Mapping Process of Digital Forensic Investigation Framework

Siti Rahayu Selamat[1], Robiah Yusof[2], Shahrin Sahib[3]

Faculty of Information Technology and Communication,
Universiti Teknikal Malaysia Melaka, Ayer Keroh, Melaka, Malaysia

Summary
Digital forensics is essential for the successful prosecution of digital criminals which involve diverse digital devices such as computer system devices, network devices, mobile devices and storage devices. The digital forensic investigation must be retrieved to obtain the evidence that will be accepted in the court of law. Therefore, for digital forensic investigation to be performed successfully, there are a number of important steps that have to be taken into consideration. The aim of this paper is to produce the mapping process between the processes/activities and output for each phase in Digital Forensic Investigation Framework (DFIF). Existing digital forensic frameworks will be reviewed and then the mapping is constructed. The result from the mapping process will provide a new framework to optimize the whole investigation process.

Key words:
Alert Digital forensic investigation framework (DFIF), map, forensic

1. Introduction

Since its inception, the field of digital forensic has not been significantly changed. It originates in solving pragmatic acquisition and chain of evidence problems related to investigations, performed by and large, by law enforcement personnel with little formal background in computing. The emergence of forensics comes from the incidence of criminal, illegal and inappropriate behaviors. In general, the role of forensics can be classified in the following areas which are to facilitate investigations of criminal activities using forensic methodologies, techniques and investigation frameworks. The areas are to preserve, gather, analyze and provide scientific and technical evidences for the criminal or civil courts of law; and to prepare proper documentations for law enforcement prosecution. In short, digital forensic is the process of identifying, preserving, analyzing, and presenting evidence in a manner that is legally acceptability [14], [16], [13], [20].

Digital investigation is a process to answer questions about digital states and events. In contrast, a digital forensics investigation is a special case of a digital investigation where the procedures and techniques that are used will allow the results to be entered into a court of law [21]. Therefore few important steps have to be taken into consideration in order to perform a successful forensic investigation. However, no formal theory exists for the process [21]. A practitioner in this field can describe how he recognizes evidence for a specific type of incident, but the recognition process cannot be typically described in a general way.

In the digital forensics investigation practices, there are over hundreds of digital forensics investigation procedures developed all over the world. Each organization tends to develop its own procedures and some focused on the technology aspects such as data acquisition or data analysis [3]. To date, the digital investigation process has been directed by technology being investigated and the available tools. Most of these procedures were developed for tackling different technology used in the inspected device. As a result, when underlying technology of the target device changes, new procedures have to be developed. This paper proposes a mapping process which can simplify the overall process of the previous research that occurs inside the Digital Forensic Investigation Framework. The result of the propose map will reveal the balance of the investigation process to produce a suitable concrete evidence for presentation in a court of law.

2. Related Work on Digital Forensic Investigation Framework

The review will only focus on thirteen published papers that represent the DFIF with their respective process or activities as shown in Table 1.

Early in 1995, [12] suggested a methodology for dealing with potential evidence. The author mapped the computer forensic process to the admission of documentary evidence in a court of law. He stated that the process used must be conformed to both the law and science. In this methodology introduced four distinct steps that are identified precedent to the admission of any evidence in court. The steps are acquisition, identification, evaluation and admission as evidence. The output of these steps or processes is media (physical context), data (logical context), information (legal context) and evidence respectively.

In 2001, The Digital Forensics Research Working Group [16] defined a generic investigation process that can be applied to all or the majority of investigations involving digital systems and networks. The processes

Manuscript received October 5, 2008
Manuscript revised October 20, 2008

that defined at that time are identification, preservation, collection, examination, analysis, presentation and decision. In this framework the processes are called classes of task and individual tasks called elements. This framework puts in place at important foundation for future work.

However in 2002, [17] proposed a framework called an abstract digital forensics framework based on DFRWS framework consists of eleven phases which are identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation and returning evidence. Its does well at providing a general framework that can be applied to categorizing of incidents. This comprehensive process offers a number of advantages as listed by the authors such as mechanism for applying the same framework to future digital technologies. However this framework is open to at least one criticism where its third phase (the approach strategy) is to an extent a duplication of its second phase (the preparation phase). This is because at the time of responding to a notification of the incident, the identification of the appropriate procedure will likely entail the determination of techniques to be used.

In 2003, digital investigation process framework is proposed by [5] that based on the investigation process of physical crime scene. This framework has high-level phases for the analysis of both the physical crime scene. It's called the Integrated Digital Investigation Process (IDIP). They define the digital crime scene as the virtual environment created by software and hardware where digital evidence of a crime or incident exists. This framework organizes the process into five groups consists of 17 phases. The groups are readiness phases, deployment phases, physical crime scene investigation phases, digital crime scene investigation phases and review phase. This highlights the reconstruction of the events that led to the incident and emphasizes reviewing the whole task, hence ultimately building a mechanism for quicker forensic examinations.

[19] views each of processes in DFRWS framework as a class and each of the actions taken as elements of the class. Then, he states that six classes define the investigative process. Therefore, he extends the processes into nine steps which he then called as End-to-End digital Investigation Process (EEDI). These nine steps in EEDI must be performed by the investigator in order to preserve, collect, examine and analyze digital evidence. He also defined the critical activities in the collection process such as to collect the images of effected computers, to collect logs of intermediate devices especially those on the internet, to collect logs of effected computers and to collect logs and data from intrusion detection systems, firewalls, etc. He then developed a formal representation of the nine steps using Digital Investigation Process Language (DIPL) and Colored Petri net Modeling. This framework mainly focused on the analysis process and merging events from multiple locations.

Table 1: Existing Digital Forensic Investigation Frameworks

No	Digital Forensic Investigation Framework	No of Phases
1	Computer Forensic Process (M.Pollitt, 1995)	4 processes
2	Generic Investigative Process (Palmer, 2001)	7 classes
3	Abstract Model of the Digital Forensic Procedure (Reith, Carr, & Gunsch, 2002)	9 components
4	An Integrated Digital Investigation Process (Carrier & Spafford, 2003)	17 phases
5	End-to-End Digital Investigation (Stephenson, 2003)	9 steps
6	Enhance Integrated Digital Investigation Process (Baryamureeba & Tushabe, 2004)	21 phases
7	Extended Model of Cybercrime Investigations (Ciardhuain, 2004)	13 activities
8	Hierarchical, Objective-based Framework (Beebe & Clark, 2004)	6 phases
9	Event-based Digital Forensic Investigation Framework (Carrier & Spafford, 2004)	16 phases
10	Forensic Process (Kent K. , Chevalier, Grance, & Dang, 2006)	4 processes
11	Investigation Framework (Kohn, Eloff, & Oliver, 2006)	3stages
12	Computer Forensics Field Triage Process Model (K.Rogers, Goldman, Mislan, Wedge, & Debrota, 2006)	4 phases
13	Investigative Process Model (Freiling & Schwittay, 2007)	4 phases

Then in 2004, [1] enhanced the Integrated Digital Investigation Process Framework (IDIP) called Enhanced Digital Investigation Process Framework (EIDIP). EIDIP separates the investigations at the primary and secondary crime scenes while depicting the phases as iterative instead of linear. In their paper, they describes two additional phases which are trace back and dynamite that seek to separate the investigation into primary crime scene (the computer) and the secondary crime scene (the physical crime scene). The objective of the enhancement is to reconstruct the two crime scenes concurrently to avoid inconsistencies.

Carrier and Spafford has proposed another framework for defining the Event-based Digital Forensic Investigation Framework by recognizing the non-

uniqueness Survey phase in IDIP and then simplifying the framework into Preservation, Search and Reconstruction phase [4]. This simple framework is based on the causes and effects of events. The goal of each of these phases is unique and the requirements can be defined. However, these three phases has not mention the completeness of each phases. Hence it is not clear that this framework is sufficient enough for Digital forensic Investigation.

The framework proposed by [7] has clear steps to be taken during the investigation process starting from preparation of investigation process right after the crime is reported until the case disseminated. The framework includes the phases which he call as activities such as awareness, authorization, planning, notification, search and identify, collection, transport, storage, examination, hypotheses, presentation, proof/defense and dissemination. The framework also provides a basis for the development of techniques and tools to support the work of investigators. Therefore, this framework is probably considered as the most complete to date [11].

[2] proposed multi-tier process after they reviewed that most of previous forensic frameworks were single tier process but in fact the process tends to be multi-tiered. They specifically propose several subtasks for the data analysis phase using survey extract and examine approach. The phases of the first tier are preparation, incident response, data collection, data analysis, presentation and incident closure. The data analysis phase is further organized into the survey phase, extract phase and examine phase in the second tier. In the proposed framework, the analysis task using the concept of objective-based tasks is introduced. As stated by the authors, this framework offers unique benefits in the areas of practicality and specificity. These benefits can overcome the problems in the framework proposed by [5].

In 2006, forensics process proposed by [10] consists of four phases which are collection, examination, analysis and reporting. The output for each phase is similar to the early process proposed by [12]. In this framework, forensic process transforms media into evidence either for law enforcement or an organization's internal usage. First, transformation occurs when collected data is examined which extracts data from media and transforms it into a format that can be processed by forensic tools. Then, the data is transformed into information through analysis and finally, the information is transform into evidence during the reporting phase.

[11] proposed a new framework by merging the existing frameworks to compile a reasonably complete framework. The proposed framework draws on the experience of others [1], [5], [6], [15], [17], [7]. Their research has highlighted two important points; the knowlegde of relevant legal base prior to setting up the framework that is vital since it will bear the whole investigative process; and the process should include three stages (preparation, investigation and presentation) to meet the minimum requirements of the definition of the word "forensic". Therefore, [11] has proposed their framework by grouping the phases in the existing framework into these three stages. This framework also sets a legal base as foundation to have clear understanding of what the legal requirements are; is established right at the start of investigation and informs each subsequent step or phase. In this framework, two requirements have been identified as needed at every level; that are the legal requirements of a specific system and documentation of all the steps taken. The advantage of this proposed framework can be easily expanded to include any number of additional phases required in future.

The Computer Forensic Field Triage Process Model (CFFTPM) proposes an onsite or field approach for providing the identification, analysis and interpretation of digital evidence in a short time frame without requirement on taking the systems/media back to the lab for an in-depth examination or acquiring a complete forensic image [9]. This framework derived from the IDIP framework [5] and the Digital Crime Scene Analysis (DCSA) framework as developed by [18]. The phases include in this framework are planning, triage, usage/user profiles, chronology/timeline, internet activity and case specific evidence. This framework is a formalization of real world investigative approaches that have distilled into a formal process framework. The major advantage of CFFTPM is on its practicality and pragmatic due to the fact that the framework was developed in reverse of most other DFIF. However, this framework is also not necessarily applicable for all investigative situations.

The Common Process Model for Incident and Computer Forensics proposed by [8] has introduced a new process framework to investigate computer security incidents and its aim is to combine the two concepts of Incident Response and Computer Forensics to improve the overall process of investigation. This framework focused greatly on the analysis and it consists of Pre-Incident Preparation, Pre-Analysis, Analysis and Post-Analysis. Pre-Analysis phase contains all steps and activities that are performed before the actual analysis starts and Post-Analysis Phase is concerned on the written report documentation of the whole activities during the investigation. The actual analysis takes place in the Analysis Phase. This framework offers a way to conduct proper incident response while applying principles known from Computer Forensics during the actual analysis phase and it integrating a forensic analysis into an Incident Response framework.

Three main issues have been analyzed from the above frameworks, which are process redundancies, area focus and framework characteristics. For example, [17] and [1] have duplication process or activities in their framework. [5] and [9] were focusing on building a mechanism for quicker forensic examinations, whereas [19], [2] and [8] were focusing on the analysis process in order to obtain the evidence and improve the overall process of investigation. [2] and [9] frameworks have the characteristics of practicality, specificity and pragmatic which is important for investigation process. All of these frameworks have their own strength; however until nowadays there is no single framework can be used as a general guideline for investigating all incidents cases. Therefore, further research is needed to design a general framework to overcome this issue.

3. Mapping Process of the Digital Forensic Investigation Framework

From the existing frameworks or models mentioned in Section 2, it can be seen quite clearly that each of the proposed frameworks builds on the experience of the previous; some of the frameworks have similar approaches and some of the frameworks focus on different areas of the investigation. However, all of the frameworks have the same output; even if the process or the activity is slightly difference on the term used and the order of the steps.

This paper proposes a map of Digital Forensic Investigation Framework (DFIF) by grouping and merging the same activities or processes that provide the same output into an appropriate phase. This mapping process is designed in order to balance the process on achieving the overriding goal that can produce concrete evidence for presentation in a court of law.

In this research, the steps implemented to design mapping process of the DFIF are as the following:

Step 1 - Identify existing frameworks

In this step, the phases, activities/processes and output for each framework is analyzed. The summarization is shown in Table 2.

Step 2 - Construct phase name

In this step, phase name is constructed based on the activities/processes and output analyzed from step 1. Five phases has been named (i.e. Phase 1 – Phase 5) as in Table 3.

Table 3: Summarization of the Output Mapping

Phase	Phase Name	Output
Phase 1	Preparation	Plan, Authorization, Warrant, Notification, Confirmation
Phase 2	Collection and Preservation	Crime type, Potential Evidence Sources, Media, Devices, Event
Phase 3	Examination and Analysis	Log Files, File, Events log, Data, Information
Phase 4	Presentation and Reporting	Evidence, Report
Phase 5	Disseminating the case	Evidence Explanation, New Policies, New Investigation Procedures, Evidence Disposed, Investigation Closed

Step 3 – Mapping the process

An analysis has been done in this step where the appropriate activities/processes and output is mapped into the new phase name and the sample of the result is represented in Table 4.

Table 4: Summarization of Mapping Process

Phase / Output	**1**	**2**	**3**	**4**	**5**
Pollitt, 1995					
Acquisition		√			
Identification		√			
Evaluation			√		
Admission as Evidence				√	
Kent et. al, 2006					
Collection		√			
Examination			√		
Analysis			√		
Reporting				√	√
Freiling and Schwittay, 2007					
Pre-Incident Preparation	√				
Pre-Analysis		√			
Analysis			√		
Post-Analysis				√	√

Table 2: Mapping of Activities/Processes into Appropriate Phases

Phase	Activities / Processes	Output
Preparation	• Monitoring authorization and management support, and obtain authorization to do the investigation • Ensuring the operations and infrastructure are able to support an investigation • Provide a mechanism for the incident to be detected and confirmed • Create an awareness so that the investigation is needed (identify the need for an investigation) • Plan on how to get the information needed from both inside and outside the investigating organization • Identify the strategy, policies and previous investigations • Informing the subject of an investigation or other concerned parties that the investigation is taking place	Plan, Authorization, Warrant, Notification, Confirmation
Collection and Preservation	• Determine what a particular piece of digital evidence is, and Identifying possible sources of data • Determine where the evidence is physically located • Translated the media into data • Ensuring integrity and authenticity of the digital evidence e.g. write protection, hashes etc. • Package, transport and store the digital evidence • Preventing people from using the digital device or allowing other electromagnetic devices to be used within an affected radius • Record the physical scene • Duplicate digital evidence using standardized and accepted procedures • Ensuring the validity and integrity of evidence for later use	Crime type, Potential Evidence Sources, Media, Devices, Event
Examination and Analysis	• Determine how the data produced, when and by whom • Determine and validate the techniques to find and interpret significant data • Extracting hidden data, Discovering the hidden data, and Matching the pattern • Recognize obvious pieces of digital evidence and assess the skill level of suspect • Transform the data into a more manageable size and form for analysis • Recognize obvious pieces of digital evidence and assess the skill level of suspect • Confirming or refuting allegations of suspicious activity • Identifying and locating potential evidence, possibly within unconventional locations • Construct detailed documentation for analysis and Draw conclusions based on evidence found • Determine significant based on evidence found • Test and reject theories based on the digital evidence • Organizing the analysis results from the collected physical and digital evidence • Eliminate duplication of analysis • Build a timeline • Construct a hypothesis of what occurred, and Compare the extracted data with the target • Document the findings and all steps taken	Log Files, File, Events log, Data, Information
Presentation and Reporting	• Preparing and presenting the information resulting from the analysis phase • Determine the issues relevance of the information, its reliability and who can testify to it • Interpret the statistical from analysis phase • Clarify the evidence, and Document the findings • Summarize and provide explanation of conclusions • Presenting the physical and digital evidence to a court or corporate management • Attempt to confirm each piece of evidence and each event in the chain each other, independently, evidence or events • Prove the validity of the hypothesis and defend it against criticism and challenge • Communicate relevance findings to a variety of audiences (management, technical personnel, law enforcement)	Evidence, Report
Disseminating the case	• Ensuring physical and digital property is returned to proper owner • Determine how and what criminal evidence must be removed • Reviewing the investigation to identify areas of improvement • Disseminate the information from the investigation • Close out the investigation and preserve knowledge gained	Evidence Explanation, New Policies and Investigation Procedures, Evidence Disposed, Investigation Closed

4. Result Analysis

Based on the mapping process done in section 3.0, we have simplified the overall phases proposed by previous researchers as shown in Fig. 1.

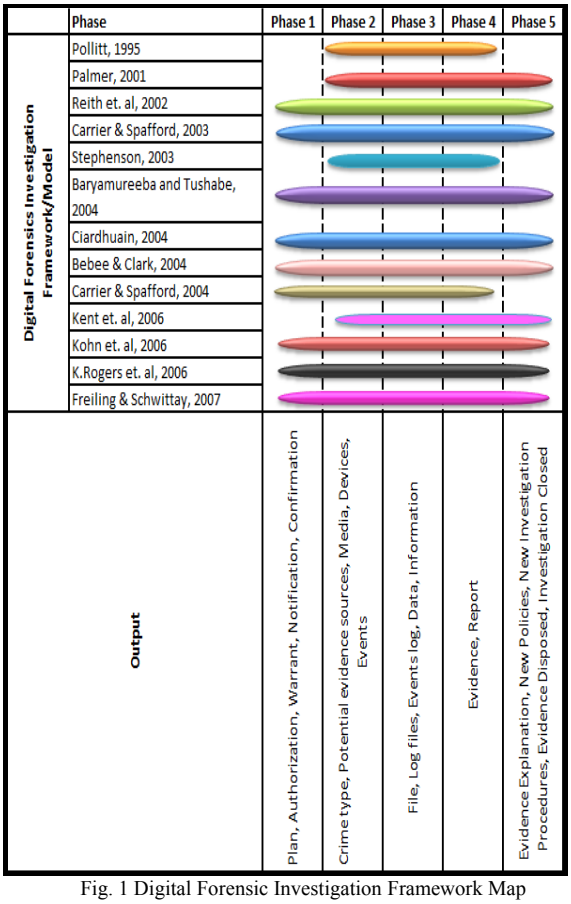

Fig. 1 Digital Forensic Investigation Framework Map

From the analysis shown in Fig. 1, most of the frameworks consist of the critical phases which are Phase 2 – Collection and Preservation, Phase 3 – Examination and Analysis, and Phase 4 – Presentation and Reporting except Phase 1 and Phase 5. Even though, Phase 1 and Phase 5 is not included in some of the framework, the study [1], [2], [5], [7], [8], [9], [11], [17] indicate that both phases are important to ensure the completeness of the investigation. Phases 1 is to ensure the investigation process can be started and run in the proper procedure, and protect the chain of custody of the evidence. While by eliminating Phase 5 will lead to the possibility of the incompletion investigation and no improvement in investigation procedures or policies. Therefore, a good framework should consist of all important phases; Preparation Phase, Collection and Preservation Phase, Examination and Analysis Phase, Presentation and Reporting, and Disseminating the case.

5 Conclusion and Future Works

The mapping process offers a simplified DFIF to establish a clear guideline on steps that should be followed in forensic process and getting the clear idea on the output or product for each of the activity involves during the investigation. These steps should enable us to define a framework that can be used in a forensic investigation. A study of previous proposed frameworks has revealed numbers of steps/processes redundancy in each phases with various terminologies, focus area and framework characteristics. The proposed map attempts to simplify the existing complex framework and it can be used as a general DFIF for investigating all incident cases without tampering the evidence and protect the chain of custody. This proposed map can be furthered map to various incident cases, digital devices and digital evidence in order to optimize the investigation process. A prototype will be developed in order to prove the effectiveness of the framework.

References

[1] Baryamureeba, V., & Tushabe, F. (2004). The Enhanced Digital Investigation Process Model. *Proceeding of Digital Forensic Research Workshop*. Baltimore, MD.

[2] Beebe, N. l., & Clark, J. G. (2004). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. *Proceedings of Digital Forensics Research Workshop*. Baltimore, MD.

[3] Brill AE, Pollitt M. (2006). The evolution of computer forensic best practices: an update on programs and publications. *Journal of Digital Forensic Practice*, 1:3–11

[4] Carrier, B., & Spafford, E. H. (2004). An Event-based Digital Forensic Investigation Framework. *Proceedings of Digital Forensics Research Workshop*. Baltimore, MD.

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

[6] Casey, E. (2004). *Digital Evidence and Computer Crime* (2 ed.). Elsevier Academic Press.

[7] Ciardhuain, S. O. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence* , 3 (1).

[8] Freiling, F. C., & Schwittay, B. (2007). A Common Process Model for Incident Response and Computer Forensics. *Proceedings of Conference on IT Incident Management and IT Forensics*. Germany.

[9] K.Rogers, M., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. *Proceedings of Conference on Digital Forensics, Security and Law*, (pp. 27-40).

[10] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response, *NIST Special Publication 800-86*. Gaithersburg: National Institute of Standards and Technology.

[11] Kohn, M., Eloff, J., & Oliver, M. (2006). Framework for a Digital Forenisc Investigation. *Proceedings of*

Information Security South Africa (ISSA) 2006 from Insight to Foresight Conference. South Afrika.
[12] M.Pollitt, M. (1995). Computer Forensics: an Approach to Evidence in Cyberspace. *Proceeding of the National Information Systems Security Conference*, (pp. 487-491). Baltimore, MD.
[13] McCombie, & Warren. (2003). Computer Forensics: An Issue of Definition. *Proceeding of First Australian Computer, Network and Information Forensics Conference*. Perth.
[14] McKemmish, R. (1999). *What is Forensic Computing?* . Canberra Australian Institute of Criminology .
[15] NIJ. (2002). Results from Tools and Technologies Working Group. *Goverors Summit on Cybercrime and Cyberterrorism*. Princeton NJ.
[16] Palmer, G. (2001). *DTR - T001-01 Technical Report*. A Road map for Digital Forensic Research. Utica, New York.
[17] Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal Digital Evidence* , 1 (3).
[18] Roger, M. (2006). *DCSA:Applied Digital Crime Scene Analysis*. In Tipton & Krause.
[19] Stephenson, P. (2003). A Comprehensive Approach to Digital Incident Investigation. *Elsevier Information Security Technical Report*. Elsevier Advanced Technology.
[20] Willassen, S. Y., & Mjolsnes, S. F. (2005). *Digital Forensics Research*. Retrieved December 30, 2007, from www.telenor.com/telektronikk/volumes/pdf/1.2005/Page_092-097.pdf
[21] Carrier, B. D. (2006). A Hypothesis-based Approach to Digital Forensic Investigations. *CERIAS Tech Report 2006-06*, Purdue University, Center for Education and Research in Information Assurance and Security, West Lafayette.

Siti Rahayu Selamat is currently a PhD student at the Universiti Teknikal Malaysia Melaka, Malaysia. She holds Bachelor of Computer Science (Hons) from Universiti Teknologi Malaysia, Malaysia and a Master degree in Computer Science with honours from the Universiti Malaya, Malaysia. Her research interests include network forensic, intrusion detection, network security and penetration testing

Robiah Yusof is currently a PhD student at the Universiti Teknikal Malaysia Melaka, Malaysia. She holds Bachelor of Computer Studies (Hons) from Liverpool John Moore's University, UK and a Master degree in Computer Science with honours from the Universiti Kebangsaan Malaysia, Malaysia. Her research interests include intrusion detection, network security, penetration testing and network forensic.

Shahrin Sahib received the Bachelor of Science in Engineering, Computer Systems and Master of Science in Engineering, System Software in Purdue University in 1989 and 1991 respectively. He received the Doctor of Philosophy, Parallel Processing from University of Sheffield in 1995. He is a professor and Dean of Faculty of Information Technology and Communication at the Universiti Teknikal Malaysia Melaka. His research interests include network security, computer system security, network administration and network design. He is a member panel of Experts National ICT Security and Emergency Response Center and also Member of Technical Working Group: Policy and Implementation Plan, National Open Source Policy