毒功能等内容的 QQ 聊天记录文件	案件链	(e_8,c_4)
记录买家基本情况的 word 文档(目标证据)	案件链	(e_{11},c_7) (e_{11},s_1)
系统历史文件夹中 filename. doc(快捷方式文件)	操作链	(e_a,s_1)
office 历史文件夹中 filename. doc(快捷方式文件)	操作链	(e_b,s_1)
~WRL ****. tmp	操作链	(e_c,s_1)
~ $ filename. doc	操作链	(e_c,s_1)
注册表文件 MRU 键	操作链	(e_d,s_1)

通过推理层的一致性判断，虽然案件链中缺失部分证据，但其他关联证据具有存在一致性，时间属性也符合一致性的需求。所以，word 文档是可信的，可以证明嫌疑人的犯罪事实。

4.3　案例讨论

目前，对于 word 文档的源头和内容的可信性分析还没有有效的解决方法，虽然可以通过其他物理证据来推导文档的可信性，但是这种方法必须依赖人工，非常耗时，而且仅凭一个调查者的个人经验进行分析也不容易证明其有效性。

对于此类案件的鉴定方法主要是使用现有的取证分析工具，如 Encase、FTK 等，通过人工列举关键词或其他过滤条件对证据存储介质进行处理，这样过滤出来的关联证据无法判断它们之间的一致性，因此分析过程及其产生的结论极大地依赖调查者的主观经验。

本文提出的模型提供了分析电子证据可信性的思路，即通过构建电子证据链的方式获取相关证据，判断其一致性，并分析目标证据的可信度，这将成为将来具体产品实现的理论基础。

结束语 本文提出了基于证据链分析主机系统电子证据可信性的模型，依据证据链的理论和现实应用方法以及电子证据的关联性和一致性，通过案例证明该方法是有效的。

目前，判断电子证据可信性主要依赖调查者的人工分析，缺乏有效的技术手段解决自动化问题。本文提出的方法提供了解决这一问题的思路，但模型仍处于初级阶段，还有一些细节问题需要完善，如处理证据链中的缺失证据、给证据链中不同阶段的电子证据赋权值等。

未来的工作将关注模型的具体实现，通过对相关案例的总结和梳理，结合领域专家经验，构建和完善不同类型的涉网案件的证据链，同时，需要确认其他可能的证据关联关系以提高模型的准确度。

参 考 文 献

[1] Wang Fang. The nature of digital evidence and the related rules [J]. Law Science, 2004, 273(8): 72-79(in Chinese)
王芳. 数字证据的性质及相关规则[J]. 法学, 2004, 273(8): 72-79

[2] Caloyannides M A. Forensics Is So "Yesterday"[J]. Security & Privacy IEEE, 2009, 7(2): 18-25

[3] Anobah M, University S, Saleem S, et al. Testing Framework for Mobile Device Forensics Tools[J]. Journal of Digital Forensics Security & Law, 2014, 9(2): 221-234

[4] Casey E, Casey E. Error, Uncertainty and Loss in Digital Evidence[J]. International Journal of Digital Evidence, 2002, 1(2): 1-45

[5] Erbacher R F. Validation for Digital Forensics [C]// 2010 Seventh International Conference on Information Technology: New Generations (ITNG). IEEE, 2010: 756-761

[6] Jansen A. Digital Records Forensics: Ensuring Authenticity and Trustworthiness of Evidence Over Time [C] // International Workshop on Systematic Approaches to Digital Forensic Engineering. 2010: 84-88

[7] Adams R, Hobbs V, Mann G. The Advanced Data Acquisition Model (ADAM): A Process Model For Digital Forensic Practice [J]. Journal of Digital Forensics Security & Law, 2014, 8(4): 25-48

[8] Horsman G, Laing C, Vickers P. A Case Based Reasoning Framework for Improving the Trustworthiness of Digital Forensic Investigations [C] // 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2012: 682-689

[9] Tanne A L, Dampie D A. An Approach for Managing Knowledge in Digital Forensic Examinations[J]. International Journal of Computer Science & Security, 2010, 4(5): 451-465

[10] Kwan M, Chow K P, Law F, et al. Reasoning about e vidence using Bayesian network[J]. Advances in Digital Forensics IV Ch, 2008, 12(3): 263-278

[11] Cohen F. A method for forensic analysis of control [J]. Computers & Security, 2010, 29(8): 891-902

[12] Levine B N, Liberatore M. DEX: Digital evidence provenance supporting reproducibility and comparison[J]. Digital Investigation the International Journal of Digital Forensics & Incident Response, 2009, 6: 48-56

[13] Tian Z H, Yu X Z, Zhang H L, et al. A Real-Time Network Intrusion Forensics Method Based on Evidence Reasoning Network[J]. Chinese Journal of Computers, 2014, 37(5): 1184-1194 (in Chinese)
田志宏, 余翔湛, 张宏莉, 等. 基于证据推理网络的实时网络入侵取证方法[J]. 计算机学报, 2014, 37(5): 1184-1194

[14] Casey E. Digital Evidence and Computer Crime-Forensic Science, Computers and the Internet(3rd Edition)[M]. Elsevier, 2011

[15] Case A, Cristina A, Marziale L, et al. FACE: Automated digital evidence discovery and correlation [J]. Digital Investigation, 2008, 5(Suppl 1): 65-75

(上接第 114 页)

[3] Chang Y C, Lin Z S, Chen J L. Cluster based self organization management protocols for wireless sensor networks[J]. IEEE Transactions on Consumer Electronics, 2006, 52(1): 75-80

[4] Kolhe J P, Shaheed M, Chandar T S, et al. Robust control of robot manipulators based on uncertainty and disturbance estimation[J]. International Journal of Robust and Nonlinear Control, 2013, 23(1): 104-122

[5] Liu Yun-tong. K-pruning algorithm for semantic relevancy calculating model of natural language[J]. Journal of Theoretical and Applied Information Technology, 2013, 48(3), 231-235

[6] Lu Xing-hua, Chen Ping-hua. Traffic Prediction Algorithm in Buffer Based on Recurrence Quantification Union Entropy Feature Reconstruction[J]. Computer Science, 2015, 42(4): 68-71 (in Chinese)
陆兴华, 陈平华. 基于定量递归联合熵特征重构的缓冲区流量预测算法[J]. 计算机科学, 2015, 42(4): 68-71

[7] Zhai Hai-bin, Zhang Hong, Liu Xin-ran, et al. A P2P Cache Capacity Design Method to Minimize the Total Traffic Cost of Access ISPs[J]. Acta Electronica Sinica, 2015, 43(5): 879-887 (in Chinese)
翟海滨, 张鸿, 刘欣然, 等. 最小化出口流量花费的接入级 P2P 缓存容量设计方法[J]. 电子学报, 2015, 43(5): 879-887

[8] Ma You-zhong, Meng Xiao-feng. Research on index technology of cloud data management[J]. Journal of Software, 2015, 26(1): 145-166(in Chinese)
马友忠, 孟小峰. 云数据管理索引技术研究[J]. 软件学报, 2015, 26(1): 145-166

[9] Sahu P K, Wu E H K, Sahoo J, et al. BAHG: Back-Bone-Assisted Hop Greedy Routing for VANET's City Environments[J]. IEEE Transactions on Intelligent Transportation Systems, 2013, 14(1): 199-213

[10] Barrachina J, Garrido P, Fogue M, et al. VEACON: A Vehicular Accident Ontology Designed to Improve Safety on the Roads [J]. Journal of Network and Computer Applications, 2012, 35 (6): 1891-1900

[11] Shi Gui-min, Lin Hong-ji. Research on Network Flow Monitoring Pattern Based on Bypass[J]. Journal of Chongqing University of Technology (Natural Science), 2011, 25 (9): 63-69 (in Chinese)
石贵民, 林宏基. 基于旁路的网络流量监控模式[J]. 重庆理工大学学报(自然科学), 2011, 25(9): 63-69