Research Trends in Digital Forensic Science: An Empirical Analysis of Published Research

Ibrahim Baggili[1], Afrah BaAbdallah[2], Deena Al-Safi[2], and Andrew Marrington[2]

[1] Tagliatela College of Engineering, Department of Electrical and Computer Engineering and Computer Science, University of New Haven, CT
Ibaggili@newhaven.edu
[2] Zayed University, Advanced Cyber Forensics Research Laboratory
Abu Dhabi, United Arab Emirates, P.O. Box 4783
Andrew.Marrington@zu.ac.ae

Abstract. Digital forensic science is a new discipline. In order to advance and improve this science, stakeholders should stay abreast over the research trends in this domain. This research studied, categorized and analyzed a sample of five-hundred publications (n=500) from this discipline. The results indicated that the rate of publication in this domain continues to increase over time. Additionally, results showed an overall lack of anti-forensics research where only 2% of the sampled papers dealt with anti-forensics. In terms of research methodology, the results indicated that 17% of the sampled publications were secondary research, 36% were exploratory studies, 33% were constructive and 31% were empirical. The results also indicated a lack of basic research in this scientific discipline where most of the research (81%) was applied, and that only 19% of the sample was categorized as basic research. Additionally, results exemplified a lack of quantitative research in the discipline, with only 20% of the research papers using quantitative methods, and 80% using qualitative methods. Furthermore, results showed that the largest portion of the research (42.9%) from the examined sample originated from the United States. The findings also showed a lack of cooperative research between academia and industry, where only 10% of the research studies examined where a collaborative effort between industry and academia. Lastly, the findings indicated an increase in the disparity between the number of published articles and the number of cited articles over the years possibly indicating isolation amongst researchers in this domain.

Keywords: Digital forensic science, research trends, research methodologies, challenges in digital forensics science.

1 Introduction

Cybercrime initially emerged as a threat to computer users and businesses; it now impacts entire nations. Internet usage continues to rise and so does this threat [1]. Yet, most computer users remain unconscious of the drastic impact it has on their daily lives. The statement "The Internet is the crime scene of the 21st century" as written in the Wall Street Journal, is a realistic indicator of the current times [2].

M. Rogers and K.C. Seigfried-Spellar (Eds.): ICDF2C 2012, LNICST 114, pp. 144–157, 2013.

Rogers and Seigfried in 2004 reported that cybercrime is constantly on the rise, spurring a massive progress in digital forensic science (DFS) [3]. This has consequently lured the attention of scientists towards a subset of DFS – computer forensics, establishing it as a recognized scientific discipline [4][5].

Patzakis in 2003 described computer forensics as a process of collecting, preserving, analyzing, and presenting electronic evidence where a computer has been an instrument to committing a crime [6]. This investigative methodology is used to reconstruct computer evidence as well as examine digital media storage devices in order to find electronic evidence which could lead to the source of the crime and its perpetrator(s). Furthermore, computer forensics is recommended whenever the security of an organization or company has been breached. In such a scenario, system administrators begin investigations by acquiring and analyzing the collected digital evidence.

Research has been conducted and articles published discussing various topics in DFS. Some researchers have illustrated specific definitions and processes in digital forensics [7], whereas others have published studies addressing anti-forensics [8]. Additionally, certain researchers have focused their attention to incident response and best practices when a computer crime occurs [9]. It is beyond this research paper's scope to provide a complete overview of all the research conducted under the DFS umbrella. Nonetheless, it is critical for scientists as well as practitioners to keep up with research trends associated with the science of digital forensics to acknowledge and further investigate gaps in the domain.

This research provides a strong primary contribution to this new scientific discipline, as it empirically studies research trends in the field. The primary goal is to empirically explore the path that DFS is moving towards through the categorization and analysis of a sample of five-hundred (n=500) publications issued between 1992 and 2011.

2 Literature Review

DFS is at its infancy and continues to be of utmost importance. Governmental agencies are obliged to depend on the scientific and private communities to derive novel methods and tools that allow the extraction and preservation of digital evidence in a scientific and law-abiding manner. Given the importance of this field and its impact, it is essential to collect, analyze, and categorize research in this scientific domain. This can help shed light on the discipline, aiding in a more appropriate response to cybercrime while contributing to the development of the science and professional practice in this field.

Garfinkel in 2010 argued that there is a genuine need for a well defined and collaborative approach to be undertaken by the researchers and institutions in digital forensics [10]. Garfinkel stated that "Without a clear strategy for enabling research efforts that build upon one another, forensic research will fall behind the market, tools will become increasingly obsolete, and law enforcement, military and other users of computer forensics products will be unable to rely on the results of forensic analysis" [10].