Modeling Digital Forensics Process – An IDEF∅ Model

Corinne Rogers

Preamble

Digital Records Forensics arises from the intersection of digital forensics and digital diplomatics to identify records in digital systems, assess their authenticity, and establish the requirements for their long-term preservation. The Digital Records Forensics research team modeled the process of conducting a digital forensics investigation in order to assess the moments in which records, as understood by archival science and laws of evidence, could be identified, their authenticity assessed, their reliability and integrity managed and preserved. The goal is to integrate the core requirement of digital forensics to establish, document and protect chain of custody, with the InterPARES Chain of Preservation model for the creation and preservation of digital records that can be presumed authentic and maintained reliable.[1]

Purpose

The purpose of the digital forensics model is to unify the concepts of digital forensics practice that have been captured in several process models previously (Beebe & Clark, 2005; Carrier & Spafford, 2006; Ciardhuáin, 2004; Mocas, 2004; Palmer, 2001; Pollitt, 1995; Reith, Carr, & Gunsch, 2002) and lay the foundation for integrating this work with the Chain of Preservation model for managing records throughout their life cycle. The activities represented in the model are intended to ensure the creation and/or collection of trustworthy digital records to be used as evidence, their maintenance throughout the judicial process, and their preservation over the long term for accountability, reference, or further action.

Perspective

The team approached the task of modeling the digital forensics process from the perspective of law enforcement. The end result, therefore, is the identification and production of digital probative material that would be admissible as evidence in a court of law. However, the model is also broad enough to apply to the analysis of security incident response.

Scope

The model has within its scope all the phases or stages in the lifecycle of digital material that may be subject to forensic analysis in the process of investigation of a crime or security breach. It situates this material in the context of a juridical system and considers the whole process of investigation as a balance between available

[1] The Research Team would like to thank Clive Blackwell, Department of Computer Science, School of Technology, Oxford Brookes University, Oxford, UK for his insightful comments and review of the model.

inputs, constraints or controls on the investigation, mechanisms available in the investigation, and desired outcomes or outputs from the investigation.

IDEF∅ Function Modeling Method

IDEFØ is a method of graphical representation of the decisions, actions, and activities of an organization or system in order to analyze and communicate the functional perspective of that organization or system. As a communication tool, IDEFØ enhances domain expert involvement and consensus decision-making. As an analytic tool, the model helps identify functions performed, what is needed to perform them, and the efficacy with which they are performed. IDEFØ was released by the National Institute of Standards and Technology (NIST) in 1993 as a standard for Function Modeling (www.idef.com/IDEFØ.htm).

IDEFØ proceeds in a top-down, general-to-specific modeling approach that results in a hierarchical series of diagrams that gradually increase the level of detail describing functions or activities and their interfaces within the context of a system. The most general features come first in the hierarchy, as the whole top-level activity is decomposed into sub-activities that compose it. Those sub-activities may be further decomposed until all the relevant detail of the system being modeled is adequately exposed and described.

The result is a graphic, structured representation of the activities in a system, supplemented with textual description. One of the challenges of this method is that the representation of activities is not intended to be temporal, but the graphical box-and-arrow format can, without intent, embed an implied temporal sequencing.

Each IDEFØ model has a top-level context diagram (A-0) in which the subject of the model is represented by a single box with its bounding arrows. This diagram represents the boundary of the process under study with respect to purpose, scope, and perspective of the model.

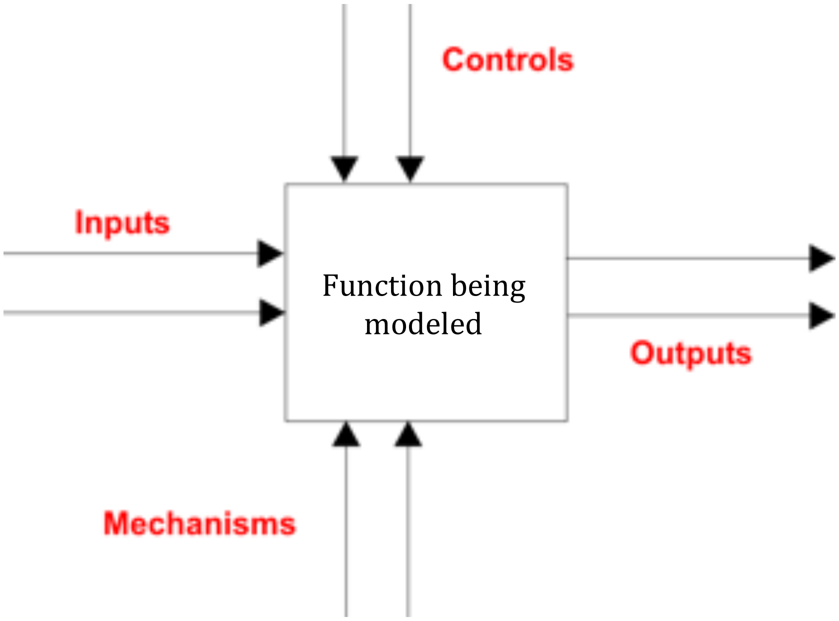

Figure 1: Structure of an IDEFØ Diagram

Box: Each box represents a single function or activity to be modeled.

Inputs: These are information, materials, objects, or data that are consumed, or transformed by the activity to produce outputs.

Controls: These are conditions required to produce the correct output. Controls impose rules that regulate the performance of an activity.

Mechanisms: Mechanisms are the physical resources or means used to perform or facilitate the activity. They may be people, infrastructure, or equipment.

Outputs: These are information, materials, objects, or data that are produced by the activity. If an activity does not produce any outputs, it should not be modeled.

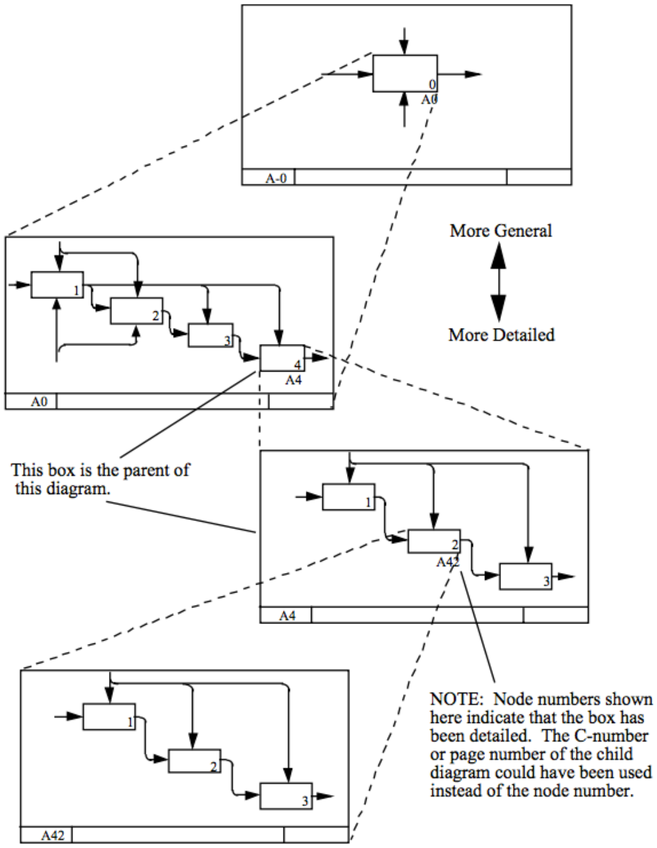
0
A0
A-0
More General
More Detailed
1
2
3
4
A4
A0
This box is the parent of this diagram.
1
2
A42
3
A4
NOTE: Node numbers shown here indicate that the box has been detailed. The C-number or page number of the child diagram could have been used instead of the node number.
1
2
3
A42

Figure 2: Decomposition Structure

Overview of the Digital Forensics Process Model

Conduct Digital Forensics (A0)

This top-level diagram delineates the subject of the model and its overall context. The bounding arrows represent the primary inputs, controls, mechanisms, and outputs. The activity represented in this diagram and all subsequent decompositions are intended to ensure the creation and/or collection of trustworthy digital records to be used as evidence, their maintenance throughout the judicial process, and their preservation over the long term for accountability, reference, or further action.

Constraints on the digital forensics process

Digital forensics is always conducted within the context of constraints and controls imposed by the juridical system in which the investigation takes place, the resources available to undertake the investigation, and the principles of digital forensics practice that are recognized through methodological and theoretical development of the discipline.

Resources available to the investigator include personnel, financial support, tools and technology, and specialized, or domain knowledge.

Digital Forensics Principles have developed to support the purpose of digital forensics investigations. They have been summarized by a variety of domain experts, and include under the guiding principle: "Action taken to secure and collect electronic evidence should not change that evidence" (US Department of Justice, 2001) concepts of

- Integrity
- Authentication
- Reproducibility
- Non-interference
- Minimalization

These concepts and principles are themselves governed by the laws of evidence, and relevant national and international standards. Finally, the investigation will also be constrained by the organizational framework within which it directly takes place.

Mechanisms instrumental to the digital forensics process

Many resources are required to conduct a successful digital forensic investigation. Most commonly, these will include litigators, investigators, digital forensics experts, and the tools, equipment and facilities they use. The model recognizes that records managers may also play an important role in recognizing records in context and offering domain expertise in records related issues such as privacy, assessment of authenticity, reliability, and accuracy, and requirements for preservation and access.

Inputs to the digital forensics process

By definition, the inputs at the top level of the model represent information or objects that originate outside of the activity being modeled. In a digital forensics investigation of a crime or system breach, an indicator is required – some information about unusual, suspicious, or criminal activity. The indicator may result in a complaint – a written or oral request to investigate. The activity may be conducted on a live digital system, on digital materials collected by an investigator, or materials produced by the other party. The activity may also be supported by records created by the investigator, or by exhibits released from the court with their accompanying documentation.

Outputs of the digital forensics process

Many different outputs may proceed from the top level activity, but all can be categorized as evidence submitted to counsel or to court, materials stored or preserved from the case and its investigation, and physical property that may be returned to its rightful owner at the completion of the investigation or trial.

The Six Main Digital Forensics Activities

The model distinguishes six main activities: 1) Prepare for forensic analysis; 2) Collect authorized digital materials; 3) Analyze digital materials; 4) Reach Conclusions; 5) Submit evidence package; and 6) Manage case materials.