ISSN 2278-3091
Volume 8, No.1.5, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse6081.53019.pdf
https://doi.org/10.30534/ijatcse/2019/6081.52019

# Comparative Study of Digital Forensic Investigation on Cyber Criminal

**Azhari Shouni Barkah[1,2], Siti Rahayu Selamat[3], Zaheera Zainal Abidin[4]**
[1]Department of Informatics, Faculty of Computer Science, Universitas AMIKOM Purwokerto, Purwokerto, Indonesia, azhari@amikompurwokerto.ac.id
[2]Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka, Malaysia
[3]Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka, Malaysia, sitirahayu@utem.edu.my
[4]Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka, Malaysia, zaheera@utem.edu.my

## ABSTRACT

Digital forensic investigation has undergone tremendous changes in the last decade from initial computers to current mobile devices and storage devices. The significance of digital forensics in the process of prosecuting digital criminals who use digital devices. The process of analysing digital forensic investigations requires a model or framework so that the investigation process can run in more detail and structure. As in previous studies, there is no digital forensic investigation that addresses one standard for all. The digital crimes have increased around the world and have resulted in being developed of survey models that can be escalade to find digital evidence. In some previous studies, there have been many discussions about models or frameworks in investigating a digital forensic case, and these models can be widely used. Some models discuss a detailed process, and some discuss a process in general, this can lead to digital forensic investigators having difficulty choosing the right model in investigating a case. The digital forensic investigation must be carried out effectively, efficiently and structured, with several significant steps that must be considered. Every step and phase must produce documentation that is important in understanding how the investigation process is built. The goal of this paper was to study and compare the digital forensic investigation model. The study also included interpretation and illustration of fundamental concepts used by the framework or model.

**Key words :** Digital Forensic Investigation, Framework, Model

## 1. INTRODUCTION

Digital forensics is now increasingly important with several vulnerable information security incidents and continues to highlight them. In digital forensics, there are two methods, namely static forensic and live forensic. Static forensic where to get the data from data that is stored permanently in a storage media device, in general, the hard drive. Live forensic requires data from a system that is running or volatile data that is usually Random Access Memory (RAM) or transit on the network [1]. Electronic evidence consists of information and data values stored or sent by the device [2]. Thus, Digital evidence is potential proof in the similarity meaning that evidence of fingerprint or DNA is potency evidence [3].

Regarding digital evidence, standard and formal processes are needed so that digital proof can be fulfilled in court. Forensic methods are important factors that support the investigation of crimes that are more effective and efficient in handling a case [4]. The models of digital forensic processes have been evolved by practician and examiner forensic investigative, based on their experience and skill, based on an ad hoc to achieve standardisation at the scene of violations. In the last decade, there have been several scientific research conducted to create a process model of a digital forensic investigation process. However, at present, there are no worldwide standards that formalise the process of digital forensic investigation, in spite of the fact that efforts to a standard process have begun in the International Standardization Organization (ISO) [5].

The digital forensics investigation focuses on the offence committed using a computer [6]. Regardless of how, in recent years, the area has been expanded to be composed of a variety of other digital appliance were digitally stored facts provided can be handled and utilized for various category of crimes [2]. Digital forensic investigations, from now on referred to as Digital forensics Investigations (DFI), are phases connecting information extracted and proof of digital to build correct details for evaluation by judicial institutions [6], [2]. Cohen [7] highlighted the necessity to construct accurate data as a result of investigations. DFI was bringing out as an investigation after the occurrence [8]. In this way, it is an alternate sort of examination "where logical methods and

modus operandi will permit results, in another word, digital proof to be acknowledged in court" [9].

Some models are given to be very detailed, and further may be too familiar. This may be somewhat awkward or even confusing, mainly for beginner investigators of forensic to take a valid or suitable investigation model [10]. The stage that is general in all procedure models are:

- Collection: At this stage evidence is collected
- Examination: Examination is based on the source of origin of the evidence.
- Analysis: Search or assessment based on inspection.
- Reporting: Conclusions from all stages.

This research began with a formal assessment of several existing models of digital forensic investigation, analysing existing models to identify strengths and some weaknesses inherent in these investigation models.

## 2. LITERATURE SURVEY

In this section, a model of digital forensic investigation and the framework that has been carried out by several researchers. The development of several digital forensic investigation models includes focusing on incident responses or investigations or emphasising certain phases or activities of investigation. Below is a brief description of the model development process.

According to the research of Ademu et al. [11], was proposed NADFM model. This research aimed at introducing an arranged and constant approach to digital forensic investigations. In improving the investigation procedures, new models have been presented to identify pursuits and help to refine the investigation process. This research additionally discusses available models that have been offered previously, such as SDFIM, IDIP, Forensic Process Model etc. Each model has different phases in conducting the digital investigation process. The proposed model has four stages derive from the location. The initial stage is composed of four-step, which include: preparation, identification, authorisation and communication. The next stage is composed of three-step, which include: collection, preservation and documentation. Thirdly stage also is composed of three-step, which include: examination, testing and exploration analysis and finally, the last stage is composed of the presentation step.

Another research from Yusoff [12], this research proposes a recent investigative model, namely the Generic Forensic Computer Investigation (GCFIM) model with five stages:

- Pre-Process: investigators do things related to work before conducting an investigation, such as preparing letters and official documents and also preparing tools for utilised.
- Acquisition & Preservation: At this stage, everything related data is taken, kept and prepared for the upcoming scene. At this stage, the investigator secures the evidence by copying and blocking the evidence and then storing it in a safe place.
- Analysis: this stage is the primary process in computer forensic investigations, namely a summary of the data that has been obtained in the previous step to be carried out to recognise the origin of crime, the motive of the offence and eventually find the fellow accountable for the crime.
- Presentation: this stage presents a presentation on the results that have been obtained. The result of this stage is to prove and/or deny the alleged crime.
- Post-Process: This stage is the final stage; both physical and digital evidence is stored in a safe place. The investigator reviews the process of investigation that has been carried out so that it can be used to improve the process of further investigation.

Other studies related to the forensic investigation model are Agarwal's research, et al. [9] proposed a new model based on the previous model. In his study conducting a comparison of disparate existing models. A systematic model of digital forensic procedures emerges based on the difference its. Primary of advantages the model has proposed is to make available for use a framework mechanism to be applied in countries based on technology. This model offers a systematic method to analyse cyber criminal by the technology used in each state.

Subsequent research on the digital forensic investigation model conducted by Al-fedaghi and Al-babtain [13] proposed a model without comparing the existing model. In this study, the model based on the proposed flow. This flow notifies the right direction and accuracy, where the evidence detached into distinct flow streams. The model proposed discusses the phase will help in dividing the flow. The stage includes: making, releasing, transferring, arriving, receiving, and processing.

Another research conducted by Kyei, et al. [14] discusses one of the significant disadvantages in the digital forensic investigation process that it does not place adequate stress on the potential for receipt of the proof gathered. Digital forensic investigations must attend to the standard of evidence and receipt of demands for successful prosecution. Hence, the techno-legitimate nature of the model has proposed, combined with the merger of best practices from previous models, produce it unique. This model is not a falls model, but it is recurrent to assist successful investigations and prosecutions. The results of this study are supposed to enhance the entire process of investigation, including the possibility of the process of taking legal action.

According to the US National Institute of Justice (NIJ) [15] was issued a process model in Investigation as a guide for first responders. This model has four steps consisting of the stages

of collection, examination, analysis and reporting. The collection stage is related to the accomplish of various shapes of evidence, and the examination phase takes digital proof of the probative value of the collection of prove. The explanation of the outcome originates the examination stage accompanied by the help of a suitable technique and a system of methods carried out at the scene of analysis. The fourth part and the latter stage contain pursuit such as the proffering of proof, equipment, the technique used, formulation of a general rule and recommendations for improvement if there is.

According to Palmer, in the workshop forensics digital research group (DFRWS) which was first held in Utica, New York, United States (2001). A workshop that aims as a communication forum between academics and practitioners in sharing knowledge about digital forensic science and revealing evidence from digital sources. The workshop participants came from professionals such as from the military, civil and law enforcement. The results of the workshop resulted in a consensus document on the digital forensic investigation process. The process includes identification, preservation, collection, examination, analysis, presentation and decision.

## 3. A STUDY OF THE ANALYSIS COMPARATIVE

In the foregoing discussion that each model has advantages and disadvantages, the comparative analysis of the model excludes strengths, weaknesses and the steps involved in each model will be carried out.

The NADFM model proposed by Ademu et al. [11] The new model based on a study different existing model. This proposed model has several pross. This model has a consistent framework for identifying the fields of research and the process of developing digital investigations. Consistent means that the examiner would act reciprocally with the existing resources. Testing based on involving exploration, the examiner using their testing method for investigation goal. The cons of this model include the majority of the model is not stated clearly and in detail.

The NIJ model proposed by the US National Institute of Justice [15] has four steps consisting of the stages of collection, examination, analysis and reporting. This model has several pros and cons. The pros, such as instil aspects related to the presentation of results in court. Stage comparable to the lucent model by that means less in an amount the level of difficulty in utilisation. The cons of this model are the model is not fully comprehensive in connection with other established of digital applied sciences, such as the computing of the cyber, Internet of Things (IoT), etc.

This DFRWS investigation model includes six stages with the first stage, namely identification. This stage is to determine the needs that will be needed for the investigation and search for digital evidence. The second stage of maintenance is to maintain evidence and ensure the authenticity or integrity of the evidence so that the evidence is genuinely valid/valid. The third stage, namely the collection stage, is the stage for identifying sources of evidence that have the potential to be strong evidence. The fourth stage is the examination phase, which is the stage to determine what will be analysed or better known as data filtering so that the investigator can focus more on the next step. The fifth stage is analysis, which is the stage to find and process data, including data obtained from where, who made it and how the data was produced. The last step is the presentation stage, which is the stage where reporting and presenting the results of the analysis can be understood by the public [16].

The IDFIF method is the development of sequential logic from the primary process in DFIF. This method is divided into four stages, namely Pre-Process, Proactive, Reactive and Post-Process. Steps of Pre-Process include Notification, Authorization, Preparation. Seven Proactive Stages are supporting: Proactive Collection, Crime Scene Investigation, Proactive preservation, Proactive Analysis, Preliminary Report, Securing the Scene, Detection of Incident / Crime. Reactive Stage is a stage that includes Identification, Collection & Acquisition, Preservation, Examination, Analysis and Presentation. Steps of Post-Process are stages that include Conclusion, Reconstruction, Dissemination [17].

GCFIM model, the method with five stages. The first stage of the Pre-Process, this stage relates to everything that needs to be done before the official investigation and data collection. The next stage is the stage of Acquisition & Preservation, the stage associated with identification, obtaining, collecting and preserving data or evidence received. The next step is Analysis. The scene where the core of digital forensics. Various things were analysed on the data obtained to identify sources of crime. The fourth stage is the Presentation. Data, information or evidence of findings from the analysis phase are documented and presented. The investigator must present in a language that is easily understood by all parties but must also be supported by acceptable evidence. The last stage is the Post-Process. This stage is to return digital and physical evidence to the authorities. This evidence can later be used as a learning resource or for training [12]

The SRDFIM investigation model [9] is a stage that will assist in the dynamics of evidence and reconstruction of events by realising the nature of Individuality, Repeatability, Reliability, Performance, Testability, Scalability, Quality and Standards in the analysis of computer fraud and cybercrime (CFCC). This SRDFIM model has several stages from the

stages of Preparation, TKP Security, Surveying and Recognition, Documenting Scenes, Communication Protection, Collecting Evidence, Preservation of Evidence, Examination, Analysis, Presentations, Results & Reviews. This model has benefited and lacked. The benefit of this model is a model that identifies the requirement for interaction. The examiner must have consistent communication with all resources to conduct an investigation. The target of the preferred case is able to determine. An additional pross of this model is testing of the exploration. This model is able to help capture investigative skillfulness as a basis for developing sophisticated tools. It combines a way of carrying out a particular task such as automatic collecting of digital evidence. The general lack of this model is not clearly stated in detail. It must apply in the contexture of an illegal act previously making it viable to clarify the process in detail.

## 4. EDITORIAL POLICY

The digital forensic investigation model described is a model that has been used by researchers with specific case scenarios. However, there is no reference to the investigation model in the world. Comparison of the models described earlier is summarised in table 1

**Table 1:** Comparison analysis digital forensic investigation model

| Phases | NADFM | NIJ | DFRWS | IDFIF | GCFIM | SRDFIM |
|---|---|---|---|---|---|---|
| Collection | | √ | √ | √ | √ | √ |
| Examination | √ | √ | √ | √ | | √ |
| Analysis | | √ | √ | √ | √ | √ |
| Reporting | | √ | | √ | | |
| Preparation | √ | | | √ | √ | √ |
| Preservation | | | √ | √ | √ | √ |
| Presentation | √ | | √ | √ | √ | √ |
| Identification | | | √ | √ | √ | |
| Recontruction | | | | √ | | |
| Documentation | √ | | | | | √ |
| Authorization | | | | √ | | |
| Survey | | | | √ | | √ |
| Communication | | | | | | √ |
| Transportation | | | | √ | | |

Based on the steps associated with theses process of the model, be able to conclude that the model of IDFIF and SRDFIM is the foremost appropriate for amidst all of another model. The model of IDFIF and SRDFIM provides having all the necessary and reliable steps to accomplish the digital of investigation. The model of NADFM and NIJ have minimal levels; for that reason, their model is not suitable to fulfil digital examination entirely. The analysis phase in the NADFM and NIJ models is not precisely and ambiguously defined. After a digital crime occurs, securing communication is very important to get proof of unauthorized access by blocking all devices such as WIFI, USB, cable etc. Only the model IDFIF and SRDFIM is that is providing that step among all these process models.The submitting author is responsible for obtaining agreement of all coauthors and any consent required from sponsors before submitting a paper. It is the obligation of the authors to cite relevant prior work.

## 5. CONCLUSION

The investigation model does not yet have simple guidelines so that it is still developed according to needs. The models above have several similarities and differences at each stage. This model can be used by the interests and needs of the investigator. The purpose of this study compares various models of investigations to help investigators to use in a variety of case scenarios, where each of these models can be quickly adopted, which are already senior and junior.

## APPENDIX

Appendixes, if needed, appear before the acknowledgment.

## ACKNOWLEDGEMENT

The authors would like to thank the financial support from Department of Informatics, Faculty of Computer Science, Universitas Amikom Purwokerto and Pusat Teknologi Pengkomputeran Termaju (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka (UTeM) for their assistance in this research.

## REFERENCES

1. M. Nur Faiz, R. Umar, and A. Yudhana, “Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email,” J. Inform. Sunan Kalijaga, vol. 1, no. 3, pp. 108–114, 2017. https://doi.org/10.14421/jiska.2017.13-02
2. R. Montasari, “Review and Assessment of the Existing Digital Forensic Investigation Process Models,” Int. J. Comput. Appl., vol. 147, no. 7, pp. 1–9, 2016.
3. A. Valjarevic and H. Venter, “Analyses of the State-of-the-art Digital Forensic Investigation Process Models,” South. Africa Telecommun. Networks Appl. Conf., 2012. https://doi.org/10.1109/ISSA.2012.6320441
4. R. Umar, A. Yudhana, and M. N. Faiz, “Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary,” in Prosiding Konferensi Nasional Ke- 4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM), 2016, pp. 207–211.
5. ISO 27043, “INTERNATIONAL STANDARD ISO / IEC 27043: Information technology — Security techniques — Incident investigation principles and processes,” 2015.
6. E. Casey, Digital Evidence and Computer Crime - Third edition. Maryland: Elsevier, 2011.

7. F. Cohen, “Chapter 2 TOWARD A SCIENCE OF DIGITAL FORENSIC EVIDENCE EXAMINATION,” in 6th IFIP WG 11.9 International Conference on Digital Forensics, 2010, pp. 17–35.
8. T. Charles and M. Pollock, “Digital forensic investigations at universities in South Africa,” in 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), 2015, pp. 53–58.
9. A. Agarwal, M. Gupta, S. Gupta, and C. S. Gupta, “Systematic Digital Forensic Investigation Model,” Int. J. Comput. Sci. Secur., vol. 5, no. 1, pp. 118–131, 2011.
10. S. Rani, “DIGITAL FORENSIC MODELS : A COMPARATIVE ANALYSIS,” Int. J. Manag. IT Eng., vol. 8, no. 6, pp. 432– 443, 2018.
11. I. O. Ademu, C. O. Imafidon, and D. S. Preston, “A New Approach of Digital Forensic Model for Digital Forensic Investigation,” Int. J. Adv. Comput. Sci. Appl., vol. 2, no. 12, pp. 175–178, 2011. https://doi.org/10.14569/IJACSA.2011.021226
12. Y. Yusoff, R. Ismail, and Z. Hassan, “Common Phases of Computer Forensics Investigation Models,” Int. J. Comput. Sci. Inf. Technol., vol. 3, no. 3, pp. 17–31, 2011. https://doi.org/10.5121/ijcsit.2011.3302
13. S. Al-fedaghi and B. Al-babtain, “Modeling the Forensics Process,” Int. J. Secur. Its Appl., vol. 6, no. 4, pp. 97–108, 2012.
14. K. Kyei, P. Zavarsky, D. Lindskog, and R. Ruhl, “A Review and Comparative Study of Digital Forensic Investigation Models,” Digit. Forensics Cyber …, pp. 314–327, 2013.
15. G. Shrivastava, K. Sharma, and A. Dwivedi, “FORENSIC COMPUTING MODELS: TECHNICAL OVERVIEW,” Comput. Sci. Inf. Technol., vol. 02, no. 02, pp. 207–216, 2012. https://doi.org/10.5121/csit.2012.2222
16. A. L. Suryana, R. R. El Akbar, and N. Widiyasono, “Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop ( DFRWS ),” J. Edukasi dan Penelit. Inform., vol. 2, no. 2, pp. 111–117, 2016. https://doi.org/10.26418/jp.v2i2.16821
17. Y. D. Rahayu and Y. Prayudi, “Membangun Integrated Digital Forensics Investigation Frameworks ( IDFIF ) Menggunakan Metode Sequential Logic,” in Seminar Nasional Teknologi Informasi dan Komunikasi 2014 (SENTIKA 2014), 2014, vol. 2014, no. Sentika.