Forensic Science International: Reports 1 (2019) 100008

Contents lists available at ScienceDirect

Forensic Science International: Reports

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

On the importance of standardising the process of generating digital forensic reports

Nickson. M. Karie [a], Victor R. Kebande [b,*], H.S. Venter [c], Kim-Kwang Raymond Choo [d]

[a] Department of Computer Science, University of Swaziland, Kwaluseni, Swaziland
[b] IoTaP Research Center, Department of Computer Science and Media Technology, Malmo University, Nordenskiöldsgatan 1, 211 19 Malmö, Sweden
[c] Department of Computer Science, University of Pretoria, Private Bag X20, Hatfield, 0028 Pretoria, South Africa
[d] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA

ARTICLE INFO

Keywords:
Standardisation
Digital forensic report generation
digital forensics
ISO/IEC 27043:2015
Blockchain

ABSTRACT

The ISO/IEC 27043:2015 international standard provides new standardised guidelines for common investigation processes across various investigation scenarios that mostly involve digital evidence. The reporting process is one of the many investigative processes described in the ISO/IEC 27043:2015 standard, but the manner in which the reporting process is presented does not constitute or cover the specificity of the presentation of the entire processes covered in the standard. In this paper, we posit the importance of having the report generation process covering details obtained from all other classes of the digital investigation processes in a standardised format, as well as the need to standardise the process of generating digital forensic reports. Such a standardised process can facilitate future automation and text analytics, sharing of reports and knowledge across jurisdictions, etc. We also identify a number of key factors, such as the use of Blockchain, which should be added to the ISO/IEC 27043 international standard in order to support a standardised digital forensic report generation process.

1. Introduction

Once a (suspected) security incident is detected, there is generally a need to conduct further investigation, which may lead to the acquisition, analysis and interpretation of evidence. Such analysis may then further inform the interpretation and attribution, and the findings are likely to be eventually presented in the form of expert reports, depositions, and testimonies in any legal or civil proceedings [1–3]. Unlike most cyber security incident investigations, a digital forensic investigation needs to ensure the validity, reliability and soundness of the evidence, and that the processes (including tools and techniques used in the acquisition and analysis of evidence) and findings are properly documented in the forensic report, in order to be admissible in a court of law [4–6].

There is, however, a lack of standardised procedures to facilitate forensic investigators, particularly those in regional law enforcement units, in generating quality forensic reports for use in the court of law during legal proceedings. This, therefore, results in disparities on how forensic reports are prepared or generated and presented to different stakeholders after an investigation process has been conducted. Hence, there is a need to develop and have in-place standardised procedures and specifications for preparing forensic reports, while taking into consideration the wide range of processes defined in existing investigation models and standards [7], such as the ISO/ISEC27043:2015 international standard.

In this paper, we highlight the need for standardising the process used in the preparation and generation of digital forensic reports, as we argue that this is a crucial step towards producing high quality forensic reports, which can encourage digital forensic best practices, facilitate sharing and admissibility of reports across jurisdictions, etc. We also hope that the issues raised in paper will also lead to further discussions and research on this topic, such as what are the internationally agreed procedures for the preparing and generating of high quality forensic reports that can be admitted in different jurisdictions.

The rest of this paper is organised as follows: Section 2 briefly introduces relevant background concepts, while Section 3 discusses the need for standardisation and what it potentially involves. In the last section, we conclude the paper.

2. Brief background

In this section, we will briefly introduce the reader to digital forensics and the ISO/IEC 27043:2015 International Standard and the Reporting process within the standard [8].

* Corresponding author.
E-mail addresses: nkarie@uniswa.sz (N. M. Karie), vitor.kebande@mau.se (V.R. Kebande), hventer@cs.up.ac.za (H.S. Venter), raymond.choo@fulbrightmail.org (K.-K.R. Choo).

http://doi.org/10.1016/j.fsir.2019.100008
Received 7 April 2019; Received in revised form 28 May 2019; Accepted 10 June 2019
Available online 28 June 2019

2.1. Digital forensics

In 2001, the report from the first Digital Forensic Research Workshop (DFRWS) held in Utica, New York defined digital forensics as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations" [9]. However, evidence required from digital forensics can be used in the courtroom, as well as civil proceedings [10].

In recent years, there have been attempts to integrate artificial intelligence (including machine learning and deep learning approaches) in digital forensic investigations [11]. Also, given the fast-pace nature of technological advances where the evidential source is no longer restricted to the conventional personal computers and servers (e.g. mobile device and apps, unmanned vehicles, and smart home devices – see [12–15], it can be challenging for digital forensic investigators and the court to keep abreast of the digital forensic landscape [15].

This necessitates the importance of forensic soundness and adequately documenting the entire digital forensic investigation process in a forensic report, to minimise the risk of evidence not been admissible in a court of law. Thus, standardised procedures need to be developed in digital forensic investigation to address the challenges and disparities associated with the preparing and generating of forensic reports for use in any court of law or legal proceedings.

In the next section, we will briefly explain ISO/IEC 27043: 2015.

2.2. ISO/IEC 27043:2015 International standard

ISO/IEC 27043 is an international standard published in 2015, which broadly covers information technology, security techniques, and incident investigation principles and processes (ISO/IEC 27043:2015). The standard describes part of a comprehensive investigative process and should be used in conjunction with other existing International Standards such as ISO/IEC 27035, ISO/IEC 27037, ISO/IEC 27042 and ISO/IEC 27041.

The primary objective for developing the ISO/IEC 27043 standard is to define and follow some standardised investigation principle and processes, to achieve the same results for different investigators under similar conditions. Such reproducibility and repeatability principles are crucial to any forensic investigation process. The ISO/IEC 27043 standard is also designed to provide clarity and transparency in the obtained results for each particular process throughout the investigation process (including report generating).

However, as discussed earlier, the manner in which the report generation process is presented is not sufficiently comprehensive and does not adequately cover the entire processes defined in ISO/IEC 27043:2015. Based on the description presented in this standard, the digital investigation processes are multi-tiered. This implies that, each process contains a set of sub-processes, which can be fully defined for a specific type of incident and investigation. Besides, legislative rules can influence the definition of these sub-processes, and this is beyond the scope of this paper.

According to the standard, more relevant digital evidence should be listed first in the report, followed by the less relevant evidence. The standard also adds that, results from the evidence interpretation process are to be compiled and written up that is in a form that can be printed on paper. However, as explained by Cahyani et al. [5] and Cahyani et al. [6], there are other visual representation approaches (e.g. multimedia) that should be considered in the presentation of the evidence, particularly those that involve complex, highly technical terminologies.

The ISO/IEC 27043 international standard also goes further to state that, the forensic report should be written in simple language and should be clear, concise and unambiguous. It should, also be readable by a wide audience including, but not limited to, a judge, jury, accused, lawyers, prosecutors, company management team, shareholders and employees. Reporting has also been adopted in different environments, such as Internet of Things (IoT) [16].

Therefore, one might ask at this point is: "How do we design a guideline or procedure to help the digital forensic investigators to generate a standardised report that includes results from all relevant processes outlined in the ISO/IEC 27043 international standard, as well as other standards related to the investigation?". This paper thus addresses the need to have standardised procedures to guide investigators in forensic report generation in a more acceptable way.

3. The need for standardising forensic report process

In ISO/IEC 27043, report generation is a process that is focused on the interpretation of digital evidence. Generally, the presentation phase in a digital forensic investigation helps to validate the forensic hypothesis, while in the context of the ISO/IEC 27043, report generation as a process is encapsulated inside the investigative process which is one of the classes of digital investigation processes [17,18]. While report generation does not constitute a process that conducts investigation, it has rather been presented as a process that shows or interprets the findings [19].

We argue that forensic reports should be prepared or generated as a standardised process, without being encapsulated in one of the classes of digital investigation (investigative process class). Note that, the generation, presentation and interpretation of forensic reports in many instances if not carefully handled may lead to misinterpretations of the forensic hypothesis or the investigation facts. This is a key limitation in the standard.

We will now describe our conceptual sub-processes to be considered as part of the report generation phase in the ISO/IEC 27043:2015 international standard.

3.1. Scope of digital forensic investigation

It is important to note that when a forensic report is being prepared or generated, it should cover the scope of digital forensic investigation process in its entirety. At this point, information contained in digital forensic investigation cannot be extracted without following prescribed processes; it needs to be explicitly highlighted because the relevance of the digital forensic investigation process is important. This allows the transparent reporting of investigation to relevant stakeholders. One could also explore the potential of using Blockchain to ensure the integrity of the evidence included in the report [20].

3.2. Technologies (tools and techniques) and methodologies used

To ensure forensic soundness, it is important to document the tools and techniques used while conducting the investigation, particularly tools and techniques that have not been trialled-and-tested. If relevant, one may also wish to include the make, model and version number of the tools and techniques used, as well as any known limitations of the tools and techniques at the time of using the tools and techniques.

It is also imperative that the methodology employed during a digital investigation process is documented in the report generation phase. This allows relevant stakeholders to understand how the investigating team arrives at some given decision or conclusion.

3.3. Qualification

Interpreting the contents of what a digital investigation process is intended to achieve requires relevant competence and expertise, for example based on up-to-date trainings. Based on this, the expected findings should be professionally interpreted in a forensic report, such that qualified experts (not part of the investigation team) are able to verify and confirm the findings. This means that a forensic report needs to

always be handled by qualified experts before and during presentation. The implications of not having qualified experts can be detrimental to the investigation outcomes, as noted by Butler and Choo [21].

3.4. Data inclusion and exclusion criteria

While forensic data collection plays a pivotal role in the digital forensic investigation process, not all data acquired and analysed need to include in the report. Therefore, there needs to be clearly defined inclusion and exclusion criteria for the content of the final report. In addition, depending on the specific investigation, data that is not included in the final report may need to be securely stored. Hence, the report may also need to include a persistent storage location and duration for data that is not included in the final report but is still available for the pre-determined duration (e.g. three years after the conclusion of the case).

3.5. Limitations, if any

No digital forensic investigation is perfect. Therefore, any decisions to omit certain steps, processes, and investigative actions should be documented, as well as any known limitations in the tools and techniques used (also discussed in Section 3.2).

4. Conclusion and future work

In this paper, we highlighted the need for standardising the report generation process, with the aim of improving the manner in which forensic evidence is presented during and after litigation, while aligning with the ISO/IEC 27043:2015 standard. Future research includes identifying the key components of such a standardised report generation process, for example in consultation with the international digital forensic community, as well as exploring how contemporary technologies, such as virtual reality, Blockchain and machine learning, can be utilised to facilitate the report generation process.

Declaration of Competing Interests

The authors declare no competing interests.

Appendix A. Supplementary data

Supplementary material related to this article can be found, in the online version, at doi:10.1016/j.fsir.2019.100008.

References

[1] N.M. Karie, H.S. Venter, Towards a framework for enhancing potential digital evidence presentation, Proceedings of the Information Security for South Africa, 2013, Johannesburg, South Africa, 2013.
[2] D. Quick, K.-K.R. Choo, Big Digital Forensic Data – Volume 1: Data Reduction Framework and Selective Imaging. SpringerBriefs on Cyber Security Systems and Networks, Springer, 2018, pp. 1–96 ISBN 978-981-10-7762-3.
[3] D. Quick, K.-K.R. Choo, Big Digital Forensic Data – Volume 2: Quick Analysis for Evidence and Intelligence. SpringerBriefs on Cyber Security Systems and Networks, Springer, 2018, pp. 1–86 ISBN 978-981-13-0262-6.
[4] N.M. Karie, H.S. Venter, A generic framework for enhancing the quality of digital evidence reports, Proceedings of the European Conference on Cyber Warfare and Security ECCWS-2014, Piraeus, Greece, 2014.
[5] N.D.W. Cahyani, B. Martini, K.-K.R. Choo, H. Ashman, An approach to enhance understanding of digital forensics technical terms in the presentation phase of a digital investigation using multimedia presentations, (SecureComm (2) (2018) 488–506.
[6] N.D.W. Cahyani, B. Martini, K.-K.R. Choo, Using Multimedia Presentations to Enhance the Judiciary's Technical Understanding of Digital Forensic Concepts: An Indonesian Case Study. HICSS, (2016) , pp. 5617–5626.
[7] N.H. Ab Rahman, K.-K. R. Choo, A survey of information security incident handling in the cloud, (Comput. Secur. 49 (2015) 45–69.
[8] ISO/IEC 27043:2015 Information technology – Security techniques – Incident investigation principles and processes.
[9] P. Gary, "A Road Map for Digital Forensic Research"; Technical Report DTR-T001-01, DFRWS, November 2001. Report from the First Digital Forensic Research Workshop (DFRWS), (2001) Available from: http://www.dfrws.org/2001/dfrws-rm-final.pdf [Accessed 26.03.19].
[10] V.R. Kebande, N.M. Karie, H.S. Venter, Cloud-centric framework for isolating big data as forensic evidence from IoT infrastructures, Proceedings of, the Next Generation Computing Applications 2017 conference (NextComp2017), July 19–21, Mauritius, 2017.
[11] N.M. Karie, V.R. Kebande, H.S. Venter, Diverging deep learning cognitive computing techniques into cyber forensics, (Forensic Sci. Int. Synergy 1 (2019) 61–67.
[12] N.-A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens, Choo D K.-K.R., Smart vehicle forensics: challenges and case study, (Future Gen. Comput. Syst. (2019) , doi:http://dx.doi.org/10.1016/j.future.2018.05.081 (in press).
[13] S. Li, K.-K.R. Choo, Q. Sun, W.J. Buchanan, J. Cao, IoT forensics: Amazon echo as a use case, (IEEE Internet Things J. (2019) , doi:http://dx.doi.org/10.1109/JIOT.2019.2906946 (in press).
[14] D.C. Paul, J. Taylor, H. Mwiki, A. Dehghantanha, A. Akibini, R. Parizi, K.-K.R. Choo, Forensic investigation of cross platform massively multiplayer online games: minecraft as a case study, (Sci. Justice 59 (May (3)) (2019) 337–348.
[15] X. Zhang, K.-K.R. Choo, N.L. Beebe, How do I share my IoT forensic experience with the broader community? An automated knowledge sharing IoT forensic platform, (IEEE Internet Things J. (2019) , doi:http://dx.doi.org/10.1109/JIOT.2019.2912118 (in press).
[16] V.R. Kebande, I. Ray, A generic digital forensic investigation framework for internet of things (iot), 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, (August), 2016, pp. 356–362.
[17] V.R. Kebande, H.S. Venter, Novel digital forensic readiness technique in the cloud environment, (Aust. J. Forensic Sci. 50 (5) (2018) 552–591.
[18] V.R. Kebande, H.S. Venter, Adding event reconstruction to a Cloud Forensic Readiness model, 2015 Information Security for South Africa (ISSA), IEEE, August, 2015, pp. 1–9.
[19] V. Kebande, H.S. Ntsamo, H.S. 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.
[20] E. Nyaletey, R.M. Parizi, Q. Zhang, K.-K.R. Choo, BlockIPFS – blockchain-enabled interplanetary file system for forensic and trusted data traceability, Proceedings of 2019 IEEE Conference on Blockchain, 14–17 July, 2019.
[21] A. Butler, K.K.R. Choo, IT standards and guides do not adequately prepare IT practitioners to appear as expert witnesses: an Australian perspective, (Secur. J. 29 (2) (2016) 306–325.