Journal of Positive School Psychology
2022, Vol. 6, No. 3, 8423–8433 http://journalppw.com

# Digital Forensic Readiness for Cyber Security Practitioners: An Integrated Model

Norulzahrah Mohd Zainudin[1] , Nor Asiakin Hasbullah[2], Muslihah Wook[3], Suzaimah Ramli[4] and Noor Afiza Mat Razali[5]

*[1,2,3]Senior Lecturer, National Defence University Malaysia, Faculty of Defence Science and Technology, Department of Computer Science*
*[4,5]Associate Professor, National Defence University Malaysia, Faculty of Defence Science and Technology, Department of Computer Science*
*Email: [1]norulzahrah@upnm.edu.my, [2]asiakin@upnm.edu.my, [3]muslihah@upnm.edu.my, [4]suzaimah@upnm.edu.my, [5]noorafiza@upnm.edu.my*

**Abstract**

The growing threat of online fraud and security breach incidents poses significant challenges to enforcement agencies and those involved with digital forensics globally. Digital forensic readiness (DFR) enables an organization to prepare itself to perform an investigation more efficiently. The issue that often arises is organizations have no proper DFR plan to deal with forensic incidents. A DFR plan will provide the proactive capability for preparing digital forensic investigation. Various factors have been mentioned in the previous studies of DFR models including legal, people, management support, policy, and many more. However, no model emphasizes the mental readiness for digital forensics investigation, that is another important factor influencing a person to be prepared in new technologies as digital forensic is always dynamic. Mental readiness in this context refers to preparing the mind for forensics incidents to accomplish the required outcome. For this reason, the existing factors in the DFR will be integrated with the Technology Readiness Index (TRI). The objectives of this study are to examine the availability of the DFR Plan, to select the optimum DFR factors for cybersecurity practitioners, and to develop an integrated DFR model. This research aims to investigate digital forensic readiness factors that influence cybersecurity practitioners to be equipped for digital forensic investigations. The expected results of this study are Digital Forensic Readiness factors for cybersecurity practitioners and the Integrated Digital Forensic Readiness model for cybersecurity practitioners.

**Keywords**: cybercrimes, digital evidence, cyber security, digital forensic readiness model

## I. INTRODUCTION

Today's huge volumes of data, heterogeneous information and communication platforms, and borderless network infrastructures are adding new challenges for cybercrime forensic security experts and law enforcement agencies (Caviglione et al., 2017). The future of digital forensics is being discussed, with an emphasis on these issues and the changes needed to effectively defend modern societies and combat cybercrime.

Forensic investigations take place after crimes have occurred in any event; in this case, the crime scenes themselves can be online. Digital forensics helps investigators figure out what happened, when it happened, where it happened, why it happened, and preferably who is accountable systematically and forensically. Such details are necessary to confirm that evidence found are sufficient to prosecute a person for the criminal act that has been committed (Rogers, 2003). All this information is required to ensure that there is sufficient

© 2022 JPPW. All rights reserved

evidence to prosecute criminals. The most difficult aspects of digital forensics are completing the analysis and reporting the results to assure that the evidence is consistent and dependable for criminal prosecution in a court of law (Al-Mahrouqi et al., 2015).

Digital Forensic Readiness (DFR) is described as the ability to which computer systems or computer networks log activities and data in such a way that the logs are significant in scope for further forensic purposes and acceptable in regarding the perceived authenticity as evidence in later forensic investigations (Sachowski & Sachowski, 2019). Digital forensic readiness provides a "win - win" situation because it complements and improves the information security program and strategies of an organization. Although not formally recognized, many organizations already carry out some information security practices, such as the diligent collection and storage of digital information in relation to digital forensic readiness.

Several different process model methodologies have been developed over the years, to group the common digital forensic activities into recognizable phases. Commonalities were found from existing process models leading to the development of a new process model that integrate readiness digital forensic investigation process.

## II. BACKGROUND

Digital forensic (DF) is one of the branches in forensic science, which focuses more on the investigation of the digital world (Conlan et al., 2016; Mothi et al., 2020). DF uses scientific methods in the investigation to find evidence like any other forensic investigations. The main goal of DF is to enable evidence obtained from investigation to be admissible in court and its validity not to be questioned (Lutui, 2016).

DF has grown rapidly in a period to become a very important part in many investigations in the cyber world (Mothi et al., 2020). There are various tools have been developed to meet the needs of the investigation involving digital forensics and has been used by digital forensic investigators and analysts from various agencies such as the police, military, customs and immigration, and the court to acquire digital evidence(Caviglione et al., 2017; Conlan et al., 2016; Mothi et al., 2020). Developments in forensic research, tools, and processes over the last few years has established this area and those related in this area now rely on the investigation models and tools that have been developed by various parties (Karie & Venter, 2015; Kebande et al., 2018; Zainudin et al., 2021; Zainudin et al., 2011). The next sections will explain in detail about digital forensics.

### A. *Digital Forensic*

There are a variety of digital forensics definitions in the literature and this term is often used equally with Forensic Computing and Computer Forensics, which indicates that they carry the same meaning and purpose (Palmer, 2001; Sammes et al., 2002). Rodney McKemmish (McKemmish, 1999) defines forensic computing as “The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable”. While Philip D. Dixon (Dixon, 2005) in his article “An overview of computer forensics” states that the core goals of computer forensics are: the preservation, identification, extraction, documentation, and interpretation of computer data. However, there are few procedures that have been defined and considered to ensure that the forensic data is valid and useful in legal affairs.

### *B. Digital Forensic Readiness*

Rowlingson (Rowlingson, 2004) has defined forensic readiness as the ability of an organization to maximize their potential in using digital evidence and minimize the costs of investigations incurred by the organization and added “forensic readiness is a security process which is more procedural and staff-intensive than technological”. Pangalos and Katos (Pangalos & Katos, 2010) extend this perspective as “the state of the organization where certain controls are in place in order to facilitate the digital forensic processes and to assist in the anticipation of unauthorized actions shown to be disruptive to planned operations”.

© 2022 JPPW. All rights reserved

Instead of forensic readiness, some authors define forensic readiness as 'proactive forensics.

Bradford et al. (Bradford et al., 2004) define proactive forensic as: "proactive computer system forensics is the design, construction and configuring of systems to make them most amenable to digital forensics analyses in the future". Mouhtaropoulos & Dimotikalis (Mouhtaropoulos et al., 2011) emphasize the similarities of "proactive forensic" and "digital forensic readiness" by commenting: "little academic research has been conducted on an organization's proactive forensic capability. This capability is referred to as digital forensic readiness and aims to maximize the forensic credibility of digital evidence, while minimizing its post-incident forensic investigation."

## III. RELATED WORK

Forensic readiness would facilitate the entire forensic process rather than only focusing on the production of credible digital evidence and adds a defensive dimension to the forensic process (Kebande & Venter, 2018; Kyaw et al., 2019). Thus, digital forensic readiness (DFR) has been studied in many areas so that it can implemented accordingly.

### *A. Digital Forensic Readiness Models*

Based on the various studies about DFR, we have gathered Digital Forensic Readiness Models that will be groundwork to our proposed model. Firstly, we have selected digital forensic model that include readiness phase in their model (Baryamureeba & Florence, 2004; Carrier & Spafford, 2004; Kohn et al., 2006; Montasari, 2016; Montasari & Hill, 2019; Valjarevic & Venter, 2015). Then, several models that were developed and dedicated for digital forensic readiness were studied thoroughly. Reddy and Venter (Reddy & Venter, 2013) has developed an architecture of a digital forensic readiness management system. The system has included digital forensic information module as one of the components in the system. The components in the system are listed here:

1) Event analysis module
2) Digital forensic readiness module
3) Costing module
4) Access control module
5) User interface module

This is a conceptual design of forensic readiness for management system.

Garba (Abdullahi Garba, 2015) developed a holistic-based digital forensic readiness framework for a financial institution that gathered various factors of DFR that are suitable for bank's operational unit. The factors implemented are:

1) Policy and procedure
2) People
3) Forensic preparation
4) System and events
5) Monitor and report
6) Risk assessment
7) Legal requirement

However, this framework is presented in a circular process which is confusing as this is shown that the process can be started anywhere in the framework. This is unsuitable as obviously no process should start at monitor and report, for instance.

Moussa et al. (Moussa et al., 2014) developed a forensics readiness framework specifically for infrastructure as a service consumer. The factors of DFR included in the frameworks are:

1) Strategy
2) Monitoring
3) Compliance
4) Procedure

Each factor has its own sub-factor to support the whole process. However, this is a conceptual framework that needs extension study to verify the model. Some other studies have been done as well to gather more information on DFR that can be implemented in this research (Díaz López, 2017; Englbrecht et al., 2020).

### *B. Technology Readiness Index (TRI)*

Another factor that is considered important in digital forensic readiness is the mental readiness that will assess a user's personal characteristics which indicates a propensity or willingness to use digital forensic technology (Koivisto et al.,

© 2022 JPPW. All rights reserved

2016). Cyber security personnel are constantly exposed to various pressures in the organization including extreme workload, exposure to extreme evidence such as child pornography, and even disruption in the family (Chatterjee, 2016; Seigfried-Spellar, 2018). Cyber security personnel should be prepared mentally and be resilient for the challenges they may confront with.

As we have explained in the previous section, computing technology is highly dynamic, as is digital forensic technology that cybersecurity personnel need to keep pace with it. New tools and technology are always produced for digital forensics, so they must be aware of the latest developments (Qasem, 2021). If users are not inclined with the latest technology in digital forensics, rejection can occur - resulting in the organization incurring financial losses, investigation will be time consuming, and evidence will not be gathered ideally.

TRI was introduced to find out the consumer's tendency towards technology. This theory is based on technological readiness factors that focus on the measurement of individual mental inclinations of users. In digital forensic context, this index will be used to measure the preparedness of cybersecurity practitioners towards digital forensic new technologies, techniques, and ideas mentally.

TRI divides the technology readiness factor into four constructs namely 'optimistic', 'innovative', 'discomfort' and 'insecurity'. The 'optimistic' construct means consumers 'positive thinking towards technology and consumers believe technology can provide increased control, flexibility and efficiency in life; the 'innovative' construct means the consumer's tendency to be a pioneer of technology; the construct of 'discomfort' is a perception of lack of control over technology and a feeling of lack of confidence in using technology well; and the construct 'insecurity' means a feeling of distrust of the technology and the user doubting the ability of the technology to do the job perfectly. The 'optimistic' and 'innovative' constructs are under the category of positive readiness factor (motivator), while the constructs of 'discomfort' and 'insecurity' are in the category of negative readiness factor (barrier). All these constructs are described in general terms only. In this study, the construct will be adapted into the research model that will be integrated with the existing factors in the previous models. TRI has been used by various studies to measure the level of technological readiness and the findings from these past studies are seen to have an impact on the issues studied (Rosalina et al., 2020; Sharma, 2020; Smith et al., 2018).

**Table 1 The Mapping of The Digital Forensic Models and Frameworks with Factors / Constructs**

| FACTOR / CONSTRUCT | DIGITAL FORENSIC READINESS MODEL / FRAMEWORK | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Moussaa, 2014 | Elyas, 2015 | Pooe, 2015 | Garba, 2015 | Lopez, 2017 | Collie, 2018 | Pooe, 2018 | Alenezi, 2019 | Pratama, 2020 | Kebande, 2020 |
| Legal requirement | | | | x | | | | | | |
| Legal and ethical | x | | | | | | | | | |
| Service level agreements (SLA) | | | | | | | | x | | |
| Multi- jurisdiction | | | | | | | | x | | |
| Control and legality | | | | | | | | | x | |
| Electronic laws | | | | | | | x | | | |
| Justice system | | | | | | | x | | | |
| Law enforcement | | | | | | | x | | | |
| Legal and regulatory | | | | | | | | | | x |
| Policy | x | x | x | | | | | | | |
| Policy and procedure | | | | x | | | | | x | |
| Policing | | | | | x | | | | | |
| Policies | | | | | | | X | x | | |
| Forensic policy | | | | | | | | | | x |
| Strategy | x | x | | x | | | | | x | |
| Readiness strategy | | | | | | | | x | | |
| Organizational forensic strategy | | | | | | | | | | x |
| Non-technical stakeholders | | x | | | | | | | | |
| Technical stakeholders | | x | | | | | | | | |
| Top management support | | x | | | | | | | | |
| People | x | | x | x | | x | | | | |
| Incident & evidence expertise | | | | | x | | | | | |
| Management support | | | | | | x | | x | | |
| Human resources | | | | | | | x | | | |
| Justice personnel | | | | | | | x | | | |
| Technology | x | x | x | | | | | | | |
| Technological capacity | | | | | x | | | | | |
| Forensic technologies | | | | | | | | x | | |
| Technology & security | | | | | | | | | x | |
| DFR technologies | | | | | | | x | | | |
| Monitoring | x | x | | | | | | | | |
| Monitor and report | | | | x | | | | | | |
| System architecture | | x | | | | | | | | x |
| Cloud architecture | | | | | | | | x | | |
| Training | | x | | | | | | | | |
| Training requirements | | | | | | | | | | x |
| Training and awareness | | | | | | | | x | | |
| Culture | | x | | | | | | | | |
| Organization culture | | | | | | | | x | | |
| Governance | x | x | | | | | | x | | |
| Procedures | x | | | | | | x | x | | |
| Process | | | x | | | | | | | |

© 2022 JPPW. All rights reserved

### *C. Summary of Related Work*

Previously we have gathered the forensic readiness factors in digital forensic readiness models and frameworks that were developed by various researchers. Table 1 shows the mapping of the digital forensic models and frameworks with their factors/ constructs. From this table we conclude that the diverse terms are basically refer to the same terms, and the conflicting terminology reflecting different interpretations of each factor / construct. Subsequently, we will choose the relevant factors that relate to cybersecurity practitioners' readiness to develop our model.

### *The Proposed Model*

This study aims to concentrate on the cyber security practitioners. We have explained the various factors as well in DFR have been identified from previous studies. Many DFR factors involve in preparing cyber security and digital forensic practitioners before they can perform digital forensic investigation forensically sound. We find that most studies that implement DFR focused more on corporate readiness, lacking on the investigative area that is equally significant. We will choose the significant factors required in DFR for cyber security practitioners and adapt the factors in Technology Readiness Index (TRI), to formulate an integrated model.

### *A. Development of Model*

Figure 1 shows the model development process which is divided into four stages. In the first stage, thorough literature study is done to figure out what are the influencing factors for digital forensic readiness. In the next stage, the relevant factors are identified, then assessment is done to eliminate irrelevant factors as well as replicated factors. Finally, we produce a conceptual model of Digital Forensic Readiness for Cybersecurity Practitioners. Table 2 shows the mapping of existing digital forensic models and the factors that were chosen. It shows that some of the factors are not yet studied and applied in forensic readiness. Thus, this study will explore those factors to measure whether they are significant in influencing digital forensic readiness for cyber security practitioners. In the final stage, we produced a conceptual model for the previously stated reason.

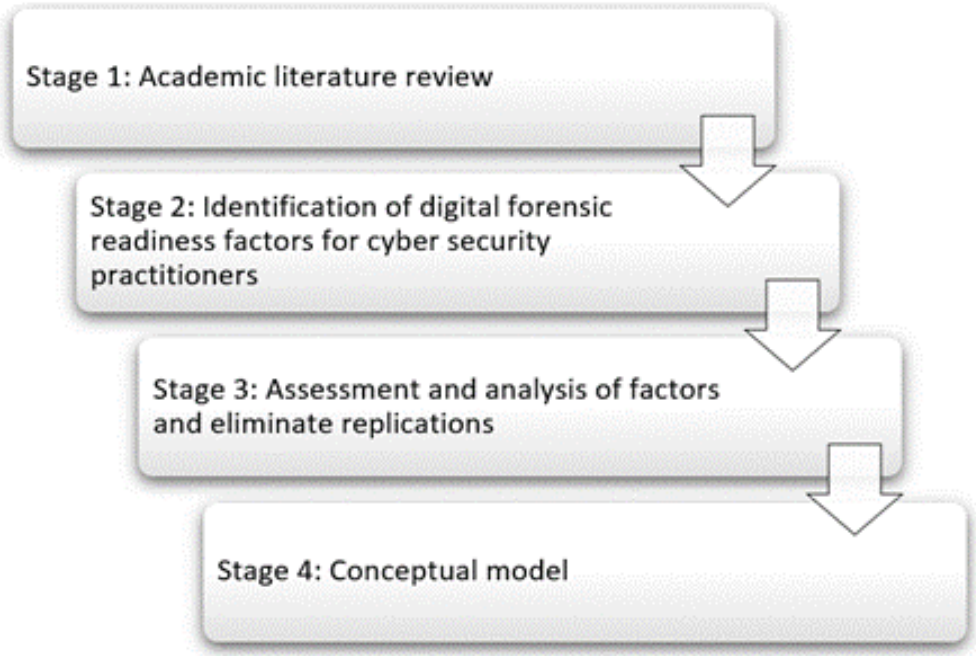


**Figure 1. The model development process**

© 2022 JPPW. All rights reserved

**Table 2 The Mapping of Digital Forensic Readiness Factors and Existing Models**

| Factor / Construct | | | Existing Forensic Readiness Model/Framework | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Moussaa, 2014 | Elyas, 2015 | Pooe, 2015 | Garba, 2015 | Lopez, 2017 | Collie, 2018 | Pooe, 2018 | Alenezi, 2019 | Pratama, 2020 | Kebande, 2020 |
| Digital Forensic Readiness based on TRI 2.0 | | Optimism | | | | | | | | | | |
| | | Innovativeness | | | | | | | | | | |
| | | Discomfort | | | | | | | | | | |
| | | Insecurity | | | | | | | | | | |
| Digital Forensic Readiness Factors | Moderator | Training | | √ | | | | | | √ | | √ |
| | Mediator | Experience | | | | | | | | | | |
| | Technical Factors | Forensic Technologies | √ | √ | √ | | √ | | √ | √ | √ | |
| | | System Architecture | | √ | | | | | | | | √ |
| | Organizational Factors | Management Support | | √ | | | | √ | | √ | | |
| | | Readiness Strategy | √ | √ | | √ | | | | √ | √ | √ |
| | | Culture | | √ | | | | | | √ | | |
| | | Procedures | √ | | | √ | | | √ | √ | √ | |
| | | Governance | √ | √ | | | | | | √ | | |
| | Legal Factors | Forensic Policy | √ | √ | √ | √ | √ | | √ | √ | √ | √ |
| | | Legal and Regulatory | √ | | | √ | | | | √ | | √ |

### *B. The Conceptual Model of Digital Forensic Readiness for Cyber Security Practitioners*

The conceptual model of digital forensic readiness for cyber security practitioners, as shown in Figure 2, illustrate the chosen factors from our literature study. These factors are explained thoroughly in the next paragraphs.

### *C. Digital Forensic Readiness based on TRI 2.0*

- Optimism: A positive view of digital forensic and belief that it offers efficiency during investigation
- Innovativeness: A tendency to learn new technology, techniques, and ideas in digital forensic
- Discomfort: A perception of being overwhelmed by digital forensic technology and digital evidence, as well as a perceived lack of control over it.
- Insecurity: Distrust of digital forensic technology, stemming from skepticism about its ability to work properly and concerns about its potential harmful consequences.

### *D. Digital Forensic Readiness Factors*

- Training: Training is incorporated in the human resource planning once an employee reports a job to increase knowledge sharing and creation. Training is used as a moderator in this research model to study if it affects the relationship between 'Forensic Technologies', 'System Architecture" and 'Forensic Personnel Capabilities'
- Experience: What people encounter and notice during their time at a company is referred to as experience. Experience is being examined as a mediator to see if it influences digital forensics readiness primarily through experience.
- Technical Factors: The technical factors describe the technical aspects that influence digital forensic readiness in organizations.
- Forensic Technologies: Forensic technologies provide advanced forensic tools hardware that enables organizations to perform a full-scale digital investigation. When gathering and analyzing digital evidence, they are considered crucial. Conducting a digital investigation can be difficult without the appropriate tools, thus these technologies must

© 2022 JPPW. All rights reserved

be effective and accurate to generate admissible evidence.

- System Architecture: The ISO/IEC 27043 defined system architecture as the organization's information system that comprises of endpoints, network, software, and data.
- Organizational Factors: The organizational factors show how an organization's and its employees' characteristics will help with digital forensic readiness.
- Management Support: This factor includes the organization's top management, which assists the organization in achieving forensic readiness, including authorization, decision-making, required personnel, and funds. It is critical that top management in organizations understands the significance of being forensically ready and has control over the formation and execution of digital forensic readiness.
- Readiness Strategy: This factor refers to an organization's strategy for achieving forensic readiness. The plan, in general, is concerned with how the readiness can be implemented. Organizations must clearly define committed strategic goals that serve the organization's needs to achieve good forensic readiness. To respond to future changes, the organization's readiness plan must be flexible.
- Culture: This is a set of ideas, attitudes, assumptions, and practices that have a direct effect on the process of digital forensics. It is critical to understand the culture before adding digital forensics, as this leads to more effective future forensics investigations.
- Procedures: This factor includes the organization's digital forensics guidelines as well as security and privacy policies during digital investigations. Organizations should make their forensics procedures transparent, as this will enable them to obtain admissible evidence. These procedures include a variety of protocols, guidelines, and principles that govern an organization's digital forensic investigation.
- Governance: This factor examines a firm's capacity to integrate digital forensics readiness. This entails overseeing processes and duties to gather evidence and conduct a successful forensic investigation.
- Legal Factors: Elements of lawful and regulatory concerns are shown in the legal factors.
- Forensic Policy: The forensic policy is the legally binding structure of the laws that regulate the forensics people, procedures, and technologies within the firm. It should have top management support, developed by the organizations' forensic and non-forensic personnel, and it should incorporate in the firm's policy strategy or as a distinct policy.
- Legal and Regulatory: Depending on the jurisdiction and sector in which an organization operates, legal and regulatory standards are imposed on it.

## IV. DISCUSSION AND CONCLUSION

This paper discussed about development of a digital forensic readiness model specifically for cyber security practitioners. We described the concept of digital forensics, digital forensic readiness and the existing digital forensics readiness models and frameworks. All models developed generally focus on the digital forensic environment itself, as well as on a specific area. The proposed model integrates cognitive aspects adapted from TRI 2.0 that measures psychological factors that influence digital forensic readiness. This model focuses on exploring influencing factors towards digital forensic readiness for cyber security practitioners. As this is a conceptual model, there are more study need to be done including verifying the model from experts and the needs to perform technical analysis.

## BIBLIOGRAPHY

1. Abdullahi Garba, A. (2015). a Holistic-Based Digital Forensic Readiness Framework for Zenith Bank, Nigeria. 551–560. http://iccss.vfast.org/@
2. Al-Mahrouqi, A., Abdalla, S., & Kechadi, T. (2015). Efficiency of network event logs as admissible digital evidence. Proceedings of the

© 2022 JPPW. All rights reserved

2015 Science and Information Conference, SAI 2015, 1257–1265. https://doi.org/10.1109/SAI.2015.7237305

3. Baryamureeba, V., & Florence, T. (2004). The Enhanced Digital Investigation Process Model. Asian Journal of Information Technology, 5, 790–794.
4. Bradford, P. G., Brown, M., Perdue, J., & Self, B. (2004). Towards proactive computer-system forensics. International Conference on Information Technology: Coding Computing, ITCC, 2(May 2014), 648–652. https://doi.org/10.1109/ITCC.2004.1286727
5. Carrier, B., & Spafford, E. (2004). An event-based digital forensic investigation framework. Digital Forensic Research Workshop, 1–12. https://doi.org/10.1145/1667053.1667059
6. Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security and Privacy, 15(6), 12–17. https://doi.org/10.1109/MSP.2017.4251117
7. Chatterjee, P. (2016). Organizational Stress , Job Satisfaction and Employee Mental Health : A Comparative Analysis among the Banking and I . T . Professionals. 5(2), 1–16.
8. Conlan, K., Baggili, I., & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation, 18(December 2015), S66–S75. https://doi.org/10.1016/j.diin.2016.04.006
9. Díaz López, A. F. (2017). Are you ready? A proposed framework for the assessment of digital forensic readiness. https://search-proquest-com.login.captechu.edu:2443/docview/1977474175/abstract/7E2C189392194D1APQ/8
10. Dixon, P. D. (2005). An overview of computer forensics. IEEE POTENTIALS, 24(5), 7–10.
11. Englbrecht, L., Meier, S., & Pernul, G. (2020). Towards a capability maturity model for digital forensic readiness. Wireless Networks, 26(7), 4895–4907. https://doi.org/10.1007/s11276-018-01920-5
12. Karie, N. M., & Venter, H. S. (2015). Taxonomy of Challenges for Digital Forensics. Journal of Forensic Sciences, 60(4), 885–893. https://doi.org/10.1111/1556-4029.12809
13. Kebande, V. R., Karie, N. M., & Venter, H. S. (2018). Adding Digital Forensic Readiness as a security component to the IoT domain. International Journal on Advanced Science, Engineering and Information Technology, 8(1), 1–11. https://doi.org/10.18517/ijaseit.8.1.2115
14. Kebande, V. R., & Venter, H. S. (2018). Novel digital forensic readiness technique in the cloud environment. Australian Journal of Forensic Sciences, 50(5), 552–591. https://doi.org/10.1080/00450618.2016.1267797
15. Kohn, M., Eloff, J. H. P., & Olivier, M. S. (2006). Framework for a Digital Forensic Investigation. Communications, March, 1–7. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.145.5855
16. Koivisto, K., Makkonen, M., Frank, L., & Riekkinen, J. (2016). Extending the technology acceptance model with personal innovativeness and technology readiness: A comparison of three models. 29th Bled EConference: Digital Economy, BLED 2016, 113–128.

© 2022 JPPW. All rights reserved

17. Kyaw, A., Cusack, B., & Lutui, R. (2019). Digital Forensic Readiness in Wireless Medical Systems. 2019 29th International Telecommunication Networks and Applications Conference, ITNAC 2019. https://doi.org/10.1109/ITNAC46935.2019.9078005
18. Lutui, R. (2016). A multidisciplinary digital forensic investigation process model. Business Horizons, 59(6), 593–604. https://doi.org/10.1016/J.BUSHOR.2016.08.001
19. McKemmish, R. (1999). What is forensic computing? Trends and Issues in Crime and Criminal Justice, 118(118), 1–6. http://www.aic.gov.au/publications/current series/tandi/101-120/tandi118.html%5Cnhttp://www.aic.gov.au/publications/current%5Cnseries/tandi/101-120/tandi118.html
20. Montasari, R. (2016). A comprehensive digital forensic investigation process model. Int. J. Electronic Security and Digital Forensics, 8(4), 285–302. https://doi.org/10.1504/IJESDF.2016.079430
21. Montasari, R., & Hill, R. (2019). Next-Generation Digital Forensics: Challenges and Future Paradigms. Proceedings of 12th International Conference on Global Security, Safety and Sustainability, ICGS3 2019. https://doi.org/10.1109/ICGS3.2019.8688020
22. Mothi, D., Janicke, H., & Wagner, I. (2020). A novel principle to validate digital forensic models. Forensic Science International: Digital Investigation, 33, 200904. https://doi.org/10.1016/j.fsidi.2020.200904
23. Mouhtaropoulos, A., Grobler, M., & Li, C. T. (2011). Digital forensic readiness: An insight into governmental and academic initiatives. Proceedings - 2011 European Intelligence and Security Informatics Conference, EISIC 2011, 191–196. https://doi.org/10.1109/EISIC.2011.30
24. Moussa, A. N., Ithnin, N. B., & Miaikil, O. A. M. (2014). Conceptual forensic readiness framework for infrastructure as a service consumers. Proceedings - 2014 IEEE Conference on System, Process and Control, ICSPC 2014, January 2018, 162–167. https://doi.org/10.1109/SPC.2014.7086250
25. Palmer, G. (2001). A Road Map for Digital Forensic Research. DFRWS.
26. Pangalos, G., & Katos, V. (2010). Information assurance and forensic readiness. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 26 LNICST(May 2014), 181–188. https://doi.org/10.1007/978-3-642-11631-5_17
27. Qasem, Z. (2021). The effect of positive TRI traits on centennials adoption of try-on technology in the context of E-fashion retailing. International Journal of Information Management, 56(March 2020), 102254. https://doi.org/10.1016/j.ijinfomgt.2020.102254
28. Reddy, K., & Venter, H. S. (2013). The architecture of a digital forensic readiness management system. Computers and Security, 32, 73–89. https://doi.org/10.1016/j.cose.2012.09.008
29. Rogers, M. (2003). The role of criminal profiling in the computer forensics process. Computers and Security, 22(4), 292–298. https://doi.org/10.1016/S0167-4048(03)00405-X
30. Rosalina, V., Munandar, T. A., Hidayanto, A. N., & Santoso, H. B.

© 2022 JPPW. All rights reserved

(2020). Measuring citizen readiness to adopt electronic citizen relationship management (E-CIRM) using technology readiness index (TRI). Journal of Theoretical and Applied Information Technology, 98(21), 3416–3425.

31. Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. Int. J. Digit. EVid., 2.
32. Sachowski, J., & Sachowski, J. (2019). Digital Forensic Readiness. Digital Forensics and Investigations, 203–217. https://doi.org/10.4324/9781315194820-13
33. Sammes, J., Jeckinson, A., & Jeckinson, B. (2002). Forensic Computing: A Practitioner's Guide. Springer.
34. Seigfried-Spellar, K. C. (2018). Assessing the Psychological Well-being and Coping Mechanisms of Law Enforcement Investigators vs. Digital Forensic Examiners of Child Pornography Investigations. Journal of Police and Criminal Psychology, 33(3), 215–226. https://doi.org/10.1007/s11896-017-9248-7
35. Sharma, B. R. (2020). Developing a Predictive Model Using Logistic Regression to Portend the Intention to Go Cashless in Mumbai Using Constructs of Technology Readiness Index. ACM International Conference Proceeding Series, 54–59. https://doi.org/10.1145/3387263.3387286
36. Smith, M., Walford, N. S., & Jimenez-Bescos, C. (2018). Assessing the user response to differences in functionality when visualising 3D models of cultural heritage sites using the Technology Readiness Index. Digital Applications in Archaeology and Cultural Heritage, 10, 1–22. https://doi.org/10.1016/j.daach.2018.e00076
37. Valjarevic, A., & Venter, H. S. (2015). A Comprehensive and Harmonized Digital Forensic Investigation Process Model. Journal of Forensic Sciences, 60(6), 1467–1483. https://doi.org/10.1111/1556-4029.12823
38. Zainudin, Norulzahrah M, Hasbullah, N. A., Wook, M., Ramli, S., & Razali, N. A. M. (2021). Online Social Networks as Supporting Evidence for Digital Forensic Investigation : A Revised Model. The 11th Annual International Conference on Industrial Engineering and Operations Management.
39. Zainudin, Norulzahrah Mohd, Merabti, M., & Llewellyn-Jones, D. (2011). Online social networks as supporting evidence: A digital forensic investigation model and its application design. 2011 International Conference on Research and Innovation in Information Systems, 1–6. https://doi.org/10.1109/ICRIIS.2011.6125728

© 2022 JPPW. All rights reserved