Online Social Networks as Supporting Evidence for Digital Forensic Investigation: A Revised Model

Norulzahrah M. Zainudin, Nor Asiakin Hasbullah, Muslihah Wook, Suzaimah Ramli and Noor Afiza Mat Razali
Department of Computer Science,
National Defence University Malaysia
Kuala Lumpur, Malaysia
norulzahrah@upnm.edu.my, asiakin@upnm.edu.my, muslihah@upnm.edu.my,
suzaimah@upnm.edu.my, noorafiza@upnm.edu.my

Abstract

In line with the increasing significance of technology today, the use of digital technology in digital forensic investigation has increased as well. The effect is that many investigations that require the expertise of digital forensics are unable be completed timely by law enforcement agencies around the world. Being consistent with the use of online social media which is the focus of the world nowadays, too many incidents of digital and physical crime have been linked to it. Therefore, a digital forensic model specifically for online social networks needs to be developed to obtain the best evidence and investigation results. A literature review related to digital forensic, models that have been developed in digital forensic and online social network has been conducted in this study. The results found that most studies involve general investigations and processes that overlap with each other. Moreover, there is no model yet to formulate a systemic investigation in the online social network. To overcome this problem, we have developed a standard model for digital forensic investigation of online social networks in this study. This model combines some of the models that have been developed before and added some new activities that are appropriate to the investigation.

Keywords
cybercrimes, digital evidence, digital forensic investigation model, online social network.

1. Introduction

Recently, we have seen an immense increase in the number of users of online social networks such as Instagram, Facebook, Youtube and Tiktok which forms the individual profiles of social media users. Online social networks have generated user profiles publicly and semi-publicly through their respective platforms. This profile provides links between users within a platform, as well as provides information related to other platforms (Pallis et al., 2011).

Criminals are also becoming smarter equivalent with the development of digital technology. They will ensure that the illicit activities are undetectable and escapable if an investigation into them is carried out. This situation occurs in the digital world by using gadgets and computer equipment as a medium of communication by performing various latest techniques and equipment (Caviglione et al., 2017; Nirkhi et al., 2012). Because of that, it is important to create a more systematic approach that can be used by digital forensic investigators to solve crimes related to online social networks, to ensure that digital evidence can be used in court.

Computer forensic has been used as a method of investigation to ensure the investigator determines what has happened, when the incident has occurred, where the incident occurred, why the incident has occurred and who can be associated with the incident (Garfinkel, 2010). All this information is required to determine that all digital evidence is adequate and not to be missed during the forensic investigation. One of the biggest challenges in forensic digital activities is to conduct analysis and produce decisions to be used as evidence to ensure that the evidence can be used in prosecution in court.

In this paper, we propose a digital forensic investigation model that covers all the activities required during the investigation on online social networks. This model is divided into two parts namely physical and digital to describe the location of the investigation.

The organization of this paper is as follows. Section 2 describes the background study of this research; Section 3 explains previous digital forensic investigation model. In Section 4 we present our proposed model and finally in Section 5 we present our conclusion and suggest future work.

2. Background

This section provides a background study on online social networks and digital forensics in order to have better understanding on the concept of this research paper. This section gives a literature review on online social networks and digital forensics hence to have better comprehension on the idea of this research.

2.1 Online social networks

The Internet has become a major tool for developing our "real-world" social networks in many ways. Online social networks provide a private space for users to get connected with their friends, make new friends with similar interests and keep in touch with them through a variety of means.

Boyd et al. (boyd & Ellison, 2007) define online social networks as:
"web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others with-in the system."

Online social networks have empowered better approaches for conveying and sharing data and are utilized consistently by many individuals. Online social networks provide different functionalities including networks of acquaintances, individual surfing, messaging privately or in groups, individual call or video call, video conferencing, event management, video blogging, and media sharing (Al-garadi et al., 2016; Wu & Chen, 2011). Nowadays online social networks are even used as formal communication and interactive medium of government agency (Sonnenberg, 2020).

As most activities now involve online social networks, users are now exposed to online threats from crime activities. There are different sorts of crime that can potentially be undertaken by means of online social networks, and plenty of evidence of the crimes committed will be located within the server of the service providers. Relevant crimes include identity theft, stalking, digital property theft, and child pornography, gangsterism and also neighbourhood crimes (to name a few) (Faust & Tita, 2019). Criminals often communicate with their victims through various social media and commit crimes there or even make it a source of support for committing physical crimes. Therefore, various forms of crime can occur, and various forms of evidence can also be obtained from the online social network storage. Among the materials that can be used as evidence include conversational text, videos, images, comments, and various other sources (boyd & Ellison, 2007; Zainudin & Llewellyn-jones, 2008). Gathering this data is time consuming, since it is invariably spread across the profiles of multiple users, increasing the likelihood that an important piece of data might be missed. Therefore, a systematic and reliable approach should be used to conduct digital forensics for online social networks.

2.2 Digital forensics

Digital forensics has grown rapidly in a period of time to become a very important part in many investigations in the cyber world (Al-Mahrouqi et al., 2015). 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. Judd Robbins (Robbins, 2002), a computer forensic investigator, defines computer forensics as "Simply the application of computer investigation and analysis techniques in the interest of deter-mining potential legal evidence".

Rodney McKemmish (McKemmish, 1999) describes forensic computing as "The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable". As Philip D. Dixon (Dixon, 2005) defines computer forensic in an article, "An overview of computer forensics" as finding the main goals of the processes in there that are preservation, identification, extraction, documentation, and interpretation of computer data.

Digital forensics is a critical area right now as internet usage is increasing, cybercrime is also on the rise. Therefore, digital forensic investigation requires a systematic process to obtain accurate and valid evidence for the court. The investigation conducted should be guided by the best procedures or methodology to ensure that data and information are protected from tampering or damage (Montasari & Hill, 2019). Digital forensics can also ensure the integrity of the computer system under investigation to enable information to be obtained as evidence. Many models and frameworks have been developed by researchers and digital forensic practitioners to produce the best methods in digital forensic investigation. Each model and framework have its own strengths to make the investigation procedure according to the proper process.

3. Digital Forensic Investigation Models and Frameworks

There are several authors that have suggested digital forensic investigation models and frameworks, for example, Kruse and Heiser (II & Heiser, 2002) proposed a computer and network forensic methodology that consists of three basic components These are 1) acquire evidence; 2) authenticate evidence; and 3) analyzing 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 (Clint et al., 2002; Mukasey et al., n.d.; M. Rogers, 2003).

The U.S. Department of Justice (Guide, 2001) has released a model that has four phases. The phases are 1) Collection; 2) Examination; 3) Analysis; and 4) Reporting. However, there are some issues that can be discussed. The analysis phase included in the model is not clearly described in its functionality and it is too common. The outcome of this phase seems to appear because of the investigation phase. This process is unclear because the two phases are obviously different in terms of the process.

Carrier and Spafford (B. Carrier & Spafford, 2003) 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 to an incident which has occurred. This phase is separated from the physical and digital investigation phase. However, in practice it is difficult to confirm that 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 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).

Lee (Lee et al., 2001) produced a model that is called The Scientific Crime Scene Investigation Model that has four stages. These are: recognition; identification; individualization, and reconstruction. The stages are only part of digital forensic investigation procedure. It only focuses on the investigation phase without involving other important processes as well.

Later Casey (Casey, 2002) developed a model that is comparable to Lee, nonetheless it just emphasizes on handling and investigating digital evidence. The steps included are: 1) recognition; 2) preservation; 3) classification, and 4) reconstruction. Both digital forensic investigation models by Lee and Casey have similar phases in the initial and final parts. Obviously, Casey is indeed focused on the forensic process in the investigation.

The Digital Forensics Research Working Group (DFRW) established by the National Institute of Justice (B. Carrier & Spafford, 2004) proposed a model with the steps as described here: 1) identification; 2) preservation; 3) collection; 4) examination; 5) analysis; 6) presentation and 7) decision. This model has produced an important foundation in digital forensic investigation by adding two important processes. The sub-processes in the investigation and presentation were described in detail.

Clint et al. (Clint et al., 2002) has developed a model that has some activities that have never been suggested by any authors before. The Abstract Digital Forensic Model is formed of nine steps: 1) Identification; 2) Preparation; 3)

Approach strategy; 4) Preservation; 5) Collection; 6) Examination; 7) Analysis; 8) Presentation and 9) Returning evidence. Basically, this model can be used for a complete investigation, but there is one drawback found. The third step, the approach strategy, seems to overlap with the second step, which is the preparation phase. This situation occurs due to the time for an investigator to respond to the notification of an incident leading to the decision of which technique will be used in the investigation.

A model proposed by Ciardhuáin (Ciardhuáin, 2004) is comprises of a set of phases that are called 'activities'. The model consists of: 1) awareness; 2) authorization; 3) planning; 4) notification; 5) search for and identify evidence; 6) collection; 7) transportation; 8) storage; 9) examination; 10) hypothesis; 11) presentation; 12) proof/defense and 13) dissemination. There is a new phase produced by this model which is hypothesis.

Rogers at. al (M. K. Rogers et al., 2006) has published his model that is called Computer Forensics Field Triage Process Model. This model involves six main phases that are planning, triage, user profiles, chronology/timeline, email & IM, and case specific evidence. The model introduced a faster process of investigation that focused on investigation on-site for faster evidence acquirement and collection. However, this model is applied well on their case study that is child pornography. It has to be improved to suit with other cases.

Perumal (Perumal, 2009) suggested a model that is constructed from the investigation process in Malaysia. This model focused on live as well as static data acquisition to gather fragile evidence. The steps including 1) planning; 2) identification; 3) reconnaissance; 4) transport and storage; 5) analysis; 6) proof and defense; and 7) archive storage.

Montasari 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 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. In the scope of this study, a standard model for online social networks will be developed to carry out a systematic and comprehensive investigation.

4. Analysis of Existing Models and Frameworks

We have discussed about the existing models and frameworks thoroughly in the previous section. In this section, we have mapped the models and processes, activities, phases. Table 1 shows that although various terms are used in the respective models and frames, they still lead to the same meaning which is to describe the workflow in forensic investigations. To standardize the use of terms, we have decided to use process for the next description. Based on this table, it can be clearly seen that all models and frameworks have their own uniqueness in producing a comprehensive investigation process, but still with the same goal of conducting forensic investigations scientifically and systematically. Therefore, we have classified several processes with identical terms to study the importance of those processes based on their frequency of use in the models and frameworks discussed. Figure 1 shows the processes that have been classified according to their frequency in use. Based on this graph, we have selected significant processes for the development of our model.

Table 1. The matrix of digital forensic models and frameworks

Processes/ phases/ activities	Digital Forensic Models/ Frameworks											
	The U.S. Department of Justice (2001)	Lee et al. (2001)	Kruse and Heiser (2002)	Carrier and Spafford (2003)	Casey (2003)	Ciardhuain (2004)	Carrier and Spafford (2004)	Rogers et al. (2006)	Perumal (2009)	Montasari et al. (2015)	Montasari (2016)	Dokko & Shin (2018
Acquiring evidence			√									
Acquisition and collection											√	
Analysis	√								√	√		
Archive storage									√			
Authenticating evidence			√									
Authorization						√						
Awareness						√						
Case specific								√				
Chronology timeline								√				
Classification					√							
Collection	√					√				√		
Deployment				√			√					
Digital crime scene investigation				√			√					
Digital evidence examination											√	
Digital evidence interpretation											√	
Dissemination						√						
Documentation												√
Evidence mapping												√
Evidence sufficiency verification												√
Examination	√					√				√		
File reduction												√
First response											√	
Hypothesis						√						
Identification		√							√	√	√	
Incident closure										√		
Incident detection											√	
Incident response										√		
Individualization		√										
Intelligence gathering											√	
Internet								√				
Investigation closure											√	
Notification						√						
Physical crime scene investigation				√			√					
Planning						√		√	√		√	
Presentation						√	√			√	√	
Preservation					√							
Proof/defence						√			√			
Readiness				√			√			√	√	
Recognition		√			√							
Reconnaissance									√			
Reconstruction		√			√							
Reporting	√										√	
Review				√								
Search/identify						√						
Secure and evaluate crime scene											√	
Storage						√					√	
Transport						√						
Triage								√				
User usage								√				

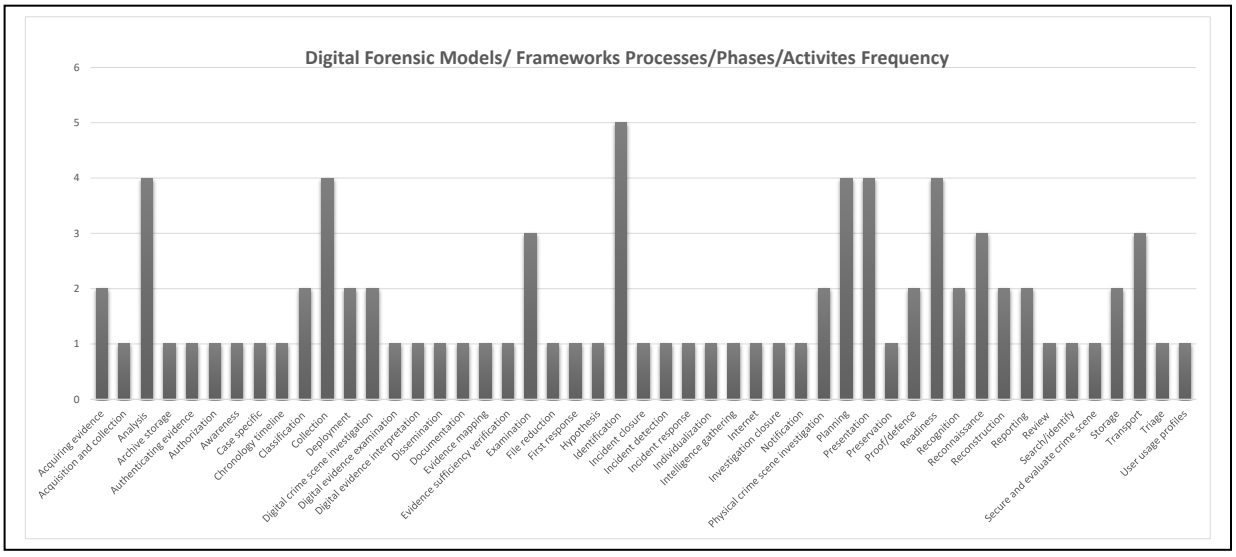

Figure 1. The process frequency of existing models and frameworks

5. The Proposed Model

In Section 2, an extensive literature study on digital forensic investigation models and frameworks has been conducted. We found that although there are several digital forensic investigation models already developed, most have quite similar approaches which has no standard and consistent model, only sets of procedures and tools. To suggest a solution in digital forensic investigation involving incidents in online social networks, a model was proposed.

Figure 2 shows the model of digital forensic investigation for online social networks that we have proposed. The proposed model comprises the whole process of online social network investigation. We have divided the processes of investigation into two sections. The physical section consists of activities that are carried out before the investigation. These are preliminary activities including notification from the enforcement body, planning of how to conduct the investigation, and surveying of any physical crime scene and evidence present. After these activities have been completed, investigators will proceed to the digital sections where they will carry out investigation and analysis of online social networks using an application prototype that will be developed. The next activity will shift back to the physical sections where all the evaluation process takes place. We will discuss about this model thoroughly in the next section.

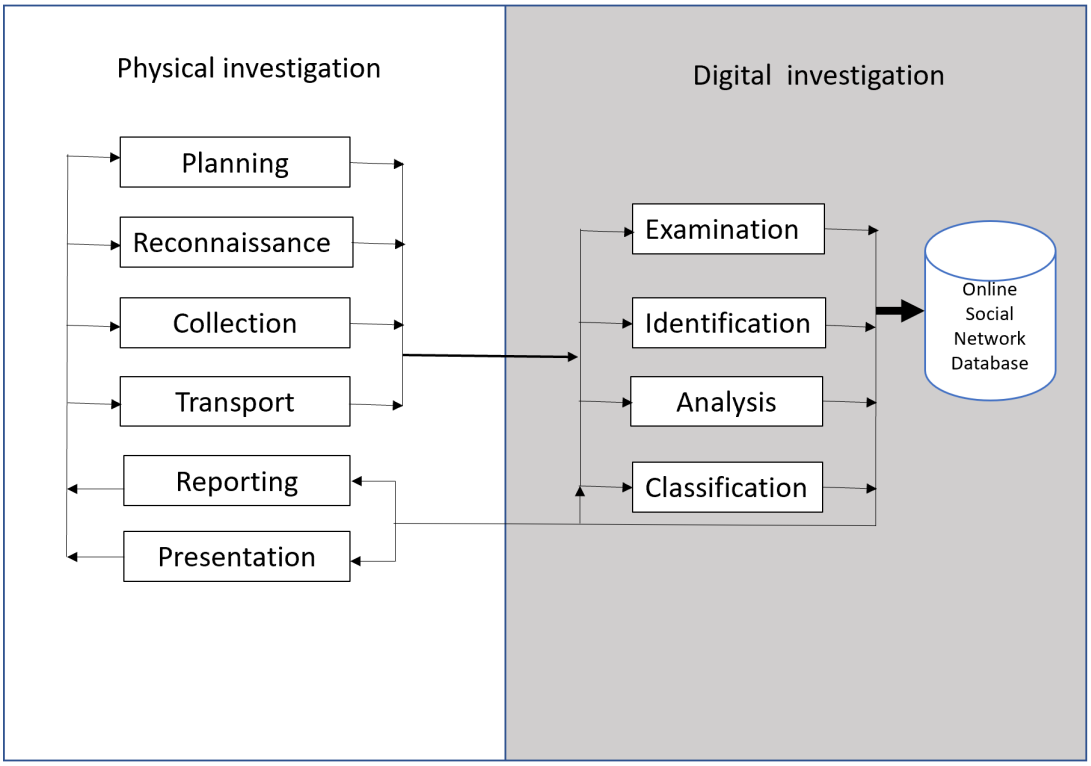

Figure 2. The proposed model

5.1. Physical investigation

The physical investigation consists of processes that are carried out before and after the investigation. The physical investigation involved a set of processes that take place in the physical section of an investigation. Carrier and Spafford (B. D. Carrier & Spafford, 2006) has emphasized the importance of physical investigation process, essentially, it is the beginning of a digital investigation where the physical objects and evidence are gathered. All processes are carried out in the physical sections to make sure that all necessary measures are understood and recognized. The processes in the physical section are described thoroughly in the next paragraph.

i. Planning- This is the earliest and one of important processes in an investigation. At this stage, the first thing to do is to confirm that an incident has occurred and how it happened. Careful planning should be done in this process including identifying the scope and perimeter of the location of the incident, the level of disaster, the number of people and locations involved, the area of expertise required, the tools required, as well as legal matters in the investigation.

ii. Reconnaissance - A survey is an initial investigation process that requires the investigator to make a general assessment of an incident. This can clarify the investigation process as all relevant issues will be thoroughly identified to ensure that nothing is overlooked in the early stages of the investigation. This process will be done during physical investigation involving the location of the incident. Carrier and Spafford (B. Carrier & Spafford, 2004) are the only authors that implemented survey process in their model.

iii. Collection- In this process, the investigator will confiscate any physical evidence that can be used during investigation. This is a crucial process as physical evidence can be admissible in court if a proper procedure in not well conducted.

v. Transport- Transporting is a process where the physical evidence is relocated systematically for further investigation to a suitable location.

vi. Reporting- Reporting is a crucial process to present the results in documentation form to ensure that the evidence is consistent and reliable for prosecution of criminals in a court of law.

vii. Presentation- The presentation of evidence that has been analyzed and all findings in an investigation should have an impact on the people involved in judging the evidence such as the prosecution teams, lawyers, jurors, or judges in court, or top management in the organization. The goal in this process is to ensure that the evidence is valid, as well as the people evaluating the evidence understand the information presented.

5.2. Digital investigation

In digital investigation section, there is four activities required which are identification, searching, filtering and classifying. The processes in this section will be discussed thoroughly in the next paragraph.

i. Examination- Examination is the process of finding information from sources that have been collected. In the context of the model developed, a search will be conducted on online social networks, computers or gadgets used during the incident. As the focus of the investigation on online social networks, plenty of information can be gained through one's profile. To interpret a profile in an online social network, there are various social visualization applications which have been designed for end-users. However, these applications currently apply only to particular networks. Boyd (Boyd & Heer, 2005) explained the use of online social network visualization as a method to identify the relationship between a complex graph structure, it can help visual analysis and search, and identify the structure of a community automatically by visualizing the structure. In digital forensic investigations these functions can allow examiners to find connections between a suspect (or member of staff being audited) and other people, thereby helping to progress the investigation. Furthermore, examiners could find supporting evidence not only by examining a profile, but also by searching the profiles of contacts and friends.

i. Identification- The first process in a digital investigation requires the investigator to identify the necessary processes before starting a digital investigation. Among the important processes is the need to identify the resources that have been collected through previous processes that have the potential to be used as evidence. This is also to ensure that no important evidence is overlooked during digital investigations.

iii. Analysis- The main purpose of analysis process is to manipulate the collected data by using various applicable methods and techniques, to make sure the results from the analysis process is precise, consistent, and accepted in digital forensic analysis.

iv. Classification- The last process in digital investigation is classification. Classification is the process of ensuring that all digital data obtained are classified according to predetermined categories. The main purpose of classifying is to prevent new information obtained from being lost.

6. Conclusion and Future Work

This paper discussed about development of a digital forensic investigation model specifically for online social networks. We described the concept of digital forensics and the existing digital forensics investigation models and frameworks. For the purposes of general investigation (e.g. analysis of a hard disc), there are various tools available because they are produced according to general investigatory requirements. However, to conduct investigations in online social networks, these tools are not suitable because they do not provide specific functions and options as discussed in the previous section. To address these limitations, a model for online social networks to conduct digital forensic investigations needs to be developed. Therefore, this model has been suggested to fill the relevant requirements. As this is a revised model, there are more works need to be done including verifying the model from experts and the needs to perform technical analysis.

References

Al-garadi, M. A., Varathan, K. D., & Ravana, S. D. (2016). Computers in Human Behavior Cybercrime detection in online communications : The experimental case of cyberbullying detection in the Twitter network. *Computers in Human Behavior*, *63*, 433–443. https://doi.org/10.1016/j.chb.2016.05.051

Al-Mahrouqi, A., Abdalla, S., & Kechadi, T. (2015). Efficiency of network event logs as admissible digital evidence. *Proceedings of the 2015 Science and Information Conference, SAI 2015*, 1257–1265. https://doi.org/10.1109/SAI.2015.7237305

boyd, danah m., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Boyd, D., & Heer, J. (2005). Vizster: Visualizing Online Social Networks. *Proceedings of the International Symposium on Information Visualization (InfoVis'05)*, 33–40. https://doi.org/10.1109/INFVIS.2005.1532126

Carrier, B. D., & Spafford, E. H. (2006). Categories of digital investigation analysis techniques based on the computer history model. *Digital Investigation*, *3*(SUPPL.), 121–130. https://doi.org/10.1016/j.diin.2006.06.011

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

Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Investigation Process. *International Journal of Digital Evidence*, *2*(2).

Casey, E. (2002). Practical approaches to recovering encrypted digital evidence. *International Journal of Digital Evidence*, *1*(3), 1–27. http://people.emich.edu/pstephen/other_papers/Recovering Encrypted Digital Evidence.pdf

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

Ciardhuáin, S. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, *3*(1), 1–22. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.80.1289&rep=rep1&type=pdf%5Cnhttps://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf

Clint, M. R., Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, *1*(3), 1–12. https://doi.org/10.1109/SADFE.2009.8

Dixon, P. D. (2005). An overview of computer forensics. *IEEE Potentials*, *24*(5), 7–10. https://doi.org/10.1109/MP.2005.1594001

Dokko, J. (2019). *A Digital Forensic Investigation and Verification Model for Industrial Espionage : 10th International EAI Conference , ICDF2C 2018 , New Orleans , LA , A Digital Forensic Investigation and Verification Model for Industrial Espionage*. *1*(June), 0–18. https://doi.org/10.1007/978-3-030-05487-8

Evans, C., & French, J. L. (2009). Crime Scene Investigation 2013 A Guide For Law Enforcement. *Forensic Science International*, *136*, 120. https://doi.org/10.1016/S0379-0738(03)90006-5

Faust, K., & Tita, G. E. (2019). Social Networks and Crime: Pitfalls and Promises for Advancing the Field. *Annual Review of Criminology*, *2*, 99–122. https://doi.org/10.1146/annurev-criminol-011518-024701

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*, S64–S73. https://doi.org/10.1016/j.diin.2010.05.009

Guide, N. (2001). A Guide for First Responders. *United States Department of Justice Office of Justice*, 93. http://www.iwar.org.uk/ecoespionage/resources/cybercrime/ecrime-scene-investigation.pdf

Hitchcock, B., Le-Khac, N. A., & Scanlon, M. (2016). Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists. *Digital Investigation*, *16*, S75–S85. https://doi.org/10.1016/j.diin.2016.01.010

II, W. K., & Heiser, J. (2002). *Computer Forensics: Incident Response Essentials*. Addison-Wesley.

Lee, H., Palmbach, T., & Miller, M. (2001). *Henry Lee's Crime Scene Handbook*. Academic Press.

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

Montasari, R. (2016a). A comprehensive digital forensic investigation process model. *International Journal of Electronic Security and Digital Forensics*, *8*(4), 285–302. https://doi.org/10.1504/IJESDF.2016.079430

Montasari, R. (2016b). An ad hoc detailed review of digital forensic investigation process models. *International Journal of Electronic Security and Digital Forensics*, *8*(3), 205–223. https://doi.org/10.1504/IJESDF.2016.077444

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*, 205–212.

https://doi.org/10.1109/ICGS3.2019.8688020
Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (n.d.). Electronic Crime Scene Investigation : A Guide for First Responders , Second Edition. *Innovation*.
Nirkhi, S. M., Dharaskar, R. V., & Thakre, V. M. (2012). Analysis of online messages for identity tracing in cybercrime investigation. *Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012*, 300–305. https://doi.org/10.1109/CyberSec.2012.6246131
Pallis, G., Zeinalipour-yazti, D., & Dikaiakos, M. D. (2011). *Online Social Networks : Status and Trends*. 213–234.
Perumal, S. (2009). Digital Forensic Model Based On Malaysian Investigation Process. *IJCSNS International Journal of Computer Science and Network Security*, *9*(8), 38–44. https://doi.org/10.1504/IJESDF.2010.033780
Robbins, J. (2002). *An Explanation of Computer Forensics*.
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
Rogers, M. K., Mislan, R., Goldman, J., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. *Conference on Digital Forensics, Security and Law*, *1*(2), 27–40. https://doi.org/10.1.1.169.1878
Sonnenberg, C. (2020). E-Government and Social Media: The Impact on Accessibility. *Journal of Disability Policy Studies*, *31*(3), 181–191. https://doi.org/10.1177/1044207320906521
Wu, Z., & Chen, C. (2011). The Study of One Online Social Network Based on Structure and Evolution. *2011 International Conference on Computer and Management (CAMAN)*, 1–4. https://doi.org/10.1109/CAMAN.2011.5778897
Zainudin, N. M., & Llewellyn-jones, D. (2008). *A Digital Forensic Investigation Model and Tool for Online Social Networks*.

Biographies

Norulzahrah Mohd Zainudin is a Lecturer in the Department of Computer Science at Faculty of Defence Science and Technology, National Defence University Malaysia (UPNM). She received her MSc at Universti Putra Malaysia, BSc at Universiti Teknology Malaysia and joined Military Academy of Malaysia in 2002. Her main research interests are in the areas of Forensic Computing, Online Social Networks and Computer Intelligence. She has published several papers in international journals and conferences. Currently she is a member of Informatics Intelligence Special Interest Group, UPNM and member of Graduate Technologist, a recognition awarded by Malaysia Board of Technologist.

Nor Asiakin Hasbullah was born in Muar, Johor. She received her PhD in Information Technology and Quantitative Sciences from MARA University of Technology Malaysia in 2017 and have done three months attachment in Glasgow Caledonian University of Glasgow under Privacy research in 2012. She holds a Master of Science in Information Technology from MARA University of Technology Malaysia in 2006, and Bachelor of Information Technology (Hons) from Universiti Kebangsaan in 2003. Currently she is a Senior Lecturer in the Department of Computer Science, National Defence University of Malaysia (UPNM). Her research interests are in the field of privacy, data protection, information security and ethics in ICT. She is a member of Malaysia Board of Technologist and Informatics Intelligence Special Interest Group, UPNM. She has published and presented most of her research findings and articles in various international conferences and international journal.

Muslihah Wook received her PhD in Information Science from Universiti Kebangsaan Malaysia in 2017, Master of Computer Science from Universiti Putra Malaysia in 2004, and Bachelor of Information Technology (Hons) from Universiti Utara Malaysia in 2001. Her research interests include data mining applications in various domain particularly in education, security and defence. Currently she is working as a senior lecturer at Department of Computer Science, Faculty of Defence Science and Technology, National Defence University of Malaysia. She has become members of International Association of Computer Science and Information Technology (IACSIT) and Institute of Research Engineers and Doctors (IRED) since 2011 and 2013 respectively. Recently, she has been appointed as a technical reviewer of Education and Information Technologies —Springer's journal indexed by Scopus (Q2)

Suzaimah Ramli was born in Temerloh Pahang. She received her PhD in Electrical, Electronic and System Engineering from Universiti Kebangsaan Malaysia in 2011, Master of Computer Science from Universiti Putra Malaysia in 2001, and Bachelor of Information Technology (Hons) from Universiti Utara Malaysia in 1997. Her research interests include image processing and artificial intelligence applications in various domain particularly in

education, security and defence. Currently she is working as an Associate Professor at Department of Computer Science, Faculty of Defence Science and Technology, National Defence University of Malaysia. She is a member of Malaysia Board of Technologist and Informatics Intelligence Special Interest Group, UPNM. She has published and presented most of her research findings to various international conferences and articles in many international journals specifically in her research niche.

Noor Afiza Mat Razali holds a bachelor's degree in Computer and Information Engineering, Master of Science in Computer Science and PhD. of Science in Computer Science from Japanese Universities. Afiza is a Senior Lecturer at Faculty of Defence Science and Technology in National Defence University of Malaysia. Afiza also appointed as Visiting Lecturer and Fellow at Management and Science University Malaysia, Academic Liaison Consultant for Japanese Universities at University Kuala Lumpur and Fellow at Education Malaysia Global Services (EMGS). Afiza research and expertise are in the area of Cyber Security, Disaster Management System, Big Data Analytics, Human Computer Interaction, Artificial Intelligence & Robotics and Blockchain Technology. Afiza also a professional technologist, a recognition given by Malaysia Board of Technologist.