ZULFAQAR Journal of Defence Science, Engineering & Technology
e-ISSN: 2773-5281
Vol. 6, Issue 2 (2023)
DOI: https://doi.org/10.58247/jdset-2023-0602-19
Journal homepage: https://zulfaqarjdset.upnm.edu.my

PRELIMINARY STUDY: DIGITAL FORENSIC PROCESS MODEL FOR DEFENSE AND SECURITY SECTORS

Syarifah Bahiyah Rahayu[a,b*], Sharudin Boriak[c], Afiqah M. Azahari[a,b]

[a] Centre of Cybersecurity, National Defence University of Malaysia Sungai Besi Camp, 57000 Kuala Lumpur, Malaysia
[b] Department of Defence Science, Faculty of Science and Defence Technology, National Defence University of Malaysia, Sungai Besi Camp, 57000 Kuala Lumpur, Malaysia
[c] WMG, International Manufacturing Centre, University of Warwick, Coventry, CV4 7AL, United Kingdom

ARTICLE INFO

ARTICLE HISTORY
Received: 05-05-2023
Revised: 10-07-2023
Accepted: 01-10-2023
Published: 31-12-2023

KEYWORDS
Digital forensic
Defence and security
Model
Web attack

ABSTRACT

Digital forensics has become an important part of legal proceedings by providing digital evidence. As more information could be extracted from a website, the number of criminal activities involving web applications increases and it becomes more crucial for digital investigators to conduct analysis properly. Therefore, a suitable process model is highly needed to ease the operation of investigating web attack incidents. This study proposes a digital forensic process model for web attack investigations in the defence and security sector. A total of twelve (12) existing digital forensic process models have been evaluated to develop a new digital forensic process model, which is applicable to be used in Malaysia's defence and security sector. The research methodology that is being utilized to develop the model is a qualitative method to gather more data to support the new digital forensic process model for the defence and security sector. The new model is expected to benefit the sectors in processing web attack incidents and ensure that the phases taken in the process can be used to find evidence and assist web attack investigation for reference in daily operations.

1.0 INTRODUCTION

Cyber threats are waiting to manipulate device or system flaws in cyberspace to jeopardize defence integrity, availability, and confidentiality. On a national level, cyber threats will target sensitive infrastructure flaws such as electricity and transport, and communications and severely undermine the combat operation's effectiveness, as infrastructure is crucial in supporting military operations [1]. The attacker always has secret agendas or motivations to ensure an effective attack on the defence sector by spending time, effort, and resources. The main goal is intended to access information that is owned or maintained in the target network. Besides, an attacker can do espionage by tracking target activities and stealing information that could jeopardize defence security. The most dangerous is sabotage when the purpose is to destroy, defame or blackmail its target. A famous case in the military is the Stuxnet worm which involves a long espionage operation and was silently launched to destroy Iran's nuclear plant. The operation uses physical devices containing infected Stuxnet worm and carried by an unsuspecting carrier. It assists in dispersing and transferring the arms to the safe facility and Siemens computers on flash drives [2]. The complexity of the Stuxnext makes most security experts believe that the worm was developed by a nation-state, however, no country has been able to take responsibility for the attack. As one of the popular worms that target industrial control systems, this demonstrates that cyber-attack could lead to real-world consequences. In an age where web applications have continued evolving, the lesson learned from the Stuxnet incident is still relevant. Another highly sophisticated threat, Advanced Persistent Threat (APT), is an example believed as a nation-state attacker operation to compromise their target [3].

*Corresponding Author | Rahayu, S. B. | syarifahbahiyah@upnm.edu.my

SQL injection, broken authentication, cross-site scripting, insecure direct object references, and vulnerability misconfiguration are among the most prevalent vulnerabilities revealed by an intruder in the OWASP Top Ten for the year 2020 [4]. In 2020, Cyber Security Malaysia presented statistics regarding incidents involving web attacks, reporting that there were more than 10,000 such incidents during the year [5]. Organizations are facing impact and loss in terms of monetary and reputation. To overcome and face the risk of web attacks, organizations have started creating a digital forensic team to increase the resilience of the organization's technology infrastructure and increase the readiness of cyber security investigation in the case of an incident. Looking at Malaysia's defence and security sector, numerous web attacks have been reported since 2013, and the trend is increasing every year. Most of the cases involve web defacement and DDOS attacks. Sensitive issues within neighbouring countries and sponsor attackers believe the main reason behind the rise of web attacks. For example, Indonesian hackers' web attack activity on Malaysian government websites increased, including the military website, because of the national flag issue in 2017 [6]. In addition, [7] reported through The Star that the Dark Web portal uploaded leaked Royal Malaysian Navy documents to the internet. The records contain sensitive information about troop strength, detail of charges in the Navy, naval exam requirements, exercise, and equipment. The source of information remains in the investigation but believed a hack of the military personnel email account. However, The Royal Malaysian Navy stated that the leaked documents were obsolete and did not disrupt naval readiness or operation. Moreover, [8] reported that North Korea hacks Israeli defence companies with fake employment to collect confidential data. The hackers are suspected to be part of the Lazarus community, linked by US intelligence to North Korea. Using a previous approach in 2019, hackers created fake LinkedIn profiles that are characterized by CEOs and high-ranking officers in global corporations to sell phony work. Attackers try to hack the machines of workers, infiltrate their networks, and collect confidential safety documents. These tactics are also used by Iran hackers to close with an individual who might hold sensitive defence information, as published by The Business of Federal Technology [9]. The latest study from the Centre of Strategic and International Studies in Washington DC, which record a list of cyber incidents, includes web attacks worldwide since 2006. They focus on government agencies, defences, high-tech companies, and economic crime that capture loss in millions. Among the list is Malaysia being hacked or espionage by other countries [10].

However, most digital forensic laboratory in Malaysia's defence and security sector is relatively growing. There is no systematic digital forensics process model in the laboratory that stresses the digital forensics process to be practiced by the staff. Besides, staff and the process are still adapting to day-to-day operations. Consequently, some staff are hesitant to simplify the investigation when dealing with facts because the higher management needed the inquiry to be reviewed within a short period. In addition to securing the evidence, digital forensic teams should follow a solid legal foundation [11]. Besides, it is essential to protect the confidentiality of investigation records and to enforce a transparent chain of custody [12]. Digital forensics should follow a set of structured processes instead of a single process in every investigation [13]. The National Institute of Standards and Technology (NIST) stresses the legal viewpoint in terms of procedure, including identifying, collecting, examining, and analysing digital media or digitally stored data. Therefore, this paper is proposing a new digital forensic process model for web attack incidents in Malaysia's defence and security. The objectives are i) to identify existing digital forensic process models for conducting a forensic investigation and ii) to propose a digital forensic process model for web attack investigations in the Malaysia defence and security sectors.

2.0 DIGITAL FORENSIC PROCESS MODEL

In this paper, the term ‘digital evidence’ refers to an exhibit of digital devices, media, or digitally stored data, while the term ‘forensic’ is an act of investigation. Digital forensics is considered a branch of forensic sciences that has been described in numerous ways by various researchers. It is also known as forensic computing or computer forensics [14]. Few researchers have defined digital forensics in the past few years. For instance, digital forensics as using scientific methods and proven techniques to obtain digital evidence [15]. The process aims to support the reconstruction of interrupted scheduled operations from illegal activities or help unauthorized acts. In which the definition is supported by [16] with an emphasis on digital forensics practices and tools. Both elements are essential in the investigation of the cases to produce the evidence. This study [17] suggests an additional stage to collect evidence from a computer processor or digital storage facility using the advancement of technologies. Besides, the researcher emphasizes evidence credibility, which includes confidentiality, integrity, and authenticity of digital devices or computer systems. These definitions have similar views on the critical element of digital forensics that science and technology usage is vital in examining or collecting digital evidence. The use of

*Corresponding Author | Rahayu, S. B. | syarifahbahiyah@upnm.edu.my

scientific methods combined with current technology enables the investigator to find the evidence to solve the case. Criminal has changed their method from conventional crime to digital crime such as hacking, fraud, and online scams. Thus, another study [18] defines digital forensics as a process of using computer science in web attack investigation procedures. Most digital forensics nowadays are mainly used for computer-related crime investigations. The selected investigation process must be accurate, predefined, and proven. It applies both scientific and systematic validated and derived approaches to digital media or digitally stored data.

Previous studies show digital forensic teams following at least four fundamental digital forensic phases during web attack investigation, which are collection, examination, analysis, and reporting. The US Department of Justice published a guideline to help responders deal with electronic crimes at the crime scene [19]. The guideline emphasizes experience and advances the skilled responder or technical expertise to utilize four processes: collection, examination, analysis, and reporting. According to [13], digital forensics should apply to a group of processes instead of a single process in every investigation. While, [20] states that the investigation process should include the necessary forensic investigation procedures consisting of preparation, investigation, and presentation. This method should be considered and measured to decide each analysis's criteria [21]. Various digital forensic method models have been established over time to aid digital forensic investigations. The majority of these digital forensic process models are developed to fix deficiencies in modern processes. It has been extended to digital forensics' reach. The purpose of the digital forensic process model is to assist digital forensic teams during web attack investigations. Thus, the process model should be systematic, practical, and suitable to be performed and followed during the investigation. This paper reviewed twelve (12) existing digital forensic process models. Overall, the existing digital forensic process models aim to improve a traditional methodology for a specific application. Table 1 summarizes the benefits and limitations of the existing digital forensic process model.

There have been several efforts to establish a digital forensic process model, but none has been widely adopted. This may be because all method models were created within a particular context, such as law enforcement. Therefore, the digital forensic process models are inapplicable to be used in other cases, such as incident response. None of them has been built and tested for any specific web attack incident, especially for Malaysia's defence and security sector. We believe that the digital forensic process model must be applicable for daily operation in the Malaysia defence and security sector, and easily adopted by the digital forensic team. Moreover, the proposed digital forensic process model should help the digital forensic team capture vital digital exhibits for legal prosecutions such as tracking cybercriminal suspects, who compromise the web or network. From the terminology used in the 12 selected digital forensic process models, we classified the terms and their process according to their shared representation of each phase, focusing on common elements and the underlying meaning within each stage. We start grouping the first phase under the 'Readiness / Preparation / Authorization / Planning' phase. According to [22], readiness means people training, tools testing, and equipment configuration before the investigation started. Another study state that their model emphasizes readiness definition on a matrix to gather case intelligence about "enemy" and "friendly" situation before arriving at a crime scene in the planning phase. The Freilling and Schwittay model's pre-incident preparation phase focuses on organizing organizations and people at the crime scene [23]. We discovered that in other models, this phase is consistently identified as the initial stage, reflecting a commonality across different approaches.

Table 1. Benefits and limitations of existing digital forensic process models

No.	Models	Benefit	Limitation	Ref
1.	Event-Based Digital Forensics Investigation Framework	Flexible to all investigation	The old model and not keep up with current technologies	[22]
2.	Guide to Integrating Forensic Techniques into Incident Response	Guideline for the first responder in the crime scene	Not for law enforcement	[19]
3.	Computer Forensics Field Triage Process Model	Successful implementation in real case	The investigator is a forensic specialist and model usage limit to a specific case	[24]
4.	A Common Process Model for Incident Response and	Unified Computer Forensic and Incident Response Model	Full-scale investigation requires many resources	[23]

*Corresponding Author | Rahayu, S. B. | syarifahbahiyah@upnm.edu.my

No.	Models	Benefit	Limitation	Ref
	Computer Forensics			
5.	Integrated Computer Forensic Investigation Model Based on Malaysian Standards	The focus of fragile evidence and data acquisition	Important phases like collection, examination, and presentation do not exist	[25]
6.	Generic Computer Forensic Investigation Model	The phase can backtrack to the previous phase	No proof in real-world case	[26]
7.	A Systematic Digital Forensic Investigation Model	The most comprehensive model with the looping phase	Limited to cybercrime and computer fraud case. No proof in a real-world case.	[27]
8.	Harmonized Digital Forensic Investigation Process Model	A multitier model with parallel action	The model has not been tested in real world	[28]
9.	Integrated Digital Forensic Process Model	Incorporates current phases / standardizes terminology	No evidence model function in any case	[29]
10.	Integrated Computer Forensics Investigation Process Model	Incorporates terminology and activities into the model	No proof that the model tested	[30]
11.	Analysis of Digital Forensic Investigation Models	Focus on data acquisition, fragile evidence & examination	No explanation of each phase and how to apply the model in the investigation	[31] [31]
12.	Behavioural Digital Forensics Model	Emphasize behaviour analysis in the model, and the model is proven in a real case	Limited expertise in both computer forensic and behavioural science	[32]

The subsequent phase includes 'Incident Response' and 'Securing the Scene'. Both phases are categorized under the same group as this activity involves the first responder. Previous researchers [33] state that this stage is mainly concerned with protecting the crime scene from illegal entry and preventing contamination of the evidence. The first responders would then determine and validate the incident before reporting it to the relevant body, such as corporate administration or the police [28]. Others also mention incident response and investigator action at the crime scene [29, 34]. The third phase is grouped as the 'Detection / Identification' phase which is related to detecting the incident and identifying what type of incident. We determined that most of the models include this phase. Researchers [29, 34-35], are among those who have integrated detection and identification into a single phase within their models.

We also determined that every model studied incorporates an 'Analysis / Hypothesis' phase. The use of a hypothesis within the forensic incident model may improve the investigation, enhancing the likelihood of uncovering the underlying causes of the cyber incident. Therefore, we have classified this essential element as a singular phase across all models.

In the following phase, 'Reporting/Proof & Defence/Presentation' is categorized under the same group. This phase involved presenting the finding either by reporting it, proof and defence process, or presenting it. In research [34] state that they combine all these activities in one phase dubbed as 'Presentation'. And this was supported by the model presented by [35-36]. We observed that most of the models studied incorporate the process of documenting the findings of the investigation. However, the terminology used to describe this aspect varies across different models [36]. The final phase is referred to as 'Closure/Archive.' This phase encompasses the procedures for closing the case, securely storing evidence, and preparing a report that includes lessons learned from the incident. Although [36] have labelled this phase as 'Post Process,' the actions and procedures they describe align closely with what is generally understood as the 'Closure/Archive' phase.

Table 2. Gap analysis of existing digital forensic process models

Phase	Existing Model	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6	Model 7	Model 8	Model 9	Model 10	Model 11	Model 12

*Corresponding Author | Rahayu, S. B. | syarifahbahiyah@upnm.edu.my

Phase / Existing Model	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6	Model 7	Model 8	Model 9	Model 10	Model 11	Model 12
Readiness / Preparation/ Authorization / Planning	X		X	X	X	X	X	X	X	X	X	
Incident Response / Securing the Scene							X	X	X	X		
Triage			X									
Detection / Identification	X			X	X	X		X	X	X	X	X
Collection	X	X	X			X	X	X	X	X	X	X
Examination	X	X	X	X			X		X	X	X	X
Reconstruction	X								X		X	
Communicate									X			
Preservation	X					X	X		X			
Transportation					X			X	X		X	
Storage					X			X	X		X	
Analysis / Hypothesis	X	X	X	X	X	X	X	X	X	X	X	X
Reporting / Proof & Defence/ Presentation	X	X		X		X	X	X	X	X	X	X
Review						X	X		X			
Closure / Archive					X	X				X	X	

Through the classification and analysis of terms, focusing on their shared representation across each phase, we have compiled Table 2. This table presents the gap analysis, highlighting the availability and absence of specific terms and procedures within each model studied.

3.0 RESEARCH METHODOLOGY

In this section, we describe the step-by-step process used to develop a new digital forensic process model, as shown in Figure 1. First, we carefully examined twelve (12) existing digital forensic process models, outlining both the advantages and disadvantages of each, as summarized in Table 1. Next, we grouped and analysed these models to find out what they had in common and how they differed. Table 2 presents the key findings from this analysis, giving us a clear understanding of what was included and what was missing in the current models. This thorough examination served as the foundation for creating the new digital forensic process model. Using the results gathered from examining the existing models, we designed a new digital forensic process model, shown in Figure 1. This model brings together the most effective parts of the models we studied. To test and show how useful this newly developed model is, we arranged an interview session to see how it might work within Malaysia's defence and security sectors. We conduct interviews with personnel from the Malaysia Armed Forces (MAF), Ministry of Défense Malaysia (MinDef), Cyber Security Malaysia (CSM), and Royal Malaysian Police (RMP). These subject-matter experts (SMEs), known for their skills in digital forensics and cybersecurity, volunteered to share their thoughts. Table 3 provides a summary of the backgrounds and expertise of these interviewed SMEs.

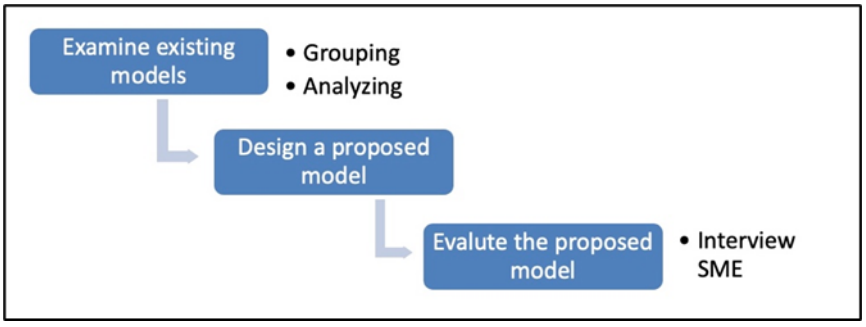

Figure 1. Research methodology

*Corresponding Author | Rahayu, S. B. | syarifahbahiyah@upnm.edu.my

This approach helped us not only to create a new digital forensic process model but also to make sure that the model was based on practical, real-world needs and expert opinions. This increases the new framework, its relevance, and its potential usefulness in the field.

Table 3. Summary of SME profiles

Respondent Number	Designation	Experience
R1	Staff Officer 1 Information System	Eighteen years' service in Royal Military Navy (RMN) and experience in IT system administration.
R2	Staff Officer 2 Cyber	Fifteen years' service in the Royal Military Air Force (RMAF). Hold various positions related to network security in MAF HQ and RMAF.
R3	Staff Officer 2 Operation A	Twenty-one years' service in the Army. Experiences in handling cybersecurity in MAF HQ and MinDef.
R4	Staff Officer 2 Forensic	Eleven years' service in RMAF. Involvement in cybersecurity or digital forensics from the first year of services.
R5	Staff Officer 2 IT	Eighteen years of services in RMN, including three years of experience in cybersecurity.
R6	Head of IT Security	Sixteen years of work as IT Officer and responsible for managing cybersecurity in MinDef since 2015.
R7	Head of Digital Forensic	Testified digital forensics subject-matter expert and experience almost fifteen years in digital forensics. He is a credited Assessor of the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB)
R8	Investigator Officer	Thirteen years' service in RMP and experience in cyber commercial crime investigation

4.0 PROPOSED DIGITAL FORENSIC MODEL FOR WEB ATTACK

The proposed digital forensic process model is built with a high-level categorization to allow for generalization across phases. The steps are designed in a logical order to give a quick rundown of the various phases of the investigation. Based on the reviews of existing digital forensic process models, a proposed digital forensic process model for web attacks is developed. There are six phases frequently appeared in each model. These phases will be used to design a new digital forensic process model for Malaysia's defence and security sector. The six phases are Readiness, Detection, Collection, Examination, Analysis, and Presentation. Figure 2 illustrates the proposed digital forensic process model. In the proposed digital forensic process model, Threat Intelligence is included to support the investigation of web attacks during the Readiness and Detection phases. Threat analysis is detailed information on potential risks that can help organizations defend themselves from the kinds of attacks that can do the most harm [37]. Threat intelligence's primary goal is to help organizations gain the dangers of the most common and dangerous external attacks, such as advanced persistent threats (APTs) and zero-day exploits. Thus, threat intelligence is information analysed regarding malicious actors' purpose, opportunity, and capabilities concerning possible or existing threats that pose a threat to an organization. It refers to the status of cyber threat intelligence after it has been gathered, measured in terms of source and reliability, coordinated, reviewed using comprehensive and systematic tradecraft methods, and optimized by security analysts.

The proposed digital forensic process model in web attack investigation is organized in systematic and practical coordination with threat intelligence support. Threat intelligence depends on people, processes, and technology.

*Corresponding Author | Rahayu, S. B. | syarifahbahiyah@upnm.edu.my

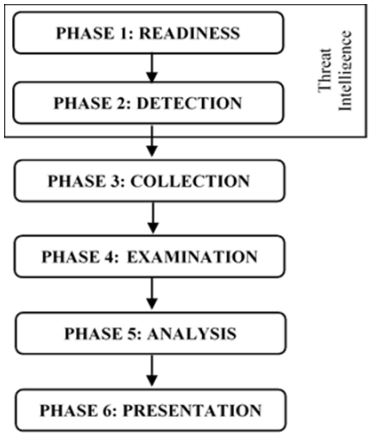

Figure 2. Proposed digital forensic process model

The proposed digital forensic process model starts with the Readiness phase. This is a phase that includes people, process, and technology preparation before investigation. According to [29], the phase maximizes the organization's readiness to use digital evidence while minimizing an investigation's costs. The organization needs to improve the system and prepare staff for the digital forensic investigation of web attacks. In terms of procedure, the organization should have transparent digital evidence handling process, chain of custody, awareness of the seizing procedure, or appropriate legal advice in digital forensic investigation. Threat intelligence supports the phase by using an open-source database of the threat in web attacks to study the threat behaviour and information. Then, the next phase is the Detection phase. The Detection phase is to detect and alert any threats using a system. Based on Carrier and Spafford models, the Detection phase is where the victim or another party detects the incident or a digital crime and the investigators are alerted [22]. Detection is required to help determine the authorship of the evidence files and artifacts contained in the units. Detection phase embedded threat intelligence to detect any threat and show the alert using the system.

During the Collection phase, the digital forensic team must classify, mark, register, and obtain data from the relevant source while maintaining data integrity by following the proper procedure as suggested by [12]. The investigator collects potential digital evidence, seizes the items, and supports the digital evidence's validity during a web attack investigation. The subsequent phase is the Examination. The Examination phase is the process of using digital forensic tools to search for evidence related to the investigation. One of the methods is to render digital evidence visible or converts the details into a human-readable format [29]. The later step, the Analysis phase, is to analyse digital exhibits and evidence. In this phase, the aim is to derive useful information that addresses the questions to construct a hypothesis. The last phase is Presentation. The Presentation step consists of putting together a concise written report on the whole investigative method, implementation hypothesis, and research findings. Other information includes legal processes, forensic tools, effective protocols, and guidelines to enhance the forensic process.

5.0 DISCUSSION

Some experts recently have experienced web attack incidents. Feedback has been summarized to support the proposed digital forensic process model for web attack investigation. Most experts agree that web defacement followed by web phishing attacks frequently happen within their organization. The attack was categorized from 'Medium' to 'High' and determined by the impact of the attack on the organization. Each attack handled by the investigators needs to be reported and presented to their high authority. Currently, three experts implement a digital forensic process model as their guide toward any digital forensic investigation. However, most of the expert organizations do not have any infrastructure to perform digital forensic investigation and do not implement any digital forensic process models. Furthermore, most experts agree that the current process model must be reviewed due to the fast-changing world of technology. Investigators must have knowledge and readiness to be established in terms of administrative, technical, and physical foundations to effectively support all phases in the digital forensic process model. Also, experts mention that expertise in people, processes, and technology matters during the first phase of digital forensic investigation. Two experts remark that getting assistance from threat intelligence tools helps to give some views of the web attack at the beginning of the incident. Based

*Corresponding Author | Rahayu, S. B. | syarifahbahiyah@upnm.edu.my

on the interviews conducted, shows that a web attack could impact an organization's reputation and operation as most of the experts understand the need for digital forensic investigation after any web attack. The experts agree that they need expertise in people, processes, and technology while handling any digital forensic investigation. Moreover, they also agree that the current process model needs to be improved following the complex and unpredictable current web attack technology.

The experts stress the importance of aligning the proposed process model with industry regulations and standards, simplifying compliance, and showcasing organizations' commitment to cybersecurity. They also highlight the benefits of integrating this improved digital forensic process model with incident response protocols, facilitating a seamless transition from identifying attacks to enacting effective containment and recovery strategies. Additionally, the experts show enthusiasm for the model's integration of a continuous improvement feedback loop, allowing it to refine methodologies based on investigation insights. Overall, they see the enhanced digital forensic process model as a valuable tool in combating web attacks, enhancing cybersecurity practices, and safeguarding digital landscapes.

6.0 CONCLUSION

The introduction of the proposed digital forensic process model holds significant promise for guiding Malaysia's defence and security sector in effectively investigating web attack incidents. This study has meticulously outlined six distinct phases that collectively contribute to the advancement of digital forensics within Malaysia's defence and security landscape. These phases, namely Readiness, Detection, Collection, Examination, Analysis, and Presentation, form a comprehensive framework for handling web attack incidents. Notably, the integration of Threat Intelligence further enhances the model's effectiveness during the readiness and detection phases, reinforcing the sector's preparedness to counter evolving cyber threats. To validate the practical applicability of the proposed model, comprehensive interviews were conducted, corresponding to each of the defined phases. This empirical approach ensures that real-world insights from experts are incorporated, lending credibility and practicality to the model. The anticipated advantages of adopting this model are multifield. The emphasis on preserved proof confidentiality ensures the integrity of evidence throughout the investigative process. By optimizing the inquiry time, the model facilitates quicker resolutions, minimizing potential damage caused by web attacks. Additionally, the meticulous attention to securing and adhering to the chain of custody standards enhances the admissibility of findings in legal proceedings, bolstering the sector's credibility. As a forward-looking initiative, the proposed digital forensic process model is composed for further validation through a rigorous testing process involving subject matter experts possessing robust backgrounds in defence and security. This validation phase aims to demonstrate the model's efficacy in real-world scenarios, ensuring its seamless integration into Malaysia's defence and security operations. By subjecting the model to practical testing within a controlled environment, the study seeks to refine its facets and identify potential areas of improvement. This validation process, rooted in expert input and hands-on investigation of web attack incidents, will ultimately cement the model's role as a pivotal asset in fortifying Malaysia's cybersecurity posture.

7.0 ACKNOWLEDGEMENT

The authors would like to thank the National Defence University of Malaysia for its moral support. Furthermore, the authors acknowledge support and cooperation from the Malaysia Armed Forces (MAF), Ministry of Defence Malaysia (MinDef), Cyber Security Malaysia (CSM), and Royal Malaysian Police (RMP).

List of Reference

[1] Zimba, A., Wang, Z., & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. Ict Express, 4(1), 14-18.
[2] Kushner, D. (2013). The real story of stuxnet. ieee Spectrum, 50(3), 48-53.
[3] Pham, L. H. (2020). Foundations of Adaptive Cyber Defense against Advanced Persistent Threats (Doctoral dissertation, George Mason University).
[4] Fredj, O. B., Cheikhrouhou, O., Krichen, M., Hamam, H., & Derhab, A. (2021). An OWASP top ten driven survey on web application protection methods. In Risks and Security of Internet and Systems: 15th International Conference, CRiSIS 2020, Paris, France, November 4–6, 2020, Revised Selected Papers 15 (pp. 235-252). Springer International Publishing.
[5] binti Mohamed, D. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the

*Corresponding Author | Rahayu, S. B. | syarifahbahiyah@upnm.edu.my

cyberlaws and the traditional laws. Computer Law & Security Review, 29(1), 66-76.
[6] Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2011). Access contested: security, identity, and resistance in Asian cyberspace. mit Press.
[7] Weimann, G. (2016). Going dark: Terrorism on the dark web. Studies in Conflict & Terrorism, 39(3), 195-206.
[8] Ayyub, R. (2020). Israel Says It Thwarted Foreign Cyber Attack on Defence Industry.
[9] Hyla, E. J. (2018). Corporate cybersecurity: the international threat to private networks and how regulations can mitigate it. Vand. J. Ent. & Tech. L., 21, 309.
[10] Smith, S. E. (2021). An Analysis of Significant Cyber Incidents and the Impact on the Past, Present, and Future.
[11] Eloff, J., Bihina Bella, M., Eloff, J., & Bella, M. B. (2018). A methodology for investigating software failures using digital forensics and near-miss analysis. Software Failure Investigation: A Near-Miss Analysis Approach, 39-56.
[12] Kent, K., Chevalier, S., & Grance, T. (2006). Guide to integrating forensic techniques into incident. Tech. Rep. 800-86.
[13] Pollitt, M. (2004, August). A framework for digital forensic science. In Digital Forensics Research Workshop (DFRWS).
[14] McKemmish, R. (2008). When is digital evidence forensically sound? (pp. 3-15). Springer US.
[15] Palmer, G. (2001, August). A road map for digital forensic research. In First digital forensic research workshop, utica, new york (pp. 27-30).
[16] Willassen, S. Y., & Mjolsnes, S. F. (2005). Digital forensic research. Telektronikk, 101(1), 92.
[17] Khan, A. A., Shaikh, A. A., Laghari, A. A., Dootio, M. A., Rind, M. M., & Awan, S. A. (2022). Digital forensics and cyber forensics investigation: security challenges, limitations, open issues, and future direction. International Journal of Electronic Security and Digital Forensics, 14(2), 124-150.
[18] Jones, A., & Vidalis, S. (2019). Rethinking digital forensics. Annals of Emerging Technologies in Computing (AETiC), Print ISSN, 2516-0281.
[19] Guide, N. I. J. (2001). A Guide for First Responders. National Institute of Justice, 4.
[20] Pladna, B. (2008). Computer Forensics Procedures, Tools, and Digital Evidence Bags: What They Are and Who Should Use Them. East Carolina University, East Carolina.
[21] Kubi, A. K., Saleem, S., & Popov, O. (2011, October). Evaluation of some tools for extracting e-evidence from mobile devices. In 2011 5th International Conference on Application of Information and Communication Technologies (AICT) (pp. 1-6). IEEE.
[22] Carrier, B., & Spafford, E. (2004). An event-based digital forensic investigation framework. Digital Investigation.
[23] Freiling, F. C., & Schwittay, B. (2007). A common process model for incident response and computer forensics.
[24] Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. Journal of Digital Forensics, Security and Law, 1(2), 2.
[25] Perumal, S., & Norwawi, N. M. (2010). Integrated computer forensic investigation model based on Malaysian standards. International Journal of Electronic Security and Digital Forensics, 3(2), 108-119.
[26] Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. International Journal of Computer Science & Information Technology, 3(3), 17-31.
[27] Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. International Journal of Computer Science and Security (IJCSS), 5(1), 118-131.
[28] Valjarevic A., & Venter, H. S., "Harmonised Digital Forensic Investigation Process Model," in 2012 Information Security for South Africa - Proceedings of the ISSA 2012 Conference, 2012.
[29] Kohn, M. D., Eloff, M. M., & Eloff, J. H. (2013). Integrated digital forensic process model. Computers & Security, 38, 103-115.
[30] Hewling, M. O. (2013). Digital forensics: an integrated approach for the investigation of cyber/computer related crimes.
[31] Mir, S. S., Shoaib, U., & Sarfraz, M. S. (2016). Analysis of digital forensic investigation models. Int. J. Comput. Sci. Inform. Secur, 14(11).
[32] Al Mutawa, N., Bryce, J., Franqueira, V. N., Marrington, A., & Read, J. C. (2019). Behavioural digital forensics model: Embedding behavioural evidence analysis into the investigation of digital crimes. Digital Investigation, 28, 70-82.
[33] Agarwal, R., & Kothari, S. (2015). Review of digital forensic investigation frameworks. In Information science and applications (pp. 561-571). Springer Berlin Heidelberg.
[34] Montasari, R., Peltola, P., & Evans, D. (2015). Integrated computer forensics investigation process

*Corresponding Author | Rahayu, S. B. | syarifahbahiyah@upnm.edu.my

model (ICFIPM) for computer crime investigations. In Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security: 10th International Conference, ICGS3 2015, London, UK, September 15-17, 2015. Proceedings 10 (pp. 83-95). Springer International Publishing.

[35] Valjarevic, A., & Venter, H. S. (2012, August). Harmonised digital forensic investigation process model. In 2012 Information Security for South Africa (pp. 1-10). IEEE.

[36] Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. International Journal of Computer Science & Information Technology, 3(3), 17-31.

[37] Vandepeer, C. (2011). Rethinking threat: intelligence analysis, intentions, capabilities, and the challenge of non-state actors (Doctoral dissertation).

*Corresponding Author | Rahayu, S. B. | syarifahbahiyah@upnm.edu.my