A Framework for Digital Forensics and Investigations: The Goal-Driven Approach

Benjamin Aziz, School of Computing, University of Portsmouth, Portsmouth, UK
Clive Blackwell, Department of Computing and Communication Technologies, Oxford Brookes University, Oxford, UK
Shareeful Islam, School of Architecture, Computing and Engineering, University of East London, London, UK

ABSTRACT

Digital forensics investigations are an important task for collecting evidence based on the artifacts left in computer systems for computer related crimes. The requirements of such investigations are often a neglected aspect in most of the existing models of digital investigations. Therefore, a formal and systematic approach is needed to provide a framework for modeling and reasoning about the requirements of digital investigations. In addition, anti-forensics situations make the forensic investigation process challenging by contaminating any stage of the investigation process, its requirements, or by destroying the evidence. Therefore, successful forensic investigations require understanding the possible anti-forensic issues during the investigation. In this paper, the authors present a new method for guiding digital forensics investigations considering the anti-forensics based on goal-driven requirements engineering methodologies, in particular KAOS. Methodologies like KAOS facilitate modeling and reasoning about goals, requirements and obstacles, as well as their operationalization and responsibility assignments. The authors believe that this new method will lead in the future to better management and organization of the various steps of forensics investigations in cyberspace as well as provide more robust grounds for reasoning about forensic evidence.

Keywords: Anti-Forensics, Digital Forensics, Investigative Methodologies, KAOS, Requirements Engineering

INTRODUCTION

Digital forensics is a complex and important field emerging because 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. The likelihood of becoming a target of cybercrime is a fear of almost every computer user. Therefore, cybercrime is a significant challenging problem that could cause severe financial damage. Digital forensics is a craft-based discipline
that has grown out of the need to enforce law and justice in cyberspace bringing together the whole body of knowledge in computer sciences to the legal system.

Generally cyber criminals leave evidence, which is correlated and analyzed by forensics investigators to understand who, what, why, when, where and how a crime was committed. Forensic evidence should be admissible, authentic, complete, reliable and believable by the legal system to prosecute the criminals (Brezinski & Killalea, 2002). However, anti-forensics methods have recently gained popularity by criminals who aim to interfere with the forensic processes by destroying digital evidence using different methods and tools or increasing the examiners' overall investigation time and cost. According to various international reports, the usage of anti-forensics has recently risen to over one third of cybercrime cases in recent years (Verizon Business, 2009). Therefore, a reliable framework for digital forensics investigations in terms of tools and methods is needed while at the same time addressing anti-forensic methods, particularly when time, cost and resources are critical constraints in an investigation.

Digital forensics investigation 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 (Leigland & Krings, 2004). For example, Carrier (2006) showed that the concept of digital forensics investigations could be mapped onto computing concepts by demonstrating that a particular program created some file, and Gladyshev (2004) analyzed a printer queue to show who printed a particular document. However, these attempts are detailed analyses of single pieces of evidence. Blackwell (2009) systematically analyzed credit card fraud using attack trees, which could also be applied to forensic investigations, and would benefit from using a more formal and systematic methodology.

According to Leigland and Krings (2004), such formalization might have several benefits, which can be classified as follows:

- **Procedural**: By reducing the amount of data and their management;
- **Technical**: By allowing digital forensic investigations to be modified to take account 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 in an investigation.

In this article, we develop a framework to support digital forensics investigations considering possible anti-forensic situations. We use a goal-driven formal requirements engineering methodology called KAOS (van Lamsweerde, 2009) in formalizing the goals, obstacles, procedures and responsibilities involved in any digital forensics investigation. Therefore, we map the KAOS concepts such as goals, obstacles and agents with concepts used in typical digital forensics investigations.

The main contributions of this paper therefore are:

- By providing a structured framework for describing the requirements of forensic processes, including anti-forensic measures, the forensic investigator will be better equipped and guided in dealing with ad-hoc crime scenarios;
- The framework aids the forensic analyst in analyzing the value of evidence collected from the crime scene;
- The use of the concept of goals and requirements along with their operationalization and responsibility assignment captures what is in our view an important aspect of any digital investigation process that is
Related Content

A Novel Medical Image Tamper Detection and Recovery Scheme using LSB Embedding and PWLCM
www.irma-international.org/article/a-novel-medical-image-tamper-detection-and-recovery-scheme-using-lsb-embedding-and-pwlcm/120218/

Spam 2.0 State of the Art
www.irma-international.org/chapter/spam-state-art/75667/

Voice Over IP: Privacy and Forensic Implications
www.irma-international.org/chapter/voice-over-privacy-forensic-implications/52842/

Extended Time Machine Design using Reconfigurable Computing for Efficient Recording and Retrieval of Gigabit Network Traffic
www.irma-international.org/chapter/extended-time-machine-design-using/50721/

ICT Security Policy: Challenges and Potential Remedies
www(irma-international.org/chapter/ict-security-policy/60993/