Towards Goal-Driven Digital Forensics Investigations

Benjamin Aziz

School of Computing
University of Portsmouth
Portsmouth PO1 3HE
United Kingdom
benjamin.aziz@port.ac.uk

Abstract. In this paper, we present a new method for guiding digital forensics investigations based on goal-driven requirements engineering methodologies. Goal-driven requirements engineering methodologies, like KAOS, facilitate modeling and reasoning about goals and requirements as well as their operationalisation and responsibility assignments. We believe that this new method will lead in the future to better management and organization of the various steps of forensics investigations in the cyberspace as well as provide more robust ground for reasoning about forensic evidence.

Keywords: Digital forensics, investigative methodologies, requirements engineering

1 Introduction

Digital forensics is a complex and important field emerging as a result of the increasing nature and complexity of modern day cybercrime and the ever increasing utilization of computer systems and digital media in real world crimes. Digital forensics, as a result, has grown out of the need to enforce law and justice in the domain of cyberspace bringing together the whole body of knowledge in computer sciences to the legal system of the society.

Various models, e.g. [1-5], have been proposed to capture the process of a digital forensics investigation, which have the purpose of managing and organizing a digital investigation rather than dictating its specific steps and procedures. Nonetheless, such models have remained at an informal level of expressivity and there are very few attempts in literature that aim at the formalization of what a digital forensics investigation is [6]. Such formalization would have several benefits [6], which can be classified as *procedural* reducing the amount of data and their management, *technical* allowing digital forensic investigations to be modified regardless of the technological changes underlying them, *social* in that the capabilities of an attack are captured within the social as well as technical dimension and finally *legal*, in that it allows the expression of the legal requirements of a digital forensics investigation.

adfa, p. 1, 2011.

The approach we introduce in this paper advocates the use of goal-driven formal requirements engineering methodologies, such as KAOS [7], in formalizing the goals, procedures and responsibilities involved in any digital forensics investigation. The main product of this approach would be to establish a pattern library for various investigation models. This library can then be used to the benefit of the investigators in *guiding* an instance of a digital investigation based on the main goal of the investigation and providing suggestions for ways to implement the requirements of the investigation and assigning responsibilities to the qualified personnel or automated systems.

The rest of the paper is organized as follows: In Section 2, we provide a brief overview of the KAOS requirements engineering methodology. In Section 3, we demonstrate how the various elements underlying a digital forensics investigation can be expressed in KAOS model elements. In Section 4, we give an example of this mapping applied to network forensics. Finally, in Section 5, we conclude the paper giving some insight into future pathways for our approach.

2 Brief Overview of KAOS

Knowledge Acquisition in autOmated Specification (KAOS) is a generic methodology based on capturing, structuring and precise formulation of system goals [7]. A goal is prescriptive description of system properties, formulated in non-operational terms. A system includes not only the software to be developed but also its environment. Goals are refined and operationalised in a top-down manner as the system is designed or in a bottom-up approach while reengineering existing systems. The approach also supports adverse environments, composed of possibly malicious external agents trying to undermine the system goal rather than to collaborate in the goal fulfillment.

A KAOS *model* is composed of a number of sub-models. We mention here three such sub-models that are mostly relevant to our approach:

- The *goal model* captures and structures the assumed and required properties of a system by formalising a property as a top-level goal which is then refined to intermediate sub-goals and finally to low-level requirements representing goals that can be operationalised. Goals may be organized in AND/OR refinement/abstraction hierarchies, where higher-level goals are generally strategic, coarse-grained and involve multiple agents whereas lower-level goals are technical, fine-grained and involve fewer agents. In such structures, AND-refinement links relate a goal to a set of sub-goals possibly conjoined with domain properties or environment assumptions; this means that satisfying all sub-goals in the refinement is a sufficient condition in the domain for satisfying the goal. OR-refinement links relate a goal to a set of alternative refinements. KAOS also provides the means for expressing a set of desirable properties of the AND/OR refinements, which includes the completeness, consistency and minimality of the refined sub-goals.
- The *agent model* assigns goals to agents in a realizable way. Discovering the responsible agents is the criterion to stop a goal-refinement process.

- The *operation model* details, at a state-transition level, the actions an agent has to perform to reach the goals it is responsible for.

It is worth noting that the rigor of the KAOS methodology stems from the fact that any concepts defined within its sub-models incorporate formal definitions using Linear Temporal Logic (LTL) [9] formulae. In this paper, we do not delve into LTL encodings of the forensic requirements, however these have the potential for establishing formally verified pieces of evidence due to the current support from technologies such as model checking, theorem proving and static analysis.

3 Goal-Driven Digital Forensics Investigations

In this section, we demonstrate how elements of a digital forensic investigation can be mapped to KAOS model elements. We assume that a digital forensic investigation consists of *processes*, *actions* and the *personnel* including law enforcement agencies and the active systems used by the personnel.

3.1 Forensic Investigations as the Root Goal

The starting point is to map a forensic investigation into the KAOS goal model. This is done by defining the root goal of a KAOS goal tree as a representation of the top-level digital forensic investigation, as shown in Figure 1.

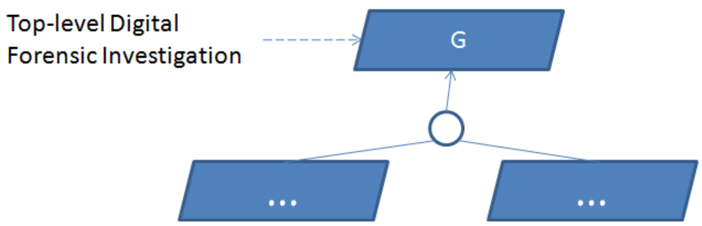

Fig. 1. Mapping Digital Forensic Investigations

In this sense, a digital forensic investigation is seen as the top-level goal that the responsible law enforcement agency aims to achieve, and is therefore the root of the KAOS-based goal tree. Examples of such a goal would be *investigate fraud case in some bank*, *investigate case of identity theft*, *investigate online criminal activity* etc. However, it is important to keep in mind that such a root goal is necessarily abstract at this stage, with the next step aiming at its refinement in terms of more concrete goals.

3.2 Forensic Processes as Sub-goals

The next mapping involves the various steps of the investigative process. For simplicity, we adopt McKemmish's [8] early and simple model, which defines a digital forensic process as "*The process of identifying, preserving, analyzing and presenting* *digital evidence in a manner that is legally acceptable*." This definition implies the activities of *identification*, *preservation*, *analysis* and *presentation*. These are modeled in terms of the sub-goals of the root goal representing the top-level investigation, as shown in Figure 2.

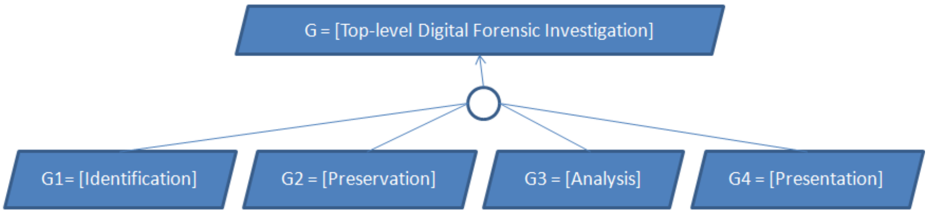

Fig. 2. Mapping Digital Forensic Activities

The specific steps involved in each of these activities will represent further sub-goals that must be achieved in order for the activity to be achieved. Such sub-goals may be linked by either the AND or the OR refinement relations. The refinement of Figure 2 is an example of an AND-refinement, which implies that unless all the sub-goals (identification, preservation, analysis and reporting) are satisfied, the main goal of the investigation will not be considered to have been achieved.

A different type of refinement is the OR-refinement, which implies that any of the sub-goals is sufficient for the achievement of the parent goal. For example, in the case of the analysis of the image corresponding to a hard disk acquired from the scene of a crime, the investigators may need to achieve both of the two different types of analysis of log files such as the analysis of the files' metadata and internal content (AND refinement), but may have more than one choice in one of the two analyses, for example, the internal analysis may be a choice of either a simple data carving or a deeper analysis of hidden and obfuscated data (OR refinement).

Each of the above main activities will be refined until one arrives at the lowest possible *requirements* corresponding to specific elements of each activity that cannot be refined (detailed) any further. A requirement is considered a *leaf* in the goal tree of the main investigation. Once all the requirements have been identified, it is necessary to a) *operationalise* by means of appropriate operations and b) *assign* the requirements to the responsible agents.

3.3 Forensic Actions as Operations

Once the goal tree has been completely specified starting from the top-level digital investigation goal and ending with the leaves corresponding to the low-level requirements, these requirements (and consequently the goal tree) need to have the necessary and sufficient forensic actions in order for the requirements to be *operationalised* leading to the satisfaction of the main goal of the investigation

Figure 3 illustrates how the sub-goal *Identification* can be first refined to the three requirements of authorized legal seizures, seizures of suspected PCs and seizures of suspected mobile devices. These then are operationalised in terms of the three operations: *warrant issuing*, *PC seizure* and *mobile device seizure*.

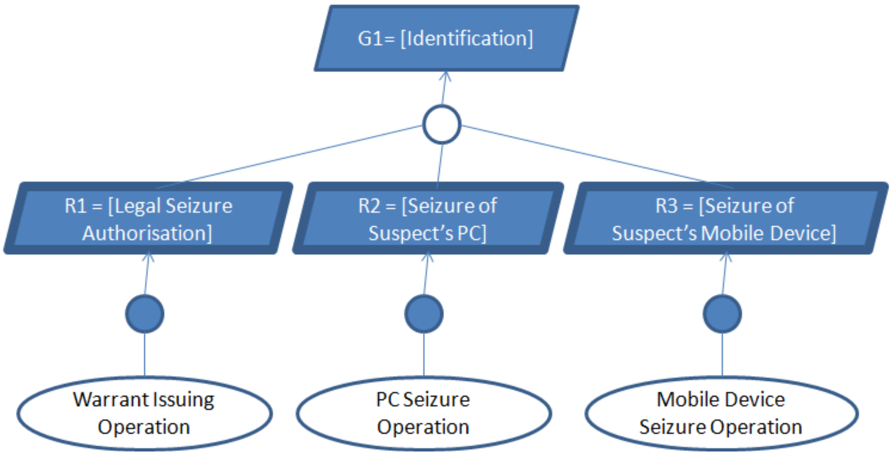

Fig. 3. Requirements Operationalisation

In general, the assignment of the requirements to the operations is crucial as it ensures that every requirement of the forensic investigation will be satisfied through the application of some appropriate operation (or method or activity).

3.4 Law Enforcement Agencies, Personnel and Systems as Agents

The final step in our modeling approach is to model law enforcement agencies and personnel as well as their active systems in terms of the KAOS agents. For example, Figure 4 illustrates a *Forensic Investigator* agent in relation to the requirements and operations of the Identification sub-goal. The dashed line represents the relation that the Forensic Investigator *applies* the forensic operations operationalising those requirements, whereas the solid line represents the relation that the Investigator is indeed *responsible* for the satisfaction of the requirement to which it is related.

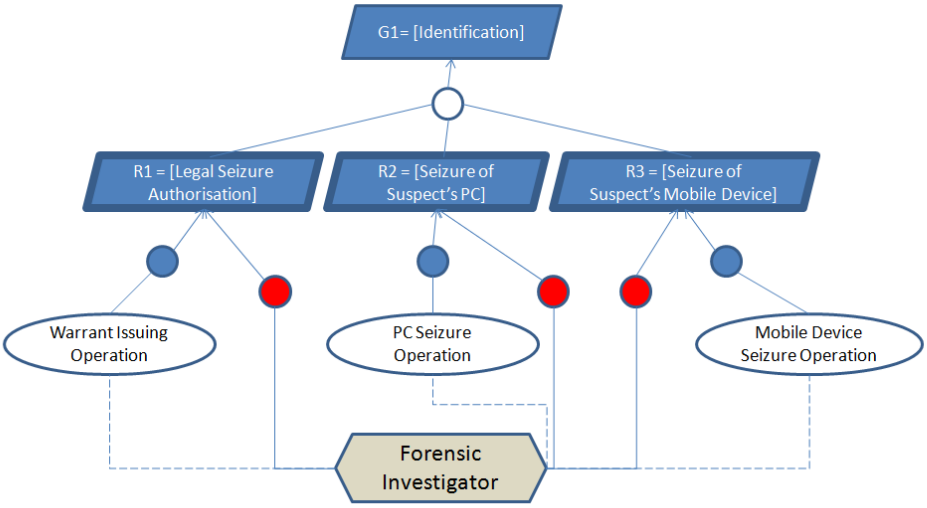

Fig. 4. Responsibility Assignment

4 Example: Goal-Driven Network Forensic Investigation

In this section, we show one simple example where the application of goal-based requirements engineering can be useful in guiding and organizing a digital forensic investigation for the case of suspicious network behavior or incidents inspired from the example by Casey [10]. We have assumed that such an investigation consists of the following steps:

- The *preparation* and *authorization* step, which involves the obtaining of the necessary permissions to proceed and the initial gathering of network information.
- The *identification* step, which involves the identification of the end-points to the network and intermediate systems, the identification of relevant network activities and any supporting systems.
- The *documentation*, *collection* and *preservation* step, which consists of documenting the results of initial examinations such as those that would normally be conducted on the network routers. In the case of Internet activity, this step also will involve the recording of any chat sessions conversations with the suspects. It also involves making sure that any log files are preserved securely by ensuring that cryptographic operations (e.g. hashing) are applied to preserve their authenticity.
- The *filtering* and *data reduction* step, which will involve the definition of data filters and the application of effective search methods of the metadata, in order to remove irrelevant data and reduce the size of the relevant state of the network.
- The *evaluation of source* step, which involves the locating of the various class and individual properties and characteristics such as those relevant to electronic messages, Web access logs and network traffic.

- The *evidence recovery* step, which consists of recovering any deleted and corrupted records and files relevant to the incident, as well as attempting to recover volatile/transient data.
- The *investigative reconstruction* step, which is about reconstructing the criminal scenario through the analysis of various relational, temporal and functional properties.
- The *reporting* step, which is the final step in the forensic investigation process involving the preparation of the final forensic report and the presentation of the findings of the investigation to the judicial system.

These steps are modeled as sub-goals in the tree of Figure 5, with the root goal being the main goal, i.e. the network forensic investigation. For the sake of simplicity, we have omitted further detail related to the refinement of these sub-goals into low-level requirements that can be directly implemented using forensic tools and applications.

Fig. 5. Part of a Goal Model for a Network Forensics Investigation

5 Conclusions and Future Work

The execution of the process of a digital forensic investigation can be a complex and disorganized exercise, often leading to invalid pieces of evidence or failure in the process leading to the reconstruction of such evidence. Therefore, we agree with Eoghan Casey that the use of a formal methodology in describing the process of a digital forensics investigation "*encourages a complete, rigorous investigation, ensures proper evidence handling and reduces the chance of mistakes created by preconceived theories, time pressures and other potential pitfalls.*" [10] In this paper, we defined one such formal approach based on a well-established and rigorous requirements engineering methodology, namely KAOS.

There are many directions this work can be extended to. First, we plan to provide a general goal library of some of the most common patterns of digital forensics investigations and their requirements. Second, we also plan to investigate other aspects by KAOS, such as the anti-goal model [11], in guiding models of attacks in the cyber world and their relation to real world crime. Finally, we also plan to conduct a case study from the real world to investigate pros and cons of this method in enhancing the process of a digital forensics investigation.

References

1. Cohen, F.: Digital Forensic Evidence Examination, Fred Cohen & Associates, (2009)
2. Ó Ciardhuáin, S.: An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence 3(1), (2004)
3. Ieong, R. S. C.: FORZA – Digital Forensics Investigation Framework that Incorporates Legal Issues. In: 8th Digital Forensic Research Workshop, Baltimore, USA, (2008)
4. Beebe, N. L.., Clark, J. G.: A Hierarchical, Objectives-based Framework for the Digital Investigations Process. Digital Investigation 2(2), pp 146-166, (2005)
5. Reith, M., Carr, C., Gunsch, G.: An Examination of Digital Forensic Models. International Journal of Digital Evidence 1(3), (2002)
6. Leigland, R., Krings, A. W.: A Formalization of Digital Forensics. International Journal of Digital Evidence 3(2), (2004)
7. van Lamsweerde, A.: Requirements Engineering: From System Goals to UML Models to Software Specifications, Wiley, (2009)
8. McKemmish, R.: What is Forensic Computing? Trends and Issues in Crime and Criminal Justice 118, (1999)
9. Vardi, M. Y.. Branching vs. Linear Time: Final showdown. In: 7th International Confrence On Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2001), Springer Lecture Notes in Computer Science 2031, pp 1–22, Genova, Italy, (2001)
10. Casey, E.: Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet (3rd Ed.), Elsevier, (2011)
11. van Lamsweerde, A.: Elaborating Security Requirements by Construction of Intentional Anti-Models. In: 26th ACM-IEEE International Conference on Software Engineering (ICSE'04), IEEE Press, pp 148-157, (2004)