Forensic Science International: Reports 2 (2020) 100137

Contents lists available at ScienceDirect

Forensic Science International: Reports

journal homepage: www.elsevier.com/locate/fsir

Digital Forensics

Mapping digital forensic application requirement specification to an international standard

Victor R. Kebande [a,*], Stacey O. Baror [b], Reza M. Parizi [c], Kim-Kwang Raymond Choo [d], H.S. Venter [b]

[a] Department of Computer Science & Media Technology, Malmö Universitet, Malmö, Sweden
[b] Department of Computer Science, University of Pretoria, South Africa
[c] College of Computing and Software Engineering, Kennesaw State University, Marietta, GA, USA
[d] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA

ARTICLE INFO

Keywords:
Digital forensics
Applications design
Software requirements specification (SRS)
ISO/IEC 27043

ABSTRACT

A potential security incident may go unsolved if standardized forensic approaches are not applied during lawful investigations. This paper highlights the importance of mapping the digital forensic application requirement specification to an international standard, precisely ISO/IEC 27043. The outcome of this work is projected to contribute to the problem of secure DF tool creation, and in the process address Software Requirements Specification (SRS) as a process of digital evidence admissibility.

1. Introduction

As our society becomes more digitalized and interconnected, the need for digital forensic investigation (DFI) will be more pronounced for both civil or criminal proceedings. While it is important to ensure the use of scientifically proven/sound approaches in DFIs, it is not always straightforward due to the rapidly advancing technologies. In addition to the importance of having forensically sound digital forensic processes (e.g., repeatable and accepted by both the scientific and legal communities), developing digital forensic applications (e.g., forensic toolkits) that can be used to reliably and effectively reconstruct, analyze, and cluster events is also crucial in the discipline [1].

A transparent design process that ensures traceability [2] and provides the known error rate of any DF application is essential for its acceptance by the forensic and legal communities [3]. In this context, the digital forensic investigators are considered the technical stakeholders, while the non-technical personnel comprises members of the judiciary, the plaintiff, and the accused person/defendant. All stakeholders need to be assured that the evidence tendered has been obtained by DFAs that have been designed based on industry best practices or international standards.

This reinforces the importance of ensuring digital forensic applications (DFAs) are designed based on correct and sound requirement specifications, which guarantee forensic soundness and admissibility of the evidence obtained using such applications. For example, [4–6] presented a DFA requirement specification (DFARS) process, to facilitate the design of forensically sound applications. The DFARS process considers the interaction of architectural requirements [7–9] and architectural constraints. The architectural requirements include quality requirements, architectural patterns, strategies, and the requirements needed for integration purposes, and the constraints include jurisdictional, legislative, and technological constraints.

In this paper, we posit the importance of having DFI process, including those designed using processes such as DFARS [4,5], to be closely aligned with relevant best practices and international standards, such as ISO/IEC 27043: 2015 [10]. Therefore, using the DFARS [4,5] process as a case study, we map the process to ISO/IEC 27043 [10].

The remainder of this paper is structured as follows. In the next section, we will introduce the relevant preliminaries. In the third section, we will explain how one can map the DRAFS process to ISO/IEC 27043. The last two sections present our discussion and conclusion, respectively.

2. Background

2.1. ISO/IEC 27043

As shown in the classes of digital investigation process in Fig. 1, ISO/IEC 27043 [10] consists of the following processes:

- Digital forensic readiness class (Pre-incident planning and preparation);

* Corresponding author.
E-mail addresses: victor.kebande@mau.se (V.R. Kebande), stacey.baror@cs.up.ac.za (S.O. Baror), rparizi1@kennesaw.edu (R.M. Parizi), raymond.choo@fulbrightmail.org (K.-K.R. Choo), hventer@cs.up.ac.za (H.S. Venter).

http://doi.org/10.1016/j.fsir.2020.100137
Received 18 June 2020; Received in revised form 20 August 2020; Accepted 31 August 2020
Available online 12 September 2020

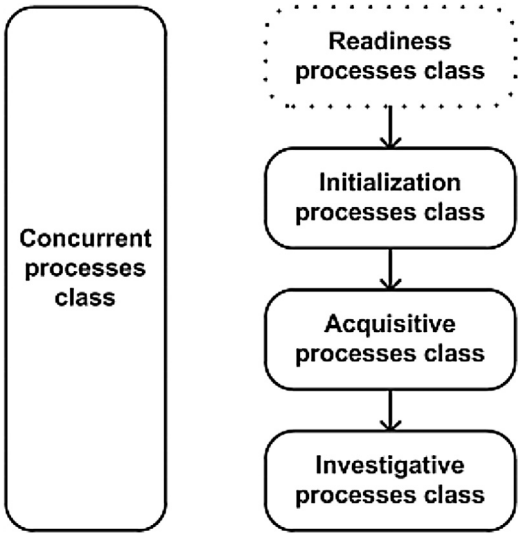

Fig. 1. Classes of digital investigation processes [10].

- Digital forensic investigation class (initialization, acquisition, and investigative processes; see also Fig. 1); and
- Legal principles and other processes pertaining to digital forensic admissibility and retention, like warrants, court orders and approval of evidential material (concurrent processes classes).

One of the key purposes of ISO/IEC 27043 [10] is to guide the forensic investigation processes that can subsequently inform stakeholders, policy-making bodies, decision-makers, and a court of law. For example, digital forensic readiness (DFR; also related to as the forensic-by-design concept introduced in [11,12]) is crucial for incident preparation and planning; and digital forensic investigation class (initialization, acquisitive, and investigative) [10,13] comprises reactive processes that are employed after a potential security incident has been identified [14]. These processes take place concurrently with other investigative processes.

Also described in ISO/IEC 27043 are readiness process groups (RPGs), which represent a state of being prepared for a digital investigation before an incident occurs. Such processes enable stakeholders to be more proactive by anticipating potential security incidents. This allows the mitigation of risks, by putting in place activities or actions that minimize the cost or efforts towards the investigation of such incidents when they eventually occur [15]. RPGs comprise the planning, implementation, and assessment groups, whose main roles are incidental preparation, risk mitigation, and the possibility of feeding the outcome to the post-event response [10,13]. RPGs form part of the proactive strategies that can be employed during the pre-incident investigation process.

The ISO/IEC 27043 standard has specific roles and applications [16], mainly, this standard has a focus on incident investigation principles and processes. Furthermore, it provides guidelines that ensures that there should be a higher chance of admissibility of digital evidence in a court of law. This provides a wider application scope for investigation processes. Notable application area that leverage ISO/IEC 27043 include interpretation of digital evidence, planning and preparation, governance and risk assessment, and information security management strategies [16].

2.2. DFARS process

As previously discussed, ensuring that the DFI investigation is forensically sound and followed is important to ensure the admissibility of the evidence [17]. In such a process, there are both technical and non-technical assumptions.

In non-technical assumptions, for example, process interdependence is important and there should exist a communication mechanism between the processes. The communication mechanism shows a symbiotic-like relationship in order to generate a forensic hypothesis that can be admissible. It is worth to note that the generation of a hypothesis from the DFARS processes that can prove or disprove a fact relies on the following assumptions:

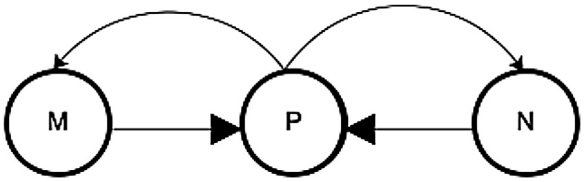

Fig. 2. Successful DFARS process communication.

- If two processes M and N are close to each other with a distance of D, these processes should be linked using a communication channel P, such that $D_M \leqslant P \leqslant D_N$. This assumption allows useful information among the processes to be dispatched among M and N (see Fig. 2). In other words, the processes communicate with each other to successfully achieve a common goal.
- If there exists no correlation among processes during the DFI, then the formulated forensic hypothesis may not be sufficient to be admissible given that the DFARS process could have been infiltrated (see Fig. 3).

The success of a software system can be measured by the extent to which the various conflicting aspects and stakeholders' needs are managed, while achieving the system's intended purpose. To effectively convey these requirements, communication that aligns to the applications' functional, architectural requirements and their constraints is key. For example, primary technical requirements of digital forensic tools include verifiability, portability, scalability, usability, cost-efficiency, and support for multi-user [18–21].

The DFARS process determines the user's and application's needs while using these to determine the architectural needs of the system and in the process addressing the overall needs of all stakeholders. In addressing the needs of the DFARS system, the architectural constraints must be considered at all levels of the design. The "users" in this context include law enforcement agencies, forensic experts and other stakeholders involved in the investigation. In other words, the DFARS process takes into consideration the diverse requirements and from different stakeholder groups in the design of a DFA.

As depicted in Fig. 4, the DFARS process consists of the following five distinct processes:

- DFARS process functional requirements (1): Eliciting events that should be accomplished by the DFA.
- DFARS process architectural constraints (2): To ensure forensic soundness of potential digital evidence (PDE) by the DFA, and constant changes and modifications should be tolerated. Generally, these constraints are focused on the needs and concerns from the stakeholders' perspective. It is important to note that these requirements are crucial when making decisions on the design of DFAs.
- DFARS process architectural requirements (3): In the context of DFARS, these requirements basically involve the collection of useful information that may be needed in designing the architecture.

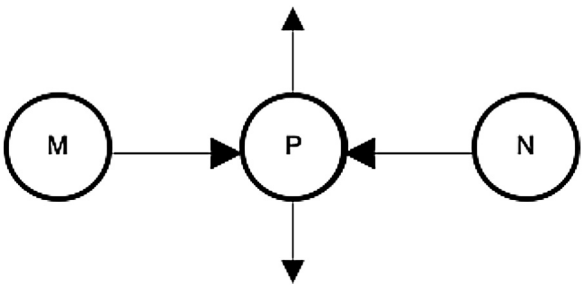

Fig. 3. Unsuccessful DFARS process communication.

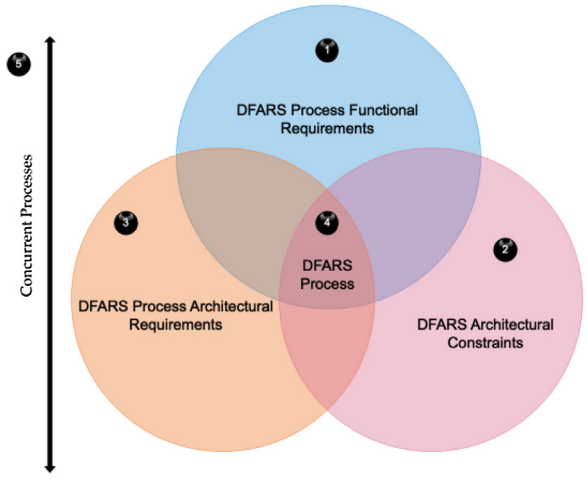

Fig. 4. digital forensic application requirement specification process [4,5].

- DFARS process (4): Determines what the user and the application needs may be.
- Concurrent processes (5): We posit the need for adopting the concurrent processes from ISO/IEC 27043 as part of tool development in order to have an assurance of the soundness of the PDE. These processes should happen in tandem with other processes during the DPA design.

3. Mapping DFARS to ISO/IEC 27043

In our attempt to map the DFARS process to the ISO/IEC 27043 standard, we need to first identify each of the sub-processes of ISO/IEC 27043 and determine how it translates and fits with the DFA using the DFARS process. It is also important is to identify any existing similar objectives between the two. Our mappings for the various levels of the DFARS process as is shown in Tables 1–Table 5. Next, a summary that shows the correlations is given. Where a process is not needed or required during development it is marked by an *X*, and ✓ denotes essential security components or processes.

Before we explain the actual mapping, we will introduce a scenario involving a company, X, that was tasked with managing Social Security Numbers (SSNs). A software failure led to a hack of millions of SSNs in what is thought to be the largest breach of personal information and the following transpired as a result:

- This attack succeed because a potential software failure/bug and as a result X was manipulated in such a manner that the administrators were not able to detect or monitor any transactions in real-time or periodically.
- All the SSN-based transactions were supposed to be logged periodically on an interval of 1 min, however, this did not happen as a result of this compromise.
- This led to the creation of fake tax returns and falsification of identities that targeted fraudulent claims.

Based on the aforementioned scenario, there is a dire need for conducting forensic investigations and it is important to demarcate a trade-off between when standardized approaches needs to be employed and when the tools that satisfies SRS are leveraged. A detailed discussion on the importance of mapping a DFARS to processes that can help increase chances of admissibility is explain systematically.

3.1. Mapping readiness process to DFARS

Forensic readiness is a core business requirement, which can help gather PDE. For example, in the earlier discussed scenario, implementing the ISO/IEC 27043 process or guidelines as part of the DFARS process would allow the collection of incriminating information, say by the internet/telecommunication service provider. We map eight ISO/IEC 27043 sub-processes from the readiness process against the functional requirements, quality requirements, constraints, patterns, and strategies.

3.2. Mapping initialization process to DFARS

To commence an investigation, an incident needs to be detected, this means that the procedures that are needed to detect the incidents should be put in place before commencement. The authors present this as an important process for tool development requirements. While it is also important to highlight that some of the sub-processes in the initialization process may be non-technical, it is also worth stressing the fact that they may be useful for purposes of validating how the DFARS process is conducted. The authors have noted that among the sub-processes in the initialization process, incident detection is a requirement that is needed in all the aspects that have been used to map against the initialization process as is shown in Table 2. Based on this, in the context of the scenario, the forensic tool would need to be aligned with the incident detection process as a functional requirement, quality requirement, constraint, pattern, and strategy in order to accelerate the digital investigation process.

Table 1
Mapping ISO/IEC 27043 readiness processes to the DFARS process.

Readiness processes	Functional requirements	Quality requirements	Constraints	patterns	Strategy
Scenario definitions	Stakeholders	X	Cost	X	X
Identification of PDE sources	X	X	X	X	X
Planning pre-incident detection	✓	X	X	X	X
Planning incident detection	✓	X	X	X	X
Storage and handling of PDE	X	X	X	X	Integrity
Defining system architecture	X	X	X	X	Confidentiality
Implementing system architecture	Use-cases	Core requirements	Legal	✓	✓
Implementing pre-incident detection	X	X	X	X	X

Table 2
Mapping ISO/IEC 27043 initialization processes to the DFARS process.

Initialization processes	Functional requirements	Quality requirements	Constraints	Patterns	Strategy
First responder	X	X	X	X	X
Incident detection	✓	✓	✓	✓	✓
Planning	X	X	X	X	X
Preparation	✓	X	X	X	X

Table 3
Mapping ISO/IEC 27043 acquisitive processes to the DFARS process.

Acquisitive processes	Functional requirements	Quality requirements	Constraints	Patterns	Strategy
PDE identification	X	X	X	X	X
PDE acquisition	✓	✓	✓	✓	✓
PDE transportation	✓	✓	✓	✓	✓
PDE storage	✓	✓	✓	✓	✓

Table 4
Mapping ISO/IEC 27043 investigative processes to the DFARS process.

Investigative processes	Functional requirements	Quality requirements	Constraints	Patterns	Strategy
PDE examination and analysis	✓	✓	✓	✓	✓
Digital evidence interpretation	✓	✓	✓	✓	✓
Preporting	✓	✓	✓	✓	✓
Presentation	✓	✓	✓	✓	✓
Investigation closure	✓	✓	✓	✓	✓

Table 5
Mapping ISO/IEC 27043 concurrent processes to the DFARS process.

Concurrent processes	Functional requirements	Quality requirements	Constraints	Patterns	Strategy
Obtain authorization	X	X	✓	X	X
Managing information flow	X	X	✓	X	X
Preserving chain of custody	X	X	✓	X	X
Preserving digital evidence	X	X	✓	X	X
Interaction with the physical investigation	X	X	✓	X	X

3.3. Mapping acquisitive process to DFARS

The principles of ISO/IEC 27043 have highlighted the manner in which digital evidence can be acquired in what is the acquisitive process. As far as the scenario is concerned, the acquisitive process would require all the aspects of the DFARS process during mapping. For example, it would require PDE acquisition, PDE transportation, and PDE storage while identification is not a required process as is shown in Table 3. It is the authors' opinion that PDE identification in this context is not required during this mapping, owing to the fact that incident detection (in the Initialization process) already preceded identification.

3.4. Mapping investigative process to DFARS

This is a crucial process for any investigative scenario, where a digital forensic tool may be required to accomplish some tasks effectively, with the aim of extracting objective data that may help in possible hypotheses formation [22]. The ISO/IEC 27043 investigative processes analyze the identified potential digital evidence to uncover the sequence of events. The investigative process includes the following sub-processes: Potential digital evidence examination and analysis, Digital evidence interpretation, Reporting, Presentation, and Investigation closure. While the authors envisage the improvement of the investigative process based on the requirements that are needed for tool development, it is also important to highlight that proper requirements may lead to more acceptable investigative results. However, with the ISO/IEC 27043 guidelines, providing proof of correctness for a digital forensic tool, this needs to be backed up with standardized approaches for purposes of litigation. That notwithstanding, while the investigative process from a generic view is more concerned with search, collection, preserving, and presentation of evidence, our mapping that is shown in Table 4 considers the inclusivity of all the aspects of the DFARS process. Notably, from the scenario it would be important after capturing the attackers information to examine, interpret, report in a standardized approach [23,24] and present this, as it would be an important determining factor on the legality of digital evidence.

3.5. Mapping concurrent processes to DFARS

The concurrent processes are the activities that occur in parallel to any digital forensic investigation, like getting court authorization to seize a device suspected to contain potential digital evidence required for a case under investigation. These principles are applied from the commencement of an investigation until closure. This is basically a core aspect of the DFARS process because all the constraints need to be taken account of as they may assist during the whole investigative process. ISO/IEC 27043 has identified the following processes in the concurrent processes: Obtaining authorization, Documentation, Managing information flow, Preserving chain of custody as is shown in Table 5. Consequently, based on the scenario, it would be imperative to focus on how the constraints in Table 5 affect the investigation process.

4. Discussions

The success of developing secure digital forensic tools has mainly been reinforced by the possibility of being able to extract forensically sound potential digital evidence. This could either be tamper-free logs or general artifacts that can provide proof of the occurrence a security incident or can assist forensic experts during litigation in a court of law. Consequently, the ISO/IEC 27043 standard is an acceptable process for investigations in the field of digital forensics. By applying the ISO/IEC 27043 processes when designing any digital forensic application while mapping to accepted standards harnesses the benefits that accrue in employing scientific methods in any new field of research like digital forensics. The authors revisit the scenario that addressed a successful hack as a result of software failure (see Section 3). The scenario application is entirely based on how the digital evidence scheme can be managed by the use of digital forensic tools. The ultimate aim is to ensure that the extracted artifacts are admissible in a court of law and are devoid of any security violations (Confidentiality and Integrity) when verifying their authenticity. To support this claim, this proposition that has been put across in this paper leverages the ISO/

IEC 27043 processes that basically have generic idealized guidelines for digital forensic investigations.

Our approach is entirely dependent on three main aspects: Using Requirements Specification Process, leveraging ISO/IEC 27043, and relying on effective process communication (see Figs. 3 and 4). All these aspects are meant to openly collude in order for the objective of designing secure digital forensic tools to be achieved with a higher degree of certainty.

By focusing on the SSN hack scenario, the authors give an analysis of how such an occurrence could be overcome if the tools are securely built using the idealized guidelines as is shown next.

- *This attack succeeded because a potential software failure/bug for X was manipulated in such a manner that the administrators were not able to detector monitor any transactions*: Basically, attackers could have capitalized on failure of different aspects like STRIDE or simply failure of the CIA security goals. In many situations, this could also be treated as an insider attack until a digital forensic investigation is conducted, this means that the forensic logs could either be with the provider or from some remote server. Usually, a subpoena will be required to warrant the provider to release such logs. An investigator would need to prove whether these logs are exactly authentic logs during verification. It may also be possible for an investigator to tamper with these logs, which may require a watcher to watch the watcher. In relying on standardized processes, the provider's location would be mapped to the scenario definition and a potential incident would explicitly be extracted in this environment. When using forensic tools one may easily need to execute these processes spontaneously while building a hypothesis.
- *All the SSN-based transactions were supposed to be logged periodically on an interval of 1 min, however, this did not happen as a result of this compromise*: Given than transactions involving SSNs are critical, the lack of periodic logging is an indication that a potential failure could have been detected There exist a number of possibilities that could have been used by X during forensic investigations. A digital forensic investigator may need to prove how the provision of false evidence could be overcome using forensic tools, where this could require forensic tools that are aligned to ISO standards.
- *This led to the creation of fake tax returns and falsification of identities that targeted fraudulent claims*: The ISO/IEC 27043 has defined modes of defining investigation scenarios, digital evidence sources, and planning pre-incident detection. Based on this premise, it is imperative that all false identities should be detected and should flagged as suspicious early enough in a forensic readiness approach [25–29] as potential threats by the forensic tools. In the scenario, the aspect of lack of periodic logging could have been flagged to avert the possibility of far much larger compromise than was reported.

Nevertheless, the DFARS process estimates the DF application production time, defines the maintainability options, shows the integrity and forensic soundness of the DF application and ensures that the processes utilized in the DF applications design adhere to accepted standards through different processes, which would include standardizing different stages like reporting [23] and presentation. Additionally, the DFARS process is focused on describing how a digital forensic tool works. This is done with respect to the understanding of the design and development process, together with the technical and non-technical audiences, who are involved in the use of digital forensic outputs in the investigation where such evidence is brought under scrutiny. In aligning the DFARS process to the ISO/IEC 27043 standard, this paper identifies the aspects of the DFARS process that require enhancing and addresses them to work in conjunction with the ISO/IEC 27043 digital forensic investigation process.

ISO/IEC 27043 as a family of standards offers incident investigative principles and processes that are concerned with planning and preparation of potential evidence identification. It is based on this premise that the proposed approach tries to map DFARS to the ISO/IEC 27043 international standard, which is beneficial to the forensic community in many ways and the advantages of these are listed as follows:

- Mapping tool creation strategies with standardized processes offers a baseline for developing secure digital forensic tools that can be relied upon by forensic experts during digital forensic investigation.
- Based on the requirements of digital evidence, for example, the Expert Witness testimony [30,31], where an expert may be required to give a testimony for evidence to be admitted, standardized approaches may be needed in order to increase chances of admissibility during litigation.
- By applying mapping approach, the aspect of usability on digital evidence that may be collected as a result is enhanced given that the tool development processes are aligned to standardised approaches.
- ISO/IEC 27043 and DFARS provides a consensus on how to securely identify and collect potential evidence, judging from the processes irrespective of the environment that digital evidence is collected from.
- Currently, there exist quite a number of tools that are focused in conducting different types of investigations, i.e. mobile forensics, cloud forensics, network forensics etc. Most of these types of investigations have a variety of investigation tools too for example, FTKs, EnCase etc. Choosing a suitable tool sometime may be a challenge owing to lack of standardised approaches while developing some of these tools. The proposed approach would, during evidence presentation provide a more trusted approach with a degree of acceptability.

Given that a majority of digital forensics tools are mainly developed for commercial purposes, it would be important if the development strategies can be aligned to the standardised approaches in order to increase chances of admissibility. This is also beneficial to the investigators and the Law Enforcement Agencies (LEAs) because adopting some of the aforementioned processes would improve the time that an investigator takes to conduct an investigation given that more acceptable processes are automated and may thus save the difficult tasks that may require human interpretation and intelligence [32–35]. This is owing to the fact that there is a constant need of developing and adopting e objective of digital forensic investigation and at the same time advance the field of digital forensics in various domains [36,37]. It is also worth to note that ISO/IEC 27043 has potential of being mapped to forensic application as long as some preconditions are met like the technical requirements and different cases, for example, where the LEAs, investigative agencies are able to give a baseline for tool validation techniques and requirements [38]. This has been compounded as strategies that can allows alignment of forensic tools to standardised processes given that digital forensics relies on prescribed scientific processes.

5. Conclusion

This paper has reinforced the importance of developing digital forensic applications using a process that is based on standardized guidelines, and in our context ISO/IEC 27043. Future research includes using the proposed approach to facilitate the design of some real-world digital forensic application (e.g., an open source mobile forensic toolkit) in order to evaluate its utility.

Declaration of Competing Interest

The authors report no declarations of interest.

References

[1] S. Garfinkel, P. Farrell, V. Roussev, G. Dinolt, Bringing science to digital forensics with standardized forensic corpora, Digit. Invest. 6 (2009) S2.

[2] N. Karie, V. Kebande, H. Venter, A generic frame work for digital evidence traceability, European Conference on Cyber Warfare and Security, Academic Conferences International Limited, 2016, pp. 361.
[3] A.R. Ikuesan, H.S. Venter, Digital behavioral-fingerprint for user attribution in digital forensics: are we there yet? Digit. Invest. 30 (2019) 73.
[4] S.A. Omeleze, Digital Forensic Evidence Acquisition to Mitigate Neighbourhood Crime, (2017) .
[5] S. Omeleze, H.S. Venter, Digital forensic application requirements specification process, Aust. J. Forens. Sci. 51 (2019) 371.
[6] S. Omeleze, H. Venter, Architectural requirements specifications for designing digital forensic applications, European Conference on Cyber Warfare and Security, Academic Conferences International Limited, 2016, pp. 405.
[7] F. Solms, What is software architecture? Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference (2012) 363–373.
[8] L. Bass, P. Clements, R. Kazman, Software Architecture in Practice, Addison-Wesley Professional, 2003.
[9] D. Garlan, M. Shaw, An introduction to software architecture, Advances in Software Engineering and Knowledge Engineering, World Scientific, 1993, pp. 1–39.
[10] ISO/IEC, 27043: 2015 International Standard, Information Technology—Security Techniques—Incident Investigation Principles and Processes, ISO.org 1, 2015, pp. 1.
[11] N.H. Ab Rahman, W.B. Glisson, Y. Yang, K.-K.R. Choo, Forensic-by-design framework for cyber-physical cloud systems, IEEE Cloud Comput. 3 (2016) 50.
[12] N.H. Ab Rahman, N.D.W. Cahyani, K.-K.R. Choo, Cloud incident handling and forensic-by-design: cloud storage as a case study, Concurr. Comput.: Pract. Exp. 29 (2017) e3868.
[13] A. Valjarevic, H.S. Venter, Harmonised digital forensic investigation process model, 2012 Information Security for South Africa, IEEE, 2012, pp. 1–10.
[14] S. Omeleze, H.S. Venter, Testing the harmonised digital forensic investigation process model-using an android mobile phone, 2013 Information Security for South Africa, IEEE, 2013, pp. 1–8.
[15] V.R. Kebande, H.S. Venter, On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges, Aust. J. Forens. Sci. 50 (2018) 209.
[16] A. Valjarević, H. Venter, R. Petrović, ISO/IEC 27043: 2015—role and application, 2016 24th Telecommunications Forum (TELFOR), IEEE, 2016, pp. 1–4.
[17] M.M. Pollitt, An ad hoc review of digital forensic models, Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07), IEEE, 2007, pp. 43–54.
[18] V.R. Kebande, H. Venter, Requirements for achieving digital forensic readiness in the cloud environment using an NMB solution, 11th International Conference on Cyber Warfare and Security: ICCWS (2016) 399.
[19] Y. Gao, G.G. Richard III, V. Roussev, Bluepipe: a scalable architecture for on-the-spot digital forensics, Int. J. Digit. Evid. 3 (2004) .
[20] V. Kebande, H. Venter, A functional architecture for cloud forensic readiness large-scale potential digital evidence analysis, European Conference on Cyber Warfare and Security, Academic Conferences International Limited, 2015, pp. 373.
[21] V.R. Kebande, H.S. Venter, Novel digital forensic readiness technique in the cloud environment, Aust. J. Forens. Sci. 50 (2018) 552.
[22] S. Costantini, G. De Gasperis, R. Olivieri, Digital forensics and investigations meet artificial intelligence, Ann. Math. Artif. Intell. 86 (2019) 193.
[23] N.M. Karie, V.R. Kebande, H. Venter, K.-K.R. Choo, On the importance of standardising the process of generating digital forensic reports, Forens. Sci. Int.: Rep. 1 (2019) 100008.
[24] A. Al-Dhaqm, S. Abd Razak, D.A. Dampier, K.-K.R. Choo, K. Siddique, R.A. Ikuesan, A. Alqarni, V.R. Kebande, Categorization and organization of database forensic investigation processes, IEEE Access 8 (2020) 112846.
[25] A.R. Ikuesan, H.S. Venter, Digital forensic readiness framework based on behavioral-biometrics for user attribution, 2017 IEEE Conference on Application, Information and Network Security (AINS), IEEE, 2017, pp. 54–59.
[26] A. Singh, A.R. Ikuesan, H.S. Venter, Digital forensic readiness framework for ransomware investigation, International Conference on Digital Forensics and Cyber Crime, Springer, 2018, pp. 91–105.
[27] H. Munkhondya, A. Ikuesan, H. Venter, Digital forensic readiness approach for potential evidence preservation in software-defined networks, ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019, vol. 268, Academic Conferences and Publishing Limited, 2019.
[28] J. Tan, Forensic Readiness, @ Stake, Cambridge, MA, 2001, pp. 1.
[29] V. Kebande, H.S. Ntsamo, H. Venter, Towards a prototype for achieving digital forensic readiness in the cloud using a distributed NMB solution, European Conference on Cyber Warfare and Security, Academic Conferences International Limited, 2016, pp. 369.
[30] M.G. Farrell, Daubert v. Merrell Dow Pharmaceuticals, Inc.: Epistemology and legal process, Cardozo L. Rev. 15 (1993) 2183.
[31] A. Abboud, Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993), Embryo Project Encyclopedia, (2017) .
[32] I. Richard, V. Roussev, Digital forensic tools: the next generation, Digital Crime and Forensic Science in Cyberspace, IGI Global, 2006, pp. 75–90.
[33] N.M. Karie, V.R. Kebande, H. Venter, Diverging deep learning cognitive computing techniques into cyber forensics, Forens. Sci. Int.: Synergy 1 (2019) 61.
[34] I.R. Adeyemi, S. Abd Razak, M. Salleh, H.S. Ven ter, Leveraging Human Thinking Style for User Attribution in Digital Forensic Process, (2017) .
[35] D. Ernsberger, R.A. Ikuesan, S.H. Venter, A. Zugenmaier, A web-based mouse dynamics visualization tool for user attribution in digital forensic readiness, International Conference on Digital Forensics and Cyber Crime, Springer, 2017, pp. 64–79.
[36] D.P.J. Taylor, H. Mwiki, A. Dehghantanha, A. Akibini, K.K.R. Choo, M. Hammoudeh, R. Parizi, Forensic investigation of cross platform massively multiplayer online games: Minecraft as a case study, Science Justice 59 (2019) 337.
[37] Y.-Y. Teing, S. Homayoun, A. Dehghantanha, K.-K.R. Choo, R.M. Parizi, M. Hammoudeh, G. Epiphaniou, Private cloud storage forensics: Seafile as a case study, Handbook of Big Data and IoT Security, Springer International Publishing, 2019, pp. 73–127.
[38] A.M. Marshall, R. Paige, Requirements in digital forensics method definition: observations from a UK study, Digit. Invest. 27 (2018) 23.