Forensic Sci Rev 36:99–125
July 2024

How Ontologies Have Supported Digital Forensics: Review and Recommendations

T. J. Silva[1], E. OliveiraJr[1*], A. F. Zorzo[2]

[1] Informatics Department
State University of Maringá
Maringá, Paraná
Brazil

[2] School of Technology
Pontifical Catholic University of
Rio Grande do Sul
Porto Alegre, Rio Grande do Sul
Brazil

TABLE OF CONTENTS

* Contact information: Dr. Edson OliveiraJr, Departamento de Informática, Universidade Estadual de Maringá, Av. Colombo 5790, Zona 07, 87020900 Maringá, PR, Brasil; edson@din.uem.br.

How Ontologies Have Supported Digital Forensics: Review and Recommendations

REFERENCE: Silva TJ, E. OliveiraJr E, Zorzo AF: How ontologies have supported digital forensics: Review and recommendations; *Forensic Sci Rev* 36:99; 2024.

ABSTRACT: The evolution of digital media has increased the number of crimes committed using digital equipment. This has led to the evolution of the computer forensics area to digital forensics (DF). Such an area aims to analyze information through its main phases of identification, collection, organization, and presentation (reporting). As this area has evolved, many techniques have been developed, mainly focusing on the formalization of terminologies and concepts for providing a common vocabulary comprehension. This has demanded efforts on several initiatives, such as the definition of ontologies, which are a means to identify the main concepts of a given area. Hence, the existing literature provides several ontologies developed for supporting the DF area. Therefore, to identify and analyze the existing ontologies for DF, this paper presents a systematic literature review (SLR) in which primary studies in the literature are studied. This SLR resulted in the identification of ontology building methodologies, ontology types, feasibility points, evaluation/assessment methods, and DF phases and subareas ontologies have supported. These results were based on the analysis of 29 ontologies that aided in answering six research questions. Another contribution of this paper is a set of recommendations on further ontology-based support of DF investigation, which can guide researchers and practitioners in covering existing research gaps.

KEYWORDS: Digital forensics, ontologies, systematic literature review.

INTRODUCTION

The evolution of technology has brought new issues to be addressed in the digital forensics (DF) area, such as storage spaces, complexity in data formats, interpretation of evidence, and collection and identification of all information on a device [19].

One of the great difficulties in DF research and practice is establishing a common vocabulary of terms, technologies, and their relationships [99]. Awareness of such terms is crucial for establishing common ground when researching and practicing DF. In addition, such terminology and their relationships help to avoid error-prone interchanging mechanisms comprehension.

There are different ways to establish such vocabularies, such as conceptual models, mind maps, or metamodels [74]. However, one of the most used techniques is the definition of ontology, which is the study of the kinds of things that exist. In this paper, digital forensics is a representation vocabulary, often specialized to some domain or subject matter. Defining an ontology has several advantages, such as clarifying the structure of knowledge, forming the heart of any system of knowledge representation for a given domain [10], and enabling knowledge sharing [43]. However, the use of ontologies also brings some challenges, like the necessity of a standard vocabulary and respective ontology for a particular research field, difficulty in turning special knowledge into an ontology, the great number of languages to write ontologies for, and the definition of structures (classes) with specific attributes [88].

DF research has increasingly adopted ontologies for different subareas and domains. Such ontologies have contributed to evolving the DF terminology and vocabulary, mainly for different types of applications, encompassing tools/software, evidence analysis techniques and standards, and the DF process [88]. Nonetheless, several challenges remain when applying ontologies to DF.

Although ontologies are a well-known technique to represent knowledge and particularities of a domain and have already been applied to some specific fields in DF, for example, DF of electronic email [93] or privacy reserving in DF [118], to the best of our knowledge, there is no research reviewing such a technique in DF in general. Therefore, we performed a systematic literature review (SLR). This review provides researchers and practitioners with a panorama of existing ontologies and how they were conceived to attend to specific DF research topics. We expect readers to gather knowledge on how ontologies might contribute to their activities, thus exposing research gaps in the form of recommendations.

Digital Forensics

With the evolution of digital devices, such as cell phones, computers, and tablets, crimes committed by these means have increased in volume and complexity, with the aim of illegally acquiring information [108]. As a way of investigating, prosecuting, and combating such crimes, a branch of forensic science has appeared, named DF [99,101,102].

ABOUT THE AUTHORS

T. J. Silva; E. OliveiraJr
A. F. Zorzo

Thiago J. Silva has a degree in analysis and systems development from the Cidade Verde University Center of Maringá and an MBA in distance education and new technologies from the University Center of Maringá (UniCesumar). He is a Ph.D. candidate at the State University of Maringá and a teacher mediator at UniCesuMarch He has experience in computer science, with an emphasis on Oracle database, and he works mainly on the following topics: PL/SQL, procedures, and functions. He also has experience in digital forensics, working with ontologies.

Edson OliveiraJr has a degree in informatics and a master's in computer science from the State University of Maringá (Maringá, Brazil), and a PhD in computer science from the Institute of Mathematical and Computer Sciences, University of São Paulo (ICMC-USP 2010) (São Paulo, Brazil). He was a visiting scholar (Feb-Dec 2009) at the University of Waterloo (Waterloo, Canada) and a postdoctoral fellow (2018–2020) in experimentation in digital forensics at Pontifical Catholic University of Rio Grande do Sul (PUCRS) (Porto Alegre, Brazil). He was also a visitor professor at PUCRS (2022-2023) researching education and training of digital forensics. Dr. OliveiraJr is currently an associate professor in the informatics department at the State University of Maringá (Maringá, Brazil).

Dr. OliveiraJr has experience in computer science, with an emphasis on software engineering, working mainly on the following topics: experimentation in software engineering, software processes, software product line, software architecture and product line evaluation, software process line, variability management, metrics and software models, frameworks, UML modeling and metamodeling, development environments, and Java technologies. He also has experience in digital forensics, working in experimentation, requirements, ontologies, conceptual models, and tools for digital forensics. Lately he has supervised MSc and PhD students on digital forensics.

Avelino F. Zorzo has a BSc (1989) and a MSc (1994) degree in computer science from Universidade Federal do Rio Grande do Sul (Porto Alegre, Brazil). He received a PhD in computer science from University of Newcastle upon Tyne (Newcastle upon Tyne, UK) in 1999, andwas a postdoctoral fellow (2012) at the Cybercrime and Computer Security Centre at the same university. Currently he is a professor at Pontifical Catholic University of Rio Grande do Sul (PUCRS), and coordinator for digital forensics at the National Institute of Science and Technology of Forensic Sciences (Porto Alegre, Brazil), financed by the Brazilian government. Lately he has supervised MSc and PhD students on digital forensics.

Dr. Zorzo served as the education director of the Brazilian Computing Society (2015–2017) and was coordinator for postgraduate accreditation at the Ministry of Education of Brazil (2014–2026). His main research topics are security, digital forensics, blockchain, fault tolerance, and software testing.