BOOK CHAPTER | *"Do Your Due Diligence"*

Exploring Lack of Due Diligence as a Threat to Forensic Analysis Preparation and Readiness

Jonas Takyi Asamoah
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: Joricomgh@Gmail.Com
Phone: +233244923832

ABSTRACT

The usage of digital technology in the digital forensic investigation has grown in tandem with the rising importance of technology today. Too many incidences of digital and physical crime which is the focus of the world nowadays. To gather the finest evidence and investigative outcomes, a digital forensic model must be established. This study included a review of the literature on digital forensics and models established in digital forensics. According to the findings, the majority of research involves broad inquiries and procedures that overlap. Furthermore, no model has been developed to design a systemic inquiry. In this study, we propose a methodology for digital forensic examination to address this issue. This model combines several of the previous models and adds some new variables that are relevant to the study.

Keywords: Due Diligence, Threats, Forensic Analysis, Preparation, Readiness, Cyber Security,

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Jonas Takyi Asamoah (2022): Exploring Lack of Due Diligence as a Threat to Forensic Analysis Preparation and Readiness
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 307-314
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P49

1. INTRODUCTION

Organizations are increasingly reliant upon information systems for almost every facet of their operations. As a result, there are legal, contractual, regulatory, security, and operational reasons why this reliance often translates into a need to conduct digital forensic investigations (Carrier & Spafford, 2004). There is an agreement in both professional and academic literature that in order for organizations to meet this challenge, they must develop 'digital forensic readiness' and the proactive capability to collect, analyze and preserve digital information (Fagbola & Venter, 2022). Unfortunately, although digital forensic readiness (DFR) is becoming a legal and regulatory requirement in many jurisdictions in the western world, studies show that most organizations especially in Australia have not developed a significant capability in this domain (e.g. the Australian Institute of Criminology reports that less than 2% of Australian organizations have a plan for digital forensics.

A key issue facing organizations intending to develop a forensic readiness capability is the lack of comprehensive and coherent guidance on how forensic readiness can be achieved in both the professional and academic literature (Kebande & Choo, 2022). A review of the literature conducted as part of this study found that the academic and professional discourse in forensic readiness is fragmented and dispersed in that it does not build cumulatively on prior knowledge (Zainudin, Hasbullah, Wook, Ramli, & Razali, 2021). Further, there is a lack of maturity in the discourse rooted in the reliance on informal definitions of key terms and concepts. For example, there is little discussion and understanding of the critical organizational factors that contribute to forensic readiness, the relationships between these factors, and the precise definitions including the scope and boundaries of these factors. Importantly, there is no collective agreement on the primary motivating factors for organizations to become forensically ready (Hughes, Ziemak, Martinez, & Stout, 2022).

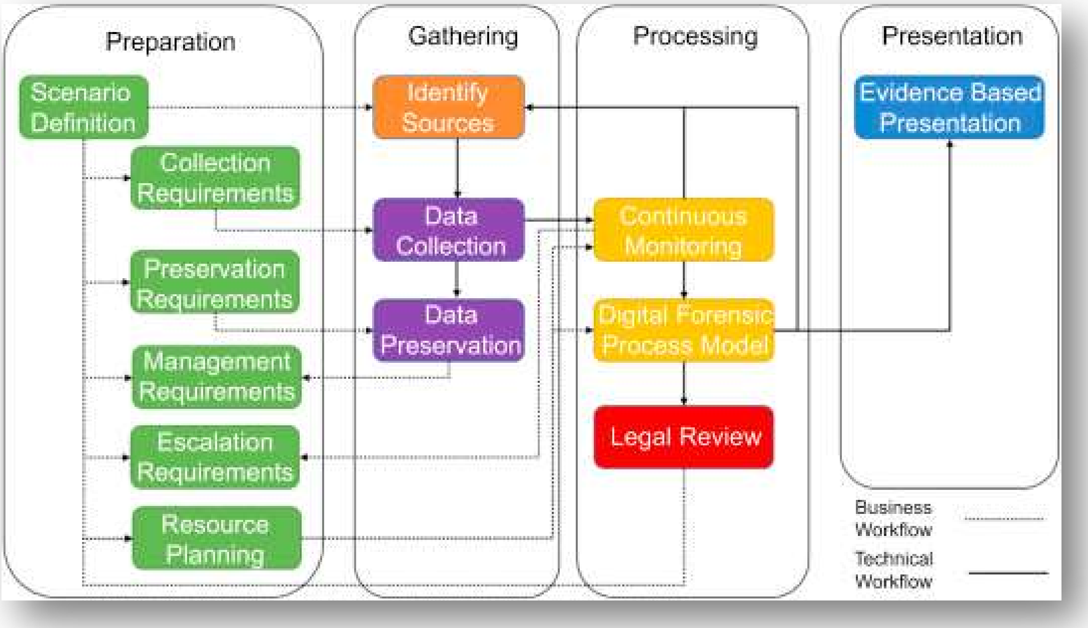

Fig 1: Forensic Readiness Framework
Source: https://www.sciencedirect.com/topics/computer-science/digital-forensic-readiness

(Lin, 2018) As information technology relies heavily on works around the information, therefore it becomes tremendously important to protect the information by ensuring that no unauthorized person can get the access and the integrity and confidentiality remain sustained. (Sudyana, 2019) Ensure the timely availability of the information for associated operations and securing these operations from the different threats such e.g., Phishing are vital tasks for the technical persons for their organization. Computer forensics emerged in response to the escalation of crimes committed by the use of computer systems either as an object of the crime, an instrument used to commit a crime, or a repository of evidence related to a crime. Computer forensics can be traced back to as early as 1984 when the FBI laboratory and other law enforcement agencies began developing programs to examine computer evidence.

In the current era, the majority of large enterprises rely heavily upon the usage of technology in operations and other segments of the business. With the increased reliance and usage of technology, the risk of cybercrime becomes also more serious in case of occurrence. To counter this risk, digital forensic investigation firms provide assistance in conducting forensic analysis after the occurrence of any cybercrime. With the passage of time, the forensic investigation process has also been modified and distributed into different phases to make this investigation more effective. Every phase has its own impact on the process of investigation (Elyas, Maynard, Ahmad, & Lonie, 2014). With the introduction of Information Technology in the business, every organization that comprises IT has started to take benefit of this technology. This is done by attaining an advantage over other competitors in the market, by providing new features to the customers after incorporating technology at the operational side especially, by increasing the operational speed, and reducing the probability of any error in operations (Ishikawa, 2016).

Research groups like the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have since been formed in order to discuss the computer forensic science as a discipline including the need for a standardized approach to examinations (Prakash, Williams, Garg, Savaglio, & Bawa, 2021).

Digital forensics has been defined as the use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation, 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 the unauthorized actions shown to be disruptive to planned operations. One important element of digital forensics is the credibility of the digital evidence. Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines, etc. The legal settings desire evidence to have integrity, authenticity, reproductiveness, non-interference, and minimization (Hughes et al., 2022).

2. LITERATURE REVIEW

Digital forensic readiness (DFR) was first described by (Carrier & Spafford, 2004) as setting up digital forensics in organizations to minimize the cost of digital forensics whilst maximizing the capability of an organization to collect legally reliable digital evidence. (Kebande & Ray, 2016) extend this perspective by defining forensic readiness 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”. Forensic readiness, as per this definition, would facilitate the entire forensic process rather than only focusing on the production of credible digital evidence and adds an ‘anticipatory’ dimension to the forensic process.

Forensic readiness has been studied from many perspectives including resourcing (Maras, 2015), technology use and selection (Hossain, Karim, & Hasan, 2018), training (Nelson, Phillips, & Steuart, 2019), legal investigations (Forrester & Irwin, n.d.), and policy (Fagbola & Venter, 2022). None of this research discusses forensic readiness holistically; rather, they each treat forensic readiness from their particular perspective.

As organizations become more subject to regulation (e.g. Sarbanes-Oxley) the importance that is placed on being forensically ready is increasing (Lutui, 2021), and therefore focusing on a comprehensive forensics readiness perspective becomes more important. But organizations need to be able to balance the cost of being forensically ready and the benefit of being able to produce digital forensic evidence as required for forensic readiness to be effective (Zainudin et al., 2021).

There are several authors that have suggested digital forensic investigation models and frameworks, for example, (Hughes et al., 2022) proposed a computer and network forensic methodology that consists of three basic components These are 1) acquire evidence; 2) authenticate evidence; and 3) analyze data. This process involves assuring that the data is valid and provides a method for analyzing the data while maintaining its integrity. Based on the model proposed by them, a few other models were created with further enhancements to several features (Maras, 2015).

(Nelson et al., 2019) has produced a model involving 17 phases divided into five groups: 1) Readiness Phases; 2) Deployment Phases; 3) Physical Crime Scene Investigation Phases; 4) Digital Crime Scene Investigation Phases, and 5) Review Phases. This model looks impeccable because it involves concerns in data protection and retrieval, imaging, extraction, interrogation, normalization, analysis, and reporting. Nonetheless, it still has a few issues. For example, it creates a deployment phase that is the confirmation of an incident that has occurred. This phase is separated from the physical and digital investigation phase. However, in practice, it is difficult to confirm whether the investigation is physical or digital because the two are interrelated. Unless an initial investigation has been conducted in both physical and digital. Furthermore, this model does not clearly describe the investigation conducted, for example, the investigation was conducted either on the suspect or on the victim (Evans & French, 2009).

As it is understood that computers can play a variety of roles for example, for criminals it is used as a tool to commit crimes or as a support medium to commit physical crimes. For the victim, it is used as a tool to store all the information that can be used by criminals without realizing it. This is where investigations should be done carefully and thoroughly to ensure that the evidence obtained is accurate and adequate (Hitchcock et al., 2016).

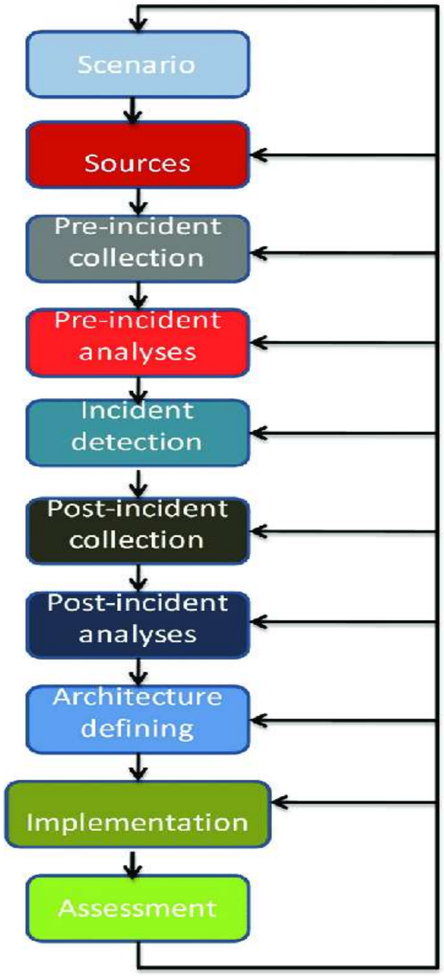

Figure 1 - Components of Digital Forensic Readiness Model

Montanari et. Al (Montasari, 2016a) has proposed a model that is called Integrated Computer Forensics Investigation Process Model (ICFIPM) for Computer Crime Investigations that have eight phases including readiness, identification, incident response, collection, examination, analysis, presentation and incident closure. This model has a generalized method that can be applied by non-technical observers. Dokko (Dokko, 2019) has developed a model: A Digital Forensic Investigation and Verification Model for Industrial Espionage that consists of six stages which are 1) file reduction, 2) file classification, 3) crime feature identification, 4) evidence mapping, 5)evidence sufficiency verification, and finally, 6) documentations.

The model emphasized on characterizing crime features and patterns in industrial espionage. As a result of studies that have been conducted on digital forensic investigation models that have been developed previously, there are several issues that can be discussed. Most of the models that have been proposed are common models with almost identical processes. Because these models are general in nature, investigations covering a wide range of current issues and challenges cannot be met by most of these models (Montasari, 2016b).

Obviously, this study shows that there are gaps to be filled to produce a standard model that can be used in an investigation.

3. PROPOSED MODEL

A comprehensive literature review on digital forensic investigation methods and frameworks was carried out. We discovered that, while various digital forensic investigation models have previously been established, the majority of them have relatively similar methods with no standard and consistent model, simply sets of processes and tools. A model was suggested to give a solution in the digital forensic investigation including occurrences in online social networks.

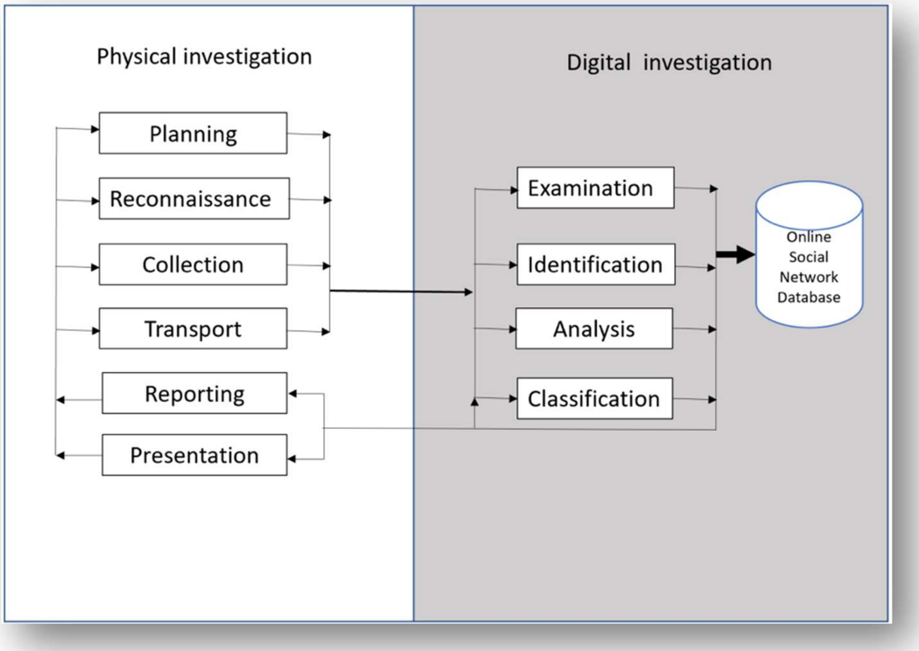

Figure 2 – Proposed Model

3. INVESTIGATIONS

Physical Investigation

The physical investigation is made up of processes that take place before and after the inquiry. The physical investigation entailed a series of procedures that occur in the physical phase of an inquiry. (Zainudin et al., 2021) have stressed the importance of the physical investigation process, which is basically the start of a digital inquiry where actual artifacts and evidence are obtained. To ensure that all essential steps are understood and acknowledged, all procedures are carried out in physical portions.

Digital Investigation

Digital forensics is a vital part of an overall incident response strategy. As such, it should be addressed by the organization through its policies, procedures, budgets, and personnel. All applicable policies and procedures should be drafted in such a way that it maximizes the effectiveness of the digital forensic process. Specific policies should be drafted covering digital forensic procedures and concerns. there are four activities required which are identification, searching, filtering and classifying

4. CONCLUSION AND FUTURE WORK

This study discusses the development of a digital forensic investigation methodology. We defined digital forensics and discussed existing digital forensics investigation methodologies and frameworks. There are numerous instruments accessible for general inquiry (e.g., hard disc analysis) since they are created in accordance with general investigatory requirements. However, these technologies are insufficient for conducting investigations since they lack specialized features. To solve these restrictions, a paradigm for conducting digital forensic investigations must be devised. As a result, this model has been proposed to meet the essential requirements. To solve these restrictions, a paradigm for conducting digital forensic investigations must be devised. As a result, this model has been proposed to meet the essential requirements. Because this is a redesigned model, there are additional tasks that must be completed, such as expert verification and technical analysis.

REFERENCES

1. Carrier, B., & Spafford, E. (2004). An event-based digital forensic investigation framework. *Digital Forensic Research Workshop*, 1–12. Retrieved from http://www.digital-evidence.org/papers/dfrws_event.pdf
2. Elyas, M., Maynard, S. B., Ahmad, A., & Lonie, A. (2014). Towards a systemic framework for digital forensic readiness. *Journal of Computer Information Systems*, *54*(3), 97–105. https://doi.org/10.1080/08874417.2014.11645708
3. Fagbola, F. I., & Venter, H. (2022). Smart Digital Forensic Readiness Model for Shadow IoT Devices. *Applied Sciences (Switzerland)*, *12*(2). https://doi.org/10.3390/app12020730
4. Forrester, J., & Irwin, B. (n.d.). a Digital Forensic Investigative Model for Business .... *Citeseer*, 1–12. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.107.434&rep=rep1&type=pdf
5. Hossain, M., Karim, Y., & Hasan, R. (2018). FIF-IoT: A forensic investigation framework for IoT using a public digital ledger. *Proceedings - 2018 IEEE International Congress on Internet of Things, ICIOT 2018 - Part of the 2018 IEEE World Congress on Services*, (February 2019), 33–40. https://doi.org/10.1109/ICIOT.2018.00012
6. Hughes, N., Ziemak, E., Martinez, C., & Stout, P. (2022). Toward a cost–benefit analysis of quality programs in digital forensic laboratories in the United States. *WIREs Forensic Science*, *4*(1), 1–15. https://doi.org/10.1002/wfs2.1422
7. Ishikawa, K. (2016). Outbreaks and control measures of PED in Japan. *Japanese Journal of Veterinary Research*, *64*, S33–S34. https://doi.org/10.14943/jjvr.64.suppl.s33

8. Kebande, V. R., & Choo, K. R. (2022). Finite state machine for cloud forensic readiness as a service (CFRaaS) events . *Security and Privacy*, *5*(1), 1–10. https://doi.org/10.1002/spy2.182
9. Kebande, V. R., & Ray, I. (2016). A generic digital forensic investigation framework for Internet of Things (IoT). *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, 356–362. https://doi.org/10.1109/FiCloud.2016.57
10. Lin, X. (2018). *Introductory Computer Forensics*. *Introductory Computer Forensics*. https://doi.org/10.1007/978-3-030-00581-8
11. Lutui, P. R. (2021). Critically Examine the Readiness of Tonga ' s Legislative Framework for e-Crimes, (Llm).
12. Maras, M. (2015). *Computer forensics: Cybercriminals, laws, and evidence 2nd edition*. Jones & Bartlett Learning.
13. Nelson, B., Phillips, A., & Steuart, C. (2019). *GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS INFORMATION SECURITY Sixth Edition*. Retrieved from www.cengage.com.
14. Prakash, V., Williams, A., Garg, L., Savaglio, C., & Bawa, S. (2021). Cloud and edge computing-based computer forensics: Challenges and open problems. *Electronics (Switzerland)*, *10*(11), 1–42. https://doi.org/10.3390/electronics10111229
15. Sudyana, D. (2019). Analysis and Evaluation Digital Forensic Investigation Framework Using Iso 27037:2012. *International Journal of Cyber-Security and Digital Forensics*, *8*(1), 1–14. https://doi.org/10.17781/p002464
16. Zainudin, N. 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. *Proceedings of the International Conference on Industrial Engineering and Operations Management*, 5338–5348.