Forensic Sci Rev 34:21–41
January 2022

Digital Forensics Experimentation: Analysis and Recommendations

E. OliveiraJr[1]*, T. J. Silva[1], A. F. Zorzo[2], C. V. Neu[3]

[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

[3]School of Computing
Newcastle University
Newcastle upon Tyne
United Kingdom

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.

Digital Forensics Experimentation: Analysis and Recommendations

REFERENCE: OliveiraJr E, Silva TJ, Zorzo AF, Neu CV: Digital forensics experimentation: Analysis and recommendations; *Forensic Sci Rev* 34:21; 2022.

ABSTRACT: Digital forensics (DF) is becoming one of the most prestigious research areas in computer science due to its inherent nature of providing a means to acquire, examine, analyze, and report evidence to be used in legal processes. To successfully perform it, novel techniques, approaches, and tools have been proposed, experimented on, and evaluated by researchers. However, the experimentation process is not a trivial task in this area as substantial evidence is not accepted in court. Therefore, the experimentation process has to be improved in DF, especially its documentation and data sharing to enable its reproducibility. The objective of this paper is to characterize the state-of-the-art research on DF experiments. We conducted a Systematic Mapping Study (SMS), analyzing 107 primary studies reporting DF experiments. We demonstrate that DF experimentation somehow fails at documenting the most essential elements of an experiment, such as hypothesis, variables, design, instrumentation, validity evaluation, setup, training, datasets and benchmarks, statistical techniques (descriptive, hypothesis, and effect-size test), limitations, and data sharing. In this work, we also propose a set of recommendations to improve experimentation in DF, especially regarding its replication and reproducibility. DF experimentation should evolve if the community intends to provide reliable and reproducible studies. By embracing this, both academicians and practitioners might benefit from such experiments and evidence.

KEYWORDS: Evidence, experiment, recommendations, replication.

INTRODUCTION

Experimentation plays a central role in science in general. However, such a role is unclear in computer science [26]. Several different areas of computer science have applied experimentation in the last decades to provide evidence on a certain cause-effect previously established theory [29]. Digital forensics (DF) [14,24] is one of these areas. As DF has grown in the last decades due to the outstanding advance of information technology, it has provided interesting solutions for several different subareas, such as cloud forensics, network forensics, and mobile device forensics. Such solutions have contributed to promoting reliable evidence to be used in legal processes. These solutions go from low-level abstractions, such as volatile memory analysis and network package attack monitoring, to high-level ones, such as cloud computing solutions. DF research plays a central role in the evolution of science, especially criminal sciences.

However, it is widely noted that DF solutions are not empirically evaluated as much as in classical sciences—e.g., medicine. Formal experimentation with DF solutions has been given little attention for reasons such as difficulty establishing experimental designs, time spent, and costs involved to set up and perform such experiments [6]. Besides, such performed experiments are generally poorly reported—hence, the essential information to allow their repetition, replication, or reproduction is missing. Therefore, the reliability and potentiality of science evolution are jeopardized [9,28].

Several authors have discussed different problems regarding DF experimentation. Marshall and Paige [18], for example, discussed the lack of clear requirements for developing new DF methods according to ISO 17025:2017[a] capabilities, especially rigorous scientific method and verification, such as experimentation, and repeatability to provide reliable evidence to be used in court.

Furthermore, Casey [6] previously discussed the challenges of experimental design in DF. According to Casey, "designing good experiments is hardly a trivial undertaking, and has been the focus of brilliant minds at least since the scientific revolution ... experiments in digital forensics pose novel challenges". Such challenges vary from the accuracy of making observations and testing hypotheses from the perspective of the studied environment, the complex influences as the setup of the experiment and the experimental objects used, to the lack of reproducibility to allow someone to run the same experiment multiple times and to verify its results. Casey also discussed experiments' completeness of reporting results and setups. The correct interpretation of findings is another issue to be considered since a degree of scientific skill is required to accurately interpret results and to provide acceptable evidence. Per another viewpoint, Horsman [11,12] discussed the need for admissible evidence in DF. Thus, he claimed that the results of any DF investigation should be reliable, based on scientific procedures and interpretation, and transformed into facts. To do so, he proposed a Framework for Reliable Experimental Design (FRED) [12] applied to the three major DF process phases: acquisition, examination/analysis, and reporting.

[a] *https://www.iso.org/standard/66912.html*

29. Wainer J, Barsottini CGN, Lacerda D, de Marco LRM: Empirical evaluation in computer science research; *Inf Softw Technol* 51:1081; 2009.
30. Wang Y, Peng X, Bian J: Computer crime forensics based on improved decision tree algorithm; *J Netw* 9:1005; 2014.
31. Wohlin C, Runeson P, Höost M, Ohlsson C, Regnell B, Wesslén A: *Experimentation in Software Engineering*, 2nd ed; Springer: New York, NY; 2012.

ABOUT THE AUTHORS

E. OliveiraJr; T. J. Silva
A. F. Zorzo; C. V. Neu

Edson OliveiraJr has a degree in informatics and a master's in computer science from the State University of Maringá (Maringá, Brazil), and a Ph.D. 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 PUCRS (Pontifical Catholic University of Rio Grande do Sul) (Porto Alegre, Brazil). 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 M.Sc. and Ph.D. students on digital forensics.

Thiago J. Silva has a degree in analysis and systems development from the Cidade Verde University Center of Maringá and an M.B.A. in distance education and new technologies from the University Center of Maringá (UniCesumar). He is currently a master's degree student at the State University of Maringá and a teacher mediator at UniCesumar. He has experience in computer science, with an emphasis on Oracle database, working mainly on the following topics: PL/SQL, procedures and functions. He also has experience in digital forensics, working with ontologies.

Avelino F. Zorzo has a B.Sc. (1989) and an M.Sc. (1994) degree in computer science from Universidade Federal do Rio Grande do Sul (Porto Alegre, Brazil). He received a Ph.D. in computer science from University of Newcastle upon Tyne (Newcastle upon Tyne, UK) in 1999 and received postdoctoral training (2012) at the Cybercrime and Computer Security Centre of the same university. Currently he is the coordinator for digital forensics in the National Institute of Science and Technology of Forensic Sciences (Porto Alegre, Brazil) financed by the Brazilian Government. Lately he has supervised M.Sc. and Ph.D. students on digital forensics.

Dr. Zorzo served as the education director of the Brazilian Computing Society (2015–2017) and coordinator for professional postgraduate accreditation for the Ministry of Education of Brazil (2014–2022). His main research topics are security, digital forensics, blockchain, fault tolerance, and software testing.

Charles V. Neu has a B.Sc. (2010) degree in computer science and an M.Sc. (2013) degree in Industrial Systems and Processes from the University of Santa Cruz do Sul (Santa Cruz do Sul, Brazil). He also received a Ph.D. (2019) in computer science—with postdoctoral internship (2019) in experimentation in digital forensics—from the Pontifical Catholic University of Rio Grande do Sul (Porto Alegre, Brazil). Dr. Neu is currently a research associate in the Secure and Resilient Systems Research Group, Newcastle University (Newcastle upon Tyne, UK).

Dr. Neu has experience in computer science, with an emphasis on IT, network and security management, computer networks, security and privacy, working mainly on the following topics: network communication, protocols and standards, network management and monitoring, network and system security, cryptography, privacy, intrusion and attack detection, prevention and response, traffic classification and analysis. Also, he has experience in digital forensics, working in forensic networks, requirements, conceptual models, and tools for digital forensics.