Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 179 (2021) 966–973

Procedia Computer Science

www.elsevier.com/locate/procedia

5th International Conference on Computer Science and Computational Intelligence 2020

An Exploratory Study on Readiness Framework in IoT Forensics

Nurul Huda Nik Zulkipli[a,b,*], Gary B.Wills[b]

[a]*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Melaka,77300 Merlimau, Melaka, Malaysia*

[b]*School of Electronics and Computer Science, University of Southampton, SO17 1BJ, Southampton,United Kingdom*

Abstract

Forensic readiness is important to ensure that the organization is fully prepared and well-equipped to be forensically ready to conduct the digital forensic investigation. Moreover, forensic readiness in IoT forensic investigation is different from the usual computer forensic readiness. This research discovered the importance of having the forensic readiness in place for the organization before conducting the IoT forensic investigation. Therefore, a readiness framework was proposed as a groundwork before further research is carried out. Literature on related this issues was collected, examined and criticized in order to scrutinize the impact factors in IoT forensics investigations. Finally, the proposed framework was validated by thirty experts from digital forensics in Malaysia using triangulation methods. From the results, this framework will be used in developing an instruments to measure readiness factors among digital forensics stakeholders.

Keywords: IoT forensic; Forensic Readiness; Triangulation Method

1. Introduction

The issues of IoT forensics are much more complicated due to the various inter-connectivity among heterogeneous IoT devices. Besides, a petabyte amount of data could be exchanged between IoT devices which makes the investigation process more difficult and it may lead to being mistakenly interpreted [1]. Therefore, the forensic readiness is required to ensure the stakeholder are well prepared operationally and infra-structurally [2] to fully support the IoT incident investigation.

* Corresponding author.

E-mail address: nurulhuda8450@uitm.edu.my

10.1016/j.procs.2021.01.086

Previous research shows that the forensic readiness is defined into two perspectives. Firstly, in 2011, The National Archives; Digital *Continuity to Support Forensic Readiness* has defined as "The *achievement of an appropriate level of capability by an organization in order for it to be able to collect, preserve, protect and analyze digital evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or court of law".* Later point of view has defined forensic readiness as the ability of the organization to minimize the cost of investigation and maximizing its potential to use of digital evidences [3]. Both definitions are focusing on the organization itself in order to optimize its resources, human powers and strategic planning to support the digital forensic investigation process.

The main objective of this research is to study the importance of digital forensic readiness for the organization especially in IoT forensic perspectives. After that, the impact factors on readiness which affected in IoT forensic investigation was listed and explained. Finally, a readiness framework is proposed and validated by the experts in the field. Next section will describe more on the importance of forensic readiness and readiness factors affected.

2. Research Background

Digital forensic investigation process can be categorized into three main phase: (1) Pre-investigation phase, (2) Investigation Phase and (3) Post-investigation phase. In this research, the pre-investigation phase is emphasized. According to the pre-investigation phase, there are three processes involved; Preparation, Acquisition and Evaluation. From these processes, one of the potential issues recommended by experts for further investigation is on Forensic Readiness – which can be used to prepare the IoT environment for digital forensic investigation and prepare the investigator for IoT incidents.

2.1. The Importance of Forensics Readiness

Forensic readiness is important to ensure that the organization is fully prepared and well equipped to be forensically ready to conduct digital forensic investigation. Moreover, forensic readiness in IoT is different from usual computer forensic readiness. The complexity involved in IoT systems and lack of unified standards impedes the digital investigation process and at some point, prevents the security agencies and the Law Enforcement Agencies (LEA) from acquiring digital forensic evidence forensically [4].

Forensic readiness helps an organization streamline its activities to make it easy with reduced hassles to retrieve digital evidence. That is, digital evidence is properly recorded and stored even before an incident occurs, without operations being interrupted [3] Getting a forensic preparation plan in place means that it is readily available and in an acceptable form in the event that electronic evidence is needed. It needs staff training and proper procedures to ensure compliance. To maximize organization's potential to use digital evidence, [5] has listed seven scenarios that would involve digital evidence as below:

(i) Disputed transactions

(ii) Allegations of employee misconduct

(iii) Showing legal and regulatory compliance

(iv) Avoidance of negligence and breach-of contract charges

(v) Assisting law enforcement investigations

(vi) Meeting disclosure requirements in civil claims

(vii) Supporting insurance claims when a loss occurs

Apart from that, forensic preparation planning complements other operational strategies and procedures,

including recovery from emergencies, business continuity, and policies for record preservation [5]. It is also a part of a quality information risk management approach. [3] also recommends that a forensic preparation program would be better for organizations with a good risk management and information security system. From [5], the advantages of preparing the forensic readiness can be summarized as follows:

- Forensic readiness can help in preparing for the future need for digital evidence
- Reducing the cost of investigation
- Preventing the potential malicious insiders to cover their tracks.
- Due diligence, good corporate governance and compliance with regulations.
- Reduce the cost of administrative and statutory information disclosure requirements.

After analyzing the importance of forensic readiness from literature, the study continues by investigating the readiness factors affected in the organization.

3. Synthesizing the Readiness Factors

A readiness process is also known as a process which deals with the pre-investigation processes. The concept of forensic readiness was introduced by [10] where the main objectives are to utilise the organisation's ability to collect potential digital evidence while limiting the cost of an investigation. The factors were used to determine the requirements in order for the organization to become forensically ready. Based on the concept introduced, further researches regarding forensic readiness has been evolved by considering many readiness factors including resourcing [7], [8], organization role [3][9], [10], technology used [2], [11] and policy [10]. Table 1 show the summarized twelve readiness factors that have been discussed by previous researches.

After reviewing and analysing the readiness factors from literature, there are several factors that can be put under the same theme. Therefore, the researcher decided to group the readiness factors into six groups thematically as the following: Capability (Cap), Resources (Res), Operability (Op), Strategic Planning (SP), Knowledge (Kn) and Awareness (Aw) on IoT. Due to the complexity of the IoT environment, the factors in forensic readiness can be used as a guideline for the organization to ensure flexibility with the investigation since various types of digital investigation is possible to involve such computer forensic, mobile forensic, network forensic and live forensic [12]. The description for each of the six factors is presented in the following subsections.

3.1.1. Capability (Cap)

The forensic capabilities comprise the ability of the organizations to conduct forensics cases which emphasize the top management responsibilities and staff involvement to support the whole investigation process. As stated in [7] and [14], this factor is required in forensic readiness plan and they vary depending upon the size of the organization whether that capability can be provided internally or externally. For example, organization may hire new staff, training existing staff or contract a specialist third party provider to carry out the forensic tasks [13],[14].

A strategic model for forensic readiness was introduced by [15] known as the HAUS model where it is an: Homogeneous, Answerable, Unified Strategy. The model is driven by the management which emphasize on the importance of staff involvement in the organizations. All the staff (technical and non-technical) need to know their own responsibilities such as what to do, how to do it and who's responsible for what. Moreover, it is vital for an organisation to have the ability to process evidence cost-effectively [3]. In the context of IoT, it is important to have staff who are knowledgeable in IoT environment to ensure potential evidence is preserved.

3.1.2. Resources (Res)

In [8], resources allocation is not optional in forensic. It is important in supporting the investigations [14] and it can be divided into three components as recommended in [7]. Firstly, is the budget. Financial allocation is needed to support the investigation, for instance, to fund the procurement of the third-party specialist to undertake any part of investigations, to fund the training for the staff so they are accredited and licensed to run the investigation.

Second component is, providing adequate equipment. In forensic readiness, the organization must be able to provide the forensic equipment's in house or they can outsource to the third-party investigator. Dedicated forensic software and forensic appliances are used to help the investigator to do their job. By providing the equipment, it can enable the investigator to do the investigation such as write blockers for the digital evidence retrieval. The equipment is expensive and should be fully licensed. A financial allocation is required to continue the subscriptions and maintenance of the equipment.

Some of the forensic tools are freeware license and open sources license. However, these tools can only access the basic features. The final component is providing dedicated environment to facilitate the forensic tasks. For example, secure storage room for the evidence, Faraday's cage room and forensic tower which provide data duplication, parallel analysis, operating systems emulation and integration with some forensic analysis software.

3.1.3. Operability (Op)

Operability is another factor in forensic readiness to ensure the investigation process runs correctly as stated in the standard of procedure. According to [2], both of the operations and infrastructure are needed to fully support the investigation process. [11] also elaborated about the technical aspects involved during investigation such as time-stamping, system hardening and compromised kernel, logging process and evidence handling.

In the IoT context, a lot of operational techniques are required since the IoT ecosystem is much more complicated than normal computing system. With a gigantic amount of data generated from heterogeneous IoT devices makes the forensics tasks more difficult especially during identification, collection and preservation process. Any error at these stages will affect the whole investigation [23]. The real challenge is applying the standard digital forensic procedure in the IoT environment [1]. Consideration of each IoT dimension including its limitation and characteristic is necessary during the investigation to avoid misleading result. Plus, dealing with volatile data is very crucial where data may be stored locally in the device or in the cloud [24]. Having an alternative plan such as backup and redundancy plan for potential evidence is also important because the lifespan of the data cannot be guaranteed since it could potentially be overwritten and wiped remotely.

Diversity of IoT devices come with different data formats, protocols and physical interfaces [25]. Yet, there are no standards formats for IoT devices. There may be a lot of digital evidence trace acquired and presented in various format leading to an overhead in the examination and analysis process [1]. Since current forensic tools are not designed for IoT [26], the investigator must have a clear understanding of how IoT's works and multiple skills need to be employed during the investigation.

3.1.4. Strategic Planning (SP)

The strategic planning in this instrument comprised several factors like forensic policy, standard of procedures, legal requirements and training which had been discussed among readiness literature. [14] had mentioned that forensic strategy is unique to each organisation and it must be designed according to the organisation objectives. The decision to implement a digital forensic readiness program must be a strategic decision for the organization concerned [18].

For each organization, a forensics policy must clearly state the forensics functionality of a system. Besides listing the rules and regulation applied, the forensic policy must also specify what event must be handled and which data must be preserved [20]. Other than that, implementation of the standard of procedures in conducting the forensic

investigation is another important issue for the organization to be forensically ready. As mentioned in [27], the standard operating procedure (SOP) is the internal procedure designed to perform a complex routine with limited time and resources.

Table 1. List of the forensic readiness factor

	Capability			Resources		Strategic Planning				Operability		Knowledge	Awareness
Readiness Factors / References	Ownership	Responsibility	Manpower	Financial	Equipment	Technology	Awareness	Legal	Training	Infrastructure	Devices & Tools	Technology	Awareness
Digital Forensic Readiness as a Component of Information Security Best Practice [16]	/	/	/	/	/	/	/	/		/	/		
A Ten Step Process for Forensic Readiness [3]	/	/	/	/	/	/	/	/	/	/	/		/
Forensic readiness: Good Practice Guide [7]	/	/	/	/	/		/	/	/		/	/	/
Policies to Enhance Computer and Network Forensics [10]		/	/	/	/	/	/	/	/		/		
A Strategic Model for Forensic Readiness [15]			/	/	/	/			/		/		
Towards a systemic framework for digital forensic readiness [13]	/	/	/	/	/	/	/	/	/	/	/	/	/
Digital forensic readiness: Expert perspectives on a theoretical framework [14]	/	/	/	/	/	/	/	/	/	/	/	/	/
The architecture of a digital forensic readiness management system [17]			/	/	/	/	/		/		/		
Forensic readiness landscape [12]	/	/	/	/	/	/	/				/		
Developing an Enterprise Digital Investigative/ Electronic Discovery Capability [8]			/	/	/	/	/				/		
Getting Physical with the Digital Investigation Process [2]			/	/	/	/					/	/	/
A digital forensic readiness framework for South African SME's [18]			/	/	/	/	/			/	/	/	/
The Need for a Structured Approach to Digital Forensic Readiness: Digital Forensic Readiness and E-Commerce [19]	/	/				/	/	/			/	/	/
Specifying digital forensics: A forensics policy approach [20]						/	/	/					
Management strategies for implementing forensic security measures [9]	/	/	/	/	/	/	/	/		/	/	/	/
Forensic readiness [11]	/	/	/	/	/		/				/	/	/
An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework [1]						/	/	/		/	/	/	/
Digital forensic research: current state of the art [21]						/	/	/			/	/	
Digital Forensic Readiness: An insight into Governmental and Academic Initiatives [22]	/	/			/	/	/	/				/	

The significance of an SOP is that, using a unified written operating procedure, the business structure, operating environment, equipment operation, work content and procedure are standardized by graphics, specifications, text, and the like. The whole process of investigation procedures must be complied with the international standards as mentioned in [3], [10] and [19].

In digital forensic readiness, an analysis of legal requirement is required in each forensic organization to ensure each action taken by the stakeholder is applicable in legal context [3] including concerning integrity protection of evidence and constraints on handling digital evidences to be lawfully [19]. The interaction between law enforcement and organization affected by crime is important in order to clarify each responsibility in the whole investigation process. Moreover, to be forensically ready, the organization also need to provide training to their stakeholders. Appropriate training is needed to prepare stakeholder for the various roles they may play before, during, and after an incident. Training on the incident awareness helps the stakeholder to understand their role in the digital evidence process and the legal sensitivities of evidence [3]. It is also necessary to ensure that staff are competent to perform any roles related to the handling and preservation of evidence [14], [15 and [17].

3.1.5. Knowledge on IoT (Kn)

As the technology evolve every day, the stakeholders are required to keep updating their knowledge in current technology. Since the digital forensic approach on IoT technology is different compare to others technology, the knowledge must cover all perspectives regarding IoT ecosystem, understanding on the operation flows including the characteristic of IoT devices and its limitations [23], [26]. The stakeholder must be prepared with this knowledge before they can handle the IoT crime incident.

3.1.6. Awareness in IoT (Aw)

IoT awareness is required in each level of stakeholders. For instance, from the management point of view, the IoT awareness will help them to understand how the IoT ecosystem works as it will help them in planning and managing the resources to support the IoT forensic investigation. IoT awareness helps the stakeholder to consider each action taken during the investigation. It is also important for the operation level (technical and non-technical) stakeholder to aware of the IoT characteristics and limitations while handling the investigation process like collecting and preserving the digital evidence. The chain of custody must be secured to be admissible to the court. With these definitions in mind, next section explained how the the readiness framework is proposed.

4. Research Methodology

In this research, the mixed method approach was chosen as different techniques were applied to collect both qualitative and quantitative data. Methodological triangulation was chosen and applied to the confirmatory research, where data and theory are mixed, by comparing, integrating and interpreting [27], [28]. Besides facilitating the confirmation of the framework, it is also used to discover any possible dimension for the IoT forensic framework. The qualitative approach was conducted beforehand, followed by a quantitative approach which allowed the researcher to explore and analyze the expert views in detail, then support the findings with an extensive analysis in the context of the research [29]. In the confirmatory research, the triangulation involves three main parts where the literature review, the experts' interviews, and the survey with industry practitioners were conducted to verify the findings. Data were collected from two different methods; quantitative and qualitative. Subsequently, the results were compared to identify similar decision patterns [30].

5. The Propose Framework

The outcome from the triangulation method has been gathered and the readiness framework is proposed as depicted in Fig.1. These factors have significantly important to ensure the readiness level among investigators at the optimal level. Hence, it will improve the productivity and enhance the quality of the IoT forensics investigation.

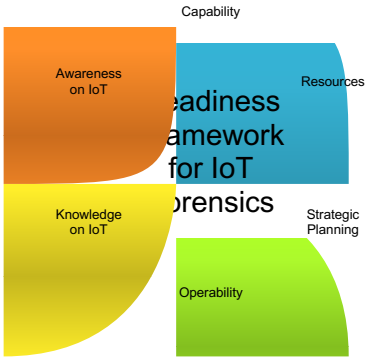

Fig. 1 Readiness Framework

The framework was validated by the digital experts and practitioners. Questions were asked to what extent they agree/familiar/aware with the statements/ questions associated with factors. After completing the designing the questionnaire, the validity and reliability test were considered to ensure the statements measure the factor accurately [31]. According to [31], a sample size of 30 is large enough for a study considering the principles of the Central Limit Theorem. Thus, thirty digital forensic practitioners were invited to participate in the study. The practitioners were enlisted based on their research background and their experience in digital forensic.

6. Conclusion and Future Work

The factors were used to determine the action that needs to be taken by the organization in order to become forensically ready. After synthesizing the literature, six readiness factors were identified. By using triangulation methodology, it combines several techniques to study the same research area. It is useful in exploring and discovering the overlaps and differences in an area subject. Moreover, it can enable validation of data through cross verification from different inputs from digital forensics experts and practitioners. Further investigation will be carried out; this framework will be used in developing an instruments to measure readiness factors among digital forensics stakeholders.

Acknowledgments

The author is grateful for the assistance provided by Associate Professor Gary B.Wills and colleagues from ECS, University of Southampton who give the comments and support for this research. Special thanks to Universiti Teknologi MARA Malaysia and Ministry of Higher Education Malaysia for funding my PhD. Constructive comments and suggestions received from the editor and anonymous reviewers of an earlier draft of the manuscript are appreciated.

References

1. M. Harbawi and A. Varol.(2017) “An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework”, in *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1-6, doi: 10.1109/ISDFS.2017.7916508.
2. Carrier, Brian D. and E. Spafford. (2003) “Getting Physical with the Digital Investigation Process”, in *International Journal of Digital Evidence*, vol.2, No.2.

3. Robert Rowlingson. (2004) "A Ten Step Process for Forensic Readiness", in *International Journal of Digital Evidence*, vol.2,no.2,pp 1–28, 2004, doi:10.1.1.65.6706

4. Kebande, Victor R. and I. Ray. (2016) "A Generic Digital Forensic Investigation Framework for Internet of Things (IoT)", in *Proc IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp.356-362.

5. Sule, D. (2014) "Importance of forensic readiness", in *ISACA Journal*, vol.1, January 2014.

6. Heathcote A. (2017) "Forensic readiness: Good Practice Guide", in *Health and Social Care Information Centre*. 2017.

7. Wiles J, Reyes A. (2007) "Developing an Enterprise Digital Investigative/ Electronic Discovery Capability", in *The Best Damn Cybercrime and Digital Forensics Book Period,* Syngress Publishing; pp. 83–114.

8. Wolfe-wilson J, Wolfe HB.(2003) "Management strategies for implementing forensic security measures", in *Information Security Technical Report,* Vol. 8, No.2, pp. 55-64.

9. Yasinsac A, Manzano Y. (2001) "Policies to enhance computer and network forensics", in *Proceedings of the 2001 IEEE Workshop On Information Assurance and Security*, pp. 289-295.

10. Tan J. (2001) "Forensic readiness". *Cambridge, MA:@ Stake*. pp. 1-23.

11. Venter, H. (2014) "Forensic readiness landscape", in *G. S. D. and B. E.-P. and P. G. and T. K. and C. Rudolph (Ed.), Digital Evidence and Forensic Readiness*, Vol. 4, https://doi.org/10.4230/DagRep.4.2.150

12. Elyas M, Maynard SB, Ahmad A, Lonie A. (2014) "Towards a systemic framework for digital forensic readiness", in *Journal of Computer Information Systems,* Vol.54. No.3, pp. 97–105.

13. Elyas M, Ahmad A, Maynard SB, Lonie A.(2015) " Digital forensic readiness: Expert perspectives on a theoretical framework", in *Computers & Security*. Vol.1, No.52, pp. 70-89. http://dx.doi.org/10.1016/j.cose.2015.04.003

14. Collie J. A (2018) "Strategic Model for Forensic Readiness", in *Athens Journal of Sciences*, Vol.5, No.2, pp.167-182.

15. Grobler CP, Louwrens CP. (2007) "Digital forensic readiness as a component of information security best practice", in *IFIP International Information Security Conference,* pp. 13-24.

16. Reddy K, Venter HS. (2013) "The architecture of a digital forensic readiness management system", in *Computers & Security*, Vol.32 pp.73-89, https://doi.org/10.1016/j.cose.2012.09.008.

17. Barske D, Stander A, Jordaan J. (2010) "A digital forensic readiness framework for South African SME's", in *2010 Information Security for South Africa* pp. 1-6.. doi: 10.1109/ISSA.2010.5588281.

18. Jerker D, Ingvar T. (2004) "The Need for a Structured Approach to Digital Forensic Readiness: Digital Forensic Readiness and E-Commerce", in *IADIS International Conference e-commerce*, pp. 417-421.

19. Taylor C, Endicott-Popovsky B, Frincke DA.(2007) "Specifying digital forensics: A forensics policy approach", in *Digital Investigation*, Vol. 4, pp. 101-104.

20. Raghavan S.(2013) "Digital forensic research: current state of the art", in *CSI Transactions on ICT,* Vol.1 No.1, pp.91–114

21. A. Mouhtaropoulos, M. Grobler and C. Li. (2001) "Digital Forensic Readiness: An Insight into Governmental and Academic Initiatives", in *2011 European Intelligence and Security Informatics Conference*, pp. 191-196. doi: 10.1109/EISIC.2011.30.

22. Oriwoh E, Jazani D, Epiphaniou G, Sant P.(2013) "Internet of things forensics: Challenges and approaches", in *9th IEEE International Conference on Collaborative computing: networking, Applications and Work sharing*, pp.608-615.

23. Pichan A, Lazarescu M, Soh ST.(2015) "Cloud forensics: Technical challenges, solutions and comparative analysis", in *Digital investigation*. Vol.13, pp.38-57. https://doi.org/10.1016/j.diin.2015.03.002.

24. Miranda J, Mäkitalo N, Garcia-Alonso J, Berrocal J, Mikkonen T, Canal C, Murillo JM.(2015) "From the Internet of Things to the Internet of People". in *IEEE Internet Computing*, Vol 19. No.2, pp.40-47.

25. Zawoad S, Hasan R.(2015) "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things", in *2015 IEEE International Conference on Services Computing (SCC)*, pp. 279–84.

26. Lin IL, Yen YS, Chang A. (2011) "A study on digital forensics standard operation procedure for wireless cybercrime", in *2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 543-548.

27. Creswell JW, Plano Clark VL, Gutmann ML, Hanson WE. (2003) "Advanced Mixed Methods Research Designs", in *Handbook of Mixed Methods in Social and Behavioral Research*. pp. 209–40.

28. Warfield D. (2010) "Is/It Research: A Research Methodologies Review", in *Journal of Theoretical & Applied Information Technology*. Vol.13, pp.28–35.

29. Creswell JW, Poth CN. (2016) "Qualitative inquiry and research design: Choosing among five approaches". *Second Edition Sage Publications*, pp.201 – 219

30. Golafshani N. (2003) "Understanding reliability and validity in qualitative research", in *The qualitative report*. Vol.4 No.8, pp. 597-607.

31. Field A.(2013) "Discovering statistics using IBM SPSS statistics". *4th Edition, Sage Publication*, pp. 262-292.