抽象数字事件重构模型的设计

杨莉莉　杨永川

（中国人民公安大学研究生部　北京 100038）

摘　要　在总结了国外关于事件重构理论的基础上，提出了一种抽象的数字事件重构模型。模型由证据检查、角色分类、事件重构、事件排序以及结论生成5部分组成。本文重点讨论事件重构阶段。模型的提出为数字取证工作人员提供了事件重构的理论指导。

关键词　数字事件，事件重构，数字对象

Design of Abstract Digital Event Reconstruction Model

YANG Li-li　YANG Yong-chuan

(Chinese People's Public Security University, Beijing 100038, China)

Abstract　An abstract digital event reconstruction model is brought up based on foreign theory about event reconstruction. The digital event reconstruction model consists of five elements which are evidence examination, role classification, event reconstruction, event sequencing and conclusion giving. In this paper, event reconstruction is emphasized. The model provides theory guidance for digital forensic investigators and is helpful for their practice work.

Keywords　Digital event, Event reconstruction, Digital object

随着计算机技术的发展，计算机事件频频发生，与计算机等数字产品相关的各种纠纷、行为过失，以及计算机犯罪案件正逐年增加。数字事件是指包括计算机事件在内的、与数字产品相关的纠纷、行为过失，以及犯罪。为了有效地防止数字事件的发生，人们通常将此类事件诉诸于法律。数字事件的调查通常包括电子证据的收集、保存、分析等步骤，但对电子证据分析完毕后，并非大功告成，仅将数字事件中涉及到的电子证据提交给法庭是不够的，如何判断该事件是否发生，以及事件发生的起因、经过、结果等情况是解决问题的根本。因此，数字事件的重构对于法庭裁决至关重要。

1　几种事件重构模型的提出

数字事件重构是伴随着数字产品的产生而出现的。而物理事件重构从人类社会出现物理事件，并对物理事件探寻其根源开始，一直延续至今，许多学者对物理事件的重构进行了细致的探讨。

Miller和Lee等人描述了物理犯罪现场的事件重构模型[1,2]，该重构模型共分为5个阶段：(1)从犯罪现场收集证据；(2)对犯罪现场发生的事件作初步推测；(3)检查从犯罪现场收集得到的数据，并根据收集到的数据阐明关于事件的假设；(4)验证与事件有关的假设；(5)形成最后结论。Miller等人提出的物理犯罪现场事件重构模型是基于物理犯罪现场而构建的，模型概括地描述了事件重构的基本步骤，没有在实施细节方面展开探讨。

Rynearon描述了"一般现场"的重构方法[3]，明确了对象如何到达某一状态。该方法侧重于犯罪现场的评估，独立对象的识别，对象之间的关系，以及对犯罪现场环境的调查。犯罪现场的每一个对象都可能包含揭示事实的调查线索，该方法中的调查线索包括关联线索、功能线索，以及时间线索。关联线索是指某一对象的位置以及与其它对象的相对位置之间的信息。功能线索是指某一对象的运行环境。时间线索可以由时间的相互影响或证据所依托的运行环境得知。Rynearon所提出的重构方法首先掌握犯罪现场的初始情况，其次构建可能发生的主要事件，并提出与事件有关的假设。若能找到否定某一假设的证据，重构则需返回至初始状态，并说明否定假设的原因。

Bevel和Gardner提出了一种概念信息分析模型[4]，该模型首先收集数据信息，评价、判断数据信息的可靠性及可信性。其次，寻找与事件相关的证据，并确定证据的最小单元、该最小单元与其它证据最小单元的关系，以及各事件之间的时间关系。最后，把事件的各个单元进行排序，重组成一个较大的事件。

Casey和Turvey将事件重构运用到数字调查中，运用时间信息、关联信息和功能信息对需重构的事件进行分析[5]。例如，利用从文件、日志，或者对目击者询问得到的信息中构建时间链。对于关联信息的获取，利用从相关设备中得到的信息，或对犯罪嫌疑人的讯问、对受害人的询问中判断可能发生了何种攻击，以及是否还存在其他有力证据。利用功能分析确定一台计算机或一个用户是否执行了证明某一犯罪成立的事件。

上述模型大多是从事件本身的角度进行事件重构，强调针对某一事件，寻找与其对应的原因与结果对象。在重构过程中，出发点是从事件本身开始的，故在重构多个事件时，容易导致重复分析涉及多个事件的同一对象。因此，本文对上述事件重构模型进行了总结，并从事件中对象的角度出发，利用事件中的对象角色关系，构建了一种抽象数字事件重构模型，该模型从对象角度出发，逐步分析与对象所对应的各个事件，有效地解决了对象重复分析问题。

2　基本概念

为了更好地理解抽象数字事件重构模型，首先对与数字事件有关的概念进行界定。

杨莉莉　博士研究生，主要研究方向为计算机犯罪侦查、数字取证；杨永川　教授，博士生导师。

数字数据：以数字形式表示的数据，通常情况下以二进制数来表示。

数字对象：是指数字数据的离散集合，如存储有数字数据的文件、日志、数据包、进程等。数字对象根据其功能、特性等因素的不同，有着各自特有的属性。

对象的状态：指对象所具有的属性值。如文本文件稍作改动，则对应该文件的对象就会有新的状态。对象状态的改变即指对象的属性值发生了变化。

事件：指一个或几个对象状态的改变。犯罪则属于违反法律或政策法规的事件。

数字事件：一个或多个数字对象的状态发生改变。由于数字对象存储于物理形态的介质当中，因此，数字对象的状态既可以被物理事件所改变，也可以被数字事件所改变。

事件的证据：如果事件改变了某一对象或某些对象的状态，状态发生变化的对象则成为事件的证据。由于数字数据存储于物理形态的介质当中，因此，用于存储数字数据的物理形态的介质，若可作为证据，则为物理证据。物理形态介质所存储的数字数据，若可用作证据，则为数字证据。例如储有数字数据的硬盘，硬盘为物理证据，硬盘中存储的数字数据为数字证据。

事件重构：利用证据的特征，还原某一现场事件发生的过程。

3 抽象数字事件重构模型

事件重构是在证据已被收集，并已对证据分析后进行的。主要目的是对犯罪事实进行还原，以便向法庭证明犯罪事实的存在，并展示犯罪事实的发生原因、经过及结果。模型由证据检查、角色分类、事件重构、事件排序，以及结论生成5部分组成，如图1所示。

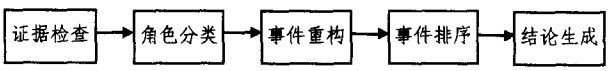

图1 抽象数字事件重构模型

3.1 证据检查

在证据检查阶段，对在犯罪现场发现的证据进行全面检查，确定证据的属性，判断哪些可以作为事件重构中的证据，哪些不在事件重构证据之列，以及确定哪些属于同一事件重构的证据。在这一阶段，为了掌握所有对象的相关信息，我们检查对象的类属性及特有属性，并给出所有对象的属性列表。类属性是指可与一组事物相关联所具备的属性，特有属性是指区别于其他事物而唯一确定某一事物所拥有的属性。由于数字证据承载于物理介质中，对于数字证据的检查，首先要判断哪些物理证据可能包含数字证据，因此该阶段既包括物理证据检查，也包括数字证据检查。

3.2 角色分类

3.2.1 角色定义

在具体的事件中，对象的角色可分为原因对象和结果对象。原因对象是指在某一事件中，用于引起结果产生的对象，在此事件中，若没有该原因对象则不会产生相应的结果对象。结果对象是指在事件中，若对象的状态被其他对象所改变，则称该对象为结果对象。同一对象既可能是原因对象，也可能是结果对象。因此，对于任一对象都存在3种可能的状态，即原因对象、结果对象、原因结果对象。根据原因及结果之间的关系，我们也可将事件表示为利用一个或多个对象的属性，来改变一个或多个对象属性的过程。我们用图示来表示原因、结果及事件之间的关系，如图2所示。每一个圈代表一个对象的状态，每一个方框代表一个事件，在图2中，a,b,c 为事件 E 的原因对象，d 为事件 E 的结果对象。

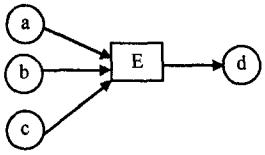

图2 事件图

3.2.2 角色分类分析

对犯罪现场的每一个对象检查完毕之后，调查人员会得到事件及对象的基本信息。对于一个完整连续的事件 E，很难清晰地判断出它的原因对象及结果对象，因此，将连续的事件分割成离散的子事件 $e_0,e_1,\cdots,e_k$ 易于分析，事件 E 为各子事件按照某种规则形成的事件链 $(e_0,e_1,\cdots,e_k)$。对每一个子事件，调查人员分别对其进行分析，找出与每一个子事件相关联的对象，并根据对象的基本信息以及与其他对象之间的关系，判断出所要分析对象的角色是原因对象还是结果对象。

3.3 事件重构

在对事件中的证据进行角色分类之后，我们将根据证据的角色，以及该证据在事件中与其他对象之间的关系，对事件进行重构，并检验重构是否正确。事件重构以对象的收集、对象角色的判断以及对象属性的明确为前提，最终构造出无序事件集，或部分有序事件集。

对于每一个发生的事件，都有与其对应的原因对象及结果对象，在这个阶段中，我们要试图寻找原因对象与结果对象相匹配的原因结果对。结果对象属性的改变与原因对象属性有着密切的关系。因此，若知道在某一事件中哪些结果对象的属性发生改变，我们则可以向前回溯，找寻原因对象。同理，我们也可以利用原因对象属性向后推理，寻找结果对象。事件重构过程如图3所示。事件重构的基本策略如下：

(1)选择某一事件中对当前被调查事件至关重要、属性变化最明显、且未被分析的结果对象。

(2)向前回溯查询所有可能的原因对象，这些原因对象中的一个或几个特征属性对结果属性的变化有影响。若需要，还应搜寻犯罪现场中其他的对象。

(3)对于已经找到的可能的原因对象，检查其类属性及特有属性，判断对于该事件的发生，是否还需要其他原因规则，若需要，则为事件发生的条件增加其他的原因规则，寻找满足角色规则的原因对象。

(4)如果在向前回溯查询中，找到一个或多个原因对象，之后的工作要向后推寻同一事件中的与原因对象相对应的结果对象。这个过程可能要对犯罪现场进行重新搜索。

(5)若在推寻结果对象过程中找到了并非与原因相对应的结果对象，则转至步骤(2)，执行新一轮的回溯查询原因对象。

(6)若没有搜寻到事件的其他原因对象和结果对象，说明该事件不缺少其他角色，则对事件进行检验，可以通过模拟实验、专家评断等方式对事件进行验证。若在事件中缺少某些角色，则提出假设，缺少何种角色，为何缺少该角色。

(7)计算被检验事件的信任度。在这里，信任度 V 与支持该事件成立的证据量 E_s 成正比，与反对该事件成立的证据量 E_o 以及与支持该事件成立，但未被找到的证据量 E_n 成反比，即 $V=K\frac{E_s}{E_oE_n}$，K 为自由调节系数，由调查人员根据具体

的案情、调查环境等因素衡量 K 的取值。若信任度 $V \geqslant P$，则事件检验通过，否则事件检验失败。P 为经验值，由调查人员或专家根据经验及其他因素选取。如果事件检验通过，那么可以认为该事件为某一完整事件中的一个子事件，并添加到可信事件集中。若事件检验失败，则丢弃该事件。

(8)对于某一结果对象，若未检验完与其对应的所有事件，则转至步骤(2)，寻找除上述被检验过事件外，在另一事件中，与该结果对象对应的其他原因对象。所要寻找对象集合的子集中不能包含有之前寻找到的对象，若将要寻找的原因对象集合的子集用 A 来表示，将已经找到原因对象的集合用 a 来表示，则 A 须满足 $a \notin A$。我们选择不同的原因对象集，目的是为了避免创建已经被检验过的同一事件。

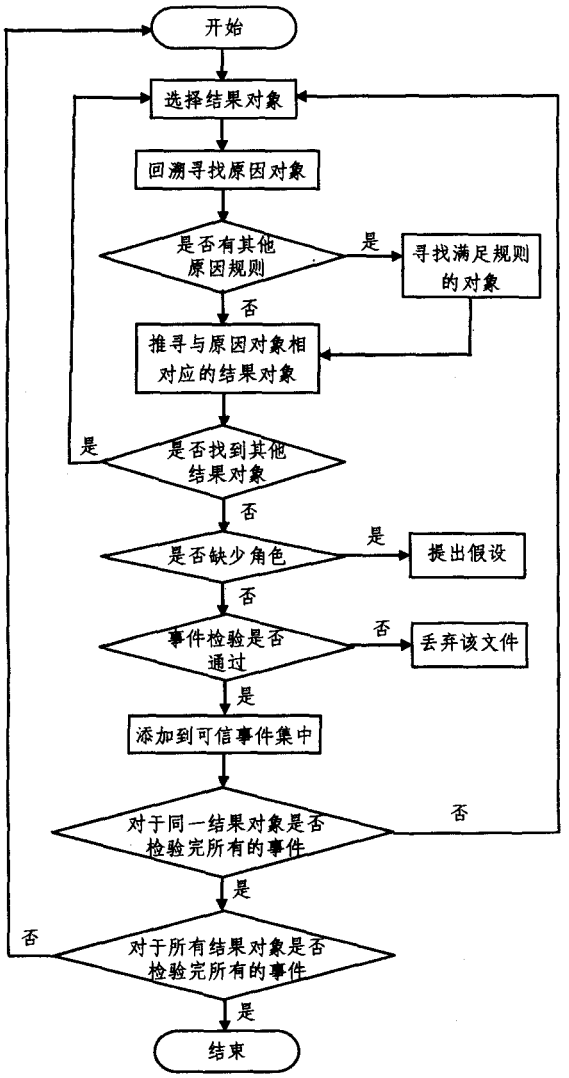

图 3　事件重构流程图

(9)当某一结果对象所对应的事件全部检验完毕后，判断是否对所有结果对象对应的事件检验完毕。若还有其他的结果对象未被检验，则转至步骤(1)，重复搜索过程，寻找其他结果对象所对应的事件。当所有结果对象都被检验完毕后，过程结束。

当事件检验通过后，将其添加到可信事件集，且构造该事件的事件图。若其中某一事件中的结果对象是另一事件的原因对象，则可将其中包含原因对象及结果对象较少的事件移至包含原因对象及结果对象相对较多的事件中，将重复的原因对象或结果对象进行合并，前提是这两个事件必须经过检验成功后方可进行上述移动，如图 4 所示。

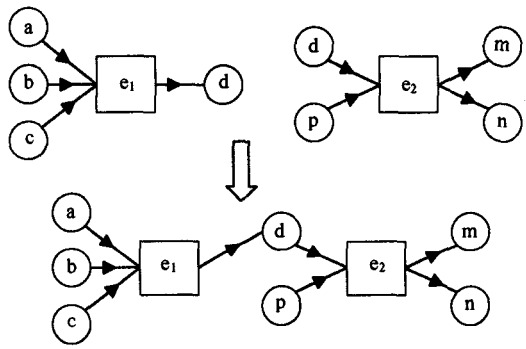

图 4　重组后的事件图

3.4　事件排序

对子事件进行重构后，可将这些子事件联系在一起形成一个完整的事件链。在通常情况下，无法构造一个完整的事件链，甚至无法为收集的所有证据构造出其相应的事件链，但可以对所掌握的子事件进行排序，构造出多个子事件链，几个子事件链联系在一起便可以揭示出有关完整事件链的信息。利用事件排序技术对事件进行排序后，可能会产生多个子事件链。对于这些子事件链，原本应将其排进一个完整的事件链之中，但经过排序后有可能形成多个子事件链，为了说明事件链之间的不衔接之处，在已知发生的不衔接事件链之间建立必要的衔接假设，将各子事件链统一在一起。

3.5　结论生成

经过对证据的检查、证据角色的分类，根据分析后的证据对事件进行重构，再把通过验证的子事件排序成有序或部分有序的事件链，至此，数字事件重构过程基本完成。为了对事件重构有一完备的描述，以便日后工作参考借鉴，最后还要对这一事件的重构过程进行归档，详细记录从证据检查到事件排序每一个过程的具体细节，包括参与工作的调查人员、时间、地点、环境，采取的策略、方法、技术、工具，以及在重构过程中出现的各种问题、解决方法、最终的结果等详细内容。最后形成《××事件重构报告》，留存归档。

结束语　本文在国外学者对事件重构研究的基础上提出了一种抽象数字事件重构模型，并介绍了模型各模块的具体功能及重构的工作流程。该数字事件重构模型从对象角度出发，由事件中的对象联系到与对象相关的事件，从而避免了涉及多个事件的同一对象的重复分析。此外，由于具有同一对象的两个或多个事件之间可能存在着某种联系，因此，利用抽象数字事件重构模型，从对象出发寻找与之对应的所有事件，可以较容易地分析出各事件之间的关联性。该模型的主要目的是对数字事件进行重构，证明计算机犯罪事实的存在，还原计算机犯罪过程。在实际公安工作当中，该模型曾多次应用到计算机犯罪案件调查中。实践证明，抽象数字事件重构模型是一种行之有效的数字事件还原方法。

参 考 文 献

[1] james S, Nordby J. Forensic science: an introduction to scientific and investigative techniques. Boca Raton, FL: CRC Press, 2003
[2] Lee H, Palmbach T, Miller M. Henry Lee's crime scene handbook. London, UK: Academic Press, 2001
[3] Rynearson J. Evidence and crime scene Reconstruction. 6th ed. Redding, CA: National Crime Investigation and Training, 2002
[4] Bevel T, Gardner R M. Bloodstain Pattern analysis: with an introduction to crime scene reconstruction. 2nd ed. Boca Raton, FL: CRC Press, 2002
[5] Casey E. Digital evidence and computer crime: forensic science, computers and internet. 2nd ed. London, UK: Academic Press, 2004