FACTORS INFLUENCING THE ADOPTION OF DIGITAL FORENSIC IN MALAYSIAN ORGANISATION: A SYSTEMATIC REVIEW USING PRISMA

Khalilul Nishad Abdullah[1], Siti Nuur-Ila Mat Kamal[2*], Mohd Shamsul Mohd Shoid[3], Yan-Ling Tan[4], Nurkhairany Amyra Mokhtar[5]

[1,2] *Information Science Studies, College of Computing, Informatics and Mathematics, Universiti Teknologi MARA Cawangan Johor, Kampus Segamat, Malaysia*

[3] *Information Science Studies, College of Computing, Informatics and Mathematics, Universiti Teknologi MARA Cawangan Selangor, Kampus Puncak Perdana, Malaysia*

[4] *Faculty of Business and Management, Universiti Teknologi MARA Cawangan Johor, Kampus Segamat, Malaysia*

[5] *Mathematical Sciences Studies, College of Computing, Informatics and Mathematics, Universiti Teknologi MARA Cawangan Johor, Kampus Segamat, Malaysia*

*Corresponding Author

Email: [1]khalilulabdullah@gmail.com, [2*]sitin509@uitm.edu.my, [3]shamsulshoid@uitm.edu.my, [4]tanya163@uitm.edu.my, [5]nurkhairany@uitm.edu.my

Received: 30 October 2025
Accepted: 7 January 2026

ABSTRACT

The digitalisation of devices and systems has become a defining feature of technological advancement in the modern era. This particular scenario is considered to have a major impact on the increasing recognition of Digital Forensics (DF) as a valuable tool for investigative procedures in assisting organisations, especially Malaysian Information Technology Organisations (MITO) in resolving issues related to digital incidents that occur in their organisations. However, MITO in Malaysia who are not exposed to the use of DF in developing countries have a negative impact on digital evidence investigations which can reduce the time to resolve digital incidents, cost effective, impactful, and efficient. This paper looks at the variables that MITO in Malaysia can consider when deciding whether to adopt Digital Forensics or not. PRISMA is the reference methodology used in this study to determine these factors and create an early adoption model. Eleven factors that influence the decision to adopt Digital Forensics were identified by the methodology. According to the premise of the TOE framework, these factors are organised into three dimensions: technology, organisation, and environment. This study contributes by addressing the key motivators that characterise the adoption of innovations at the organisational level, where they will then be used to develop an adoption model, and an understanding of the Digital Forensics context.

Keywords: Computational Forensic, Computer Forensic, Cyber Forensic, Digital Forensic, Electronic Record Forensic

1.0 INTRODUCTION

The proliferation of digital devices and systems has been a defining feature of the rapid evolution of the information age. As a result, there is a growing demand for Digital Forensics (DF), a useful tool that helps organisations in respond to various types of cybercrime and produce digital evidence that can be admissible in court through legitimate evidentiary investigation. The rate at which DF technologies are being incorporated into the technological structure of organisations in developing countries is not encouraging, despite the benefits that can be realized from DF technologies (Aswami et al., 2012; Kasun et al., 2016; Khuram et al., 2014). IT companies are among the businesses needed in developing countries to deal with digital incidents. Their expertise in identifying and mitigating cybersecurity threats has contributed significantly to recovery efforts, strengthening system security for prevention in the future. But only a small proportion of these businesses have integrated and adopted DF into their company systems to facilitate fast, affordable, effective, and low-impact digital investigations (Aswami et al., 2012; Aswami & Izwan, 2008).

Rafizah and Aishah (2013) reported an increasing demand for DF investigations and incident cases to be handled by Cyber Security Malaysia (CSM), an organisation under the Ministry of Science, Technology and Innovation that acts as one of the authoritative bodies in matters related to cyber and digital security. This situation has shown how dependent businesses are on DF technical assistance. In this situation, the problem that makes DF investigations ineffective has worsened the situation (Aswami et al., 2012; Aswami & Izwan, 2008; Sarah, Miratun, & Zabri, 2018). This is because the process has become very time-consuming and this has resulted in slow response to reported incidents. At this point, the inefficiency and loss of productivity experienced by companies due to business operations being disrupted during the investigation. In fact, if the DF function is contracted out to an external party, the company's privacy issues will be easily affected such as data leakage (Daniel & Hart, 2004). As a result, businesses need to understand the role that DF plays in their workplace is particularly important. The ability of a company to respond quickly to security incidents will be enhanced by having a DF (Elyas et al., 2015; Suhaila et al., 2011; Mankantshu, 2013; Saleh, 2013). When an incident occurs, efforts to investigate it can be done quickly and effectively so that a response can be made without delay (Mouhtaropoulos et al., 2014; Mouhtaropoulos et al., 2013). The weak nature of DF practices in organizations is generally found to stem from a lack of strong understanding and guidance on DF practices (Hamdi, 2011; Suhaila et al., 2011). Aswami et al. (2012) and Aswami and Izwan (2008) fairly explored the topic of DF in the Malaysian context, especially to offer a solid understanding of the factors that can help organisations in adopting DF. Therefore, it is expected that acknowledging this element will solve the aforementioned problems.

This study aims to establish a framework that can be seen as the motivation that influence the use of DF by a Malaysian Information Technology Organisations (MITO). The proposed model is expected to help the Malaysian MITO in using DF while also serving as a reference for the company's decision makers to better understand the evaluation of DF use. Furthermore, this study is expected to fill the gap in the DF domain in the context of organisational adoption, as DF is mainly being studied from a technical perspective. According to Pangalos et al. (2010), the current effort is in line with the proposals put forward by proponents of the notion that the forensic field should be expanded to encompass multiple perspectives and sustain the continuous development of the field.

2.0 RELATED STUDIES

Many researchers have examined the use of DF, (Hamdi, 2011; Obwaya, 2011; Suhaila et al., 2011). However, Yang et al. (2015) stated that to accurately reflect the underlying characteristics of an innovation, it is important to consider technological, organisational, and environmental factors when studying innovation adoption. As a result, these studies fail to

offer a comprehensive analysis of the factors that influence the use of DF. For example, Hamdi (2011) conducted a quantitative study to examine differences in Digital Forensics procedures used by large American local police departments. However, the study found that it was limited to organisational and environmental considerations. As a result, this study presents a theoretical perspective that provides a more comprehensive range of important elements that represent unique adoption contexts.

3.0 LITERATURE REVIEW

3.1 The Current Scenario of Digital Forensics in Malaysian Information Technology Organisations

The topic of DF has been thoroughly examined in the Malaysian context, particularly in relation to MITO 's decision to adopt DF (Suhaila et al., 2011). In the context of an American police agency, Hamdi's (2011) study on DF adoption and practice only examined organisational and environmental factors. However, it becomes crucial to consider the holistic aspects of organisational, technological, and environmental factors when researching how innovation is adopted by organisations (Yang et al., 2015). Incorporating these variables yields a more thorough comprehension of innovation's attributes, particularly in developing nations (Riyadh et al., 2009; Hemla et al., 2014). Thus, in the context of developing nations, investigating factors that consider the distinctive qualities of DF can be highly valuable in encouraging MITO to use it. The goal of this study is in accordance with the suggestions made by Pangalos and Katos (2010), supporting the expansion of DF research to incorporate a variety of viewpoints and guarantee the discipline's continued maturity.

According to a study by Suhaila et al. (2011), MITO still incorporate DF at a low rate. This is due to the lack of awareness, expertise, and knowledge in the field, and the possibility of implementation costs being the bigger barrier. Greater corporations are aware of the significance of implementing Digital Forensics when it comes to security risk management. Smaller MITO businesses, however, frequently undervalue the significance of keeping records and proof in case future digital investigations are necessary (Sinangin, 2002). Companies that have incorporated forensic functions into their operations reap advantages from having the capacity to gather, preserve, scrutinise, and assess information or proof to appraise the condition of their systems and determine if private and confidential data has been exposed. Digital Forensics techniques and methodologies can aid not only in Digital Forensics investigations but also in the analysis of security and operational incidents and in the recovery of systems that have already been implemented (Radack, 2009).

Furthermore, not as much is being said in Malaysia about problems pertaining to the practice of Digital Forensics. The bulk of the research concentrated on how prepared a nation, business, or organisation was for Malaysian Digital Forensics. Because resources are limited, there is not a framework that could be used by Malaysian decision-makers, particularly MITO, to help them explore, assess, and evaluate the variables influencing the adoption of Digital Forensics innovations in their operational environments. The research model that has been suggested for this study will help them in making decisions about implementing Digital Forensics and will also help them to anticipate factors that might improve the process of adopting innovations. Thus, this study may lay the groundwork for Malaysian relevant organisations to adopt Digital Forensics practices. The study may offer a better understanding of the successful adoption of Digital Forensics, which may encourage more agencies, including modern organisations from various sectors, particularly the MITO, to adopt Digital Forensics as their work practice, given that the guidelines for the adoption of Digital Forensics practice are currently available.

3.2 Digital Forensic

Several experts have defined Digital Forensics, and they all have different but equally insightful opinions about what it covers and why. The foundation was established by Pollitt (2007), who defined DF as a synthesis of science and law that involves applying engineering and science to legal issues involving digital evidence. Fundamentally, it entails the careful examination of digital data with the ultimate objective of generating legally acceptable results. Palmer (2001) provided a widely accepted definition of Digital Forensics (DF), characterizing it as the use of scientifically developed techniques for digital evidence collection, preservation, verification, analysis, and presentation. Scholars in the field have agreed upon this definition, which was developed at the Digital Forensic Research Workshop.

The definition was broadened by Willassen and Mjolsnes (2005), who emphasised the legal (results) and scientific (digital investigation) components. The practice of using technically sound, scientifically derived methods and tools for post-event digital information analysis from digital sources is included in their definition. The goal of this procedure is to make it easier to reconstruct events using forensic evidence. Notably, their definition includes event reconstruction for the purpose of analysing security and operational incidents, expanding the scope beyond criminal elements.

Another perspective is found in the context of curation, archiving, and preservation, where DF is regarded as an important source of methods and instruments for preserving digital evidence of the past (John, 2012). DF plays a critical role in the organisational context for effectively handling digital incidents, especially in MITO. To ensure the admissibility of evidence, the sub-processes involved in digital investigation, such as identifying, extracting, collecting, documenting, and interpreting digital evidence, must follow clear, repeatable protocols (Stephen et al., 2011). In the end, Digital Forensics (DF) is a tool that helps find and preserve digital evidence efficiently for prosecution, reducing the amount of time that digital investigations take and the effect that it has on operational activities (Hamdi, 2011; Obwaya, 2011). To summarise, the present study acknowledges Digital Forensics (DF) as the utilisation of specialised knowledge in advanced technology-based criminal investigations to guarantee the effective identification and preservation of digital evidence from digital sources for legal intent.

In order to build a strong foundation for knowledge advancement and theory development in DF in Malaysia, a thorough review of prior research is necessary. Notably, little research has been done expressly to look at DF in relation to MITO. Studies that have already been done primarily emphasise the benefits of DF and evaluate how prepared an organisation is to adopt it.

3.3 Malaysian Information Technology Organisations

Malaysian Information Technology Organisations (MITO) is a broad sector and not a single organisation (Awamleh & Ertugan, 2021). It comprises of government digital economy agencies, IT support and service companies, ICT industry and investment agencies, technology development & foresight agencies, and digital marketing and creative digital agencies. The government digital economy agency in Malaysia provides strategic leadership and implementation for the country's digital transformation, particularly under the Malaysia Digital Economy Action Plan (MyDIGITAL) covering 2021-2030. Among the organisations operating under this industry are the Malaysian Digital Economy Corporation (MDEC), the Malaysian Communications and Multimedia Commission (MCMC), and CyberSecurity Malaysia (CSM). These organisations play a role in initiating a formal institutional framework to promote and regulate the digital economy in Malaysia (Edrak et al., 2022). These organisations play an important role in driving digital adoption among small and medium enterprises (SME), support digital entrepreneurs, and attracting digital investments,

particularly through initiatives aligned with Malaysia strategic plan (Loh et al., 2021). In addition, these organisations also integrate cloud-first policies, whole-of-government digital architecture, and public sector transformation strategies to improve service delivery, data governance, and the use of smart infrastructure (Ahmad et al., 2025). These organisations work through enterprise architecture and sector coordination mechanisms to avoid duplication and ensure integrated e-government services and ease of access for the public. These institutions reflect a coordinated governance framework where public organisation unify policy direction and cybersecurity fundamentals to strengthen the transformation of Malaysia's digital economy.

Meanwhile, IT support and services companies such as IBM Malaysia and Tata Consultancy Service in Malaysia play a key role in enabling digital transformation for businesses, especially SMEs, by providing cloud solutions, system integration, managed services, cybersecurity, and data analytics support. These services help organisations improve operational efficiency, support product development, and expand sales and marketing capabilities as part of their digital adoption strategies (Lee et al., 2021). In Malaysia, the ICT industry and investment agencies play a key role in coordinating and promoting the development of the digital sector and high-value investments that form a key pillar of the national strategy under MyDIGITAL. These organisations, notably the Malaysian Investment Development Authority (MIDA), operate through the Digital Investment Office (DIO), which is a collaborative platform designed to facilitate and coordinate digital investment (Felker et al., 2023).

Next, technology development and foresight agencies in Malaysia act as strategic enablers for the country’s long-term innovation capacity by prioritising the high-tech sector, guiding the direction of research and development, and incorporating future thinking into national planning. Agencies such as the Malaysian Industry-Government Group for High Technology (MIGHT) and the Malaysian Institute of Microelectronic Systems (MIMOS) are organisations that fall under this industry. MIGHT, established in 1993, functions as a high-level consultative body that coordinates government, academia, and industry to set strategic technology roadmaps, national R&D priorities, and advanced technology policies (Felker et al. 2007).

Finally, digital marketing and creative digital agencies in Malaysia empower businesses to play a role in building brand identity, increasing online visibility and engaging customers through data-driven and multimedia strategies. Among the organisations operating under this industry are 2Stallions and INFLUASIA. Digital marketing in Malaysia acts as a key facilitator in enhancing competitiveness and supporting creative output through storytelling, visuals, and interactive platforms.

3.4 Technology Organization Environment (T-O-E) Theory

The T-O-E Framework provides an organised method for organisations to evaluate the adoption of technological innovations. It was developed by Xu et al. (2004) and is comparable to models by Salwani et al. (2009). It highlights how important internal and external elements are in shaping adoption decisions, including organizational size, strategy, and environmental dynamics. An organisation's readiness to adopt new technologies is shaped by three main factors: technology, organisation, and environment. These factors can range from technological capabilities to regulatory landscapes. The T-O-E framework has drawbacks even with its extensive application. Academics have observed shortcomings in the definitions of the variables and the capacity of the framework to elucidate variations in adoption rates in diverse settings. More investigation is needed to improve the framework and incorporate new factors that could increase its capacity to explain phenomena and make it more applicable to a range of organisational contexts.

Within the T-O-E framework, technology development refers to the variety of technologies that an organisation can use; on the other hand, the organisational context emphasises characteristics like creativity, resources, and hierarchical dynamics that impact adoption readiness. Adoption decisions are further influenced by the environmental context, which includes industry conditions and regulatory frameworks. It introduces elements such as government incentives and market competition. The T-O-E framework has drawn criticism for its limited applicability to small and medium-sized businesses and the need for further refinement in variable definitions, despite offering a comprehensive perspective on adoption.

The T-O-E framework is still frequently used to analyse technology adoption in spite of its drawbacks, especially when taking organisational, environmental, and technological factors into account. In order to improve its explanatory power, researchers have called for more study to address its shortcomings and include other variables, such as sociological and cognitive factors. Given the circumstances, the T-O-E framework is a useful tool for companies trying to manage the challenges of adopting technological innovations and match their plans with the state of the environment.

4.0 METHODOLOGY

This study used the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) statement by Moher et al. (2010) stating that this method is to review and analyse the literature on technology use and DF adoption before developing an initial theoretical model to investigate the factors influencing the MITO's assessment of DF adoption. Through the use of statistical techniques together with a systematic and explicit approach, the structured review presents integrated results from the included studies (Moher et al., 2010).

This methodology has been widely used in many different academic disciplines to compile a broad literature review (Vaismoradi et al., 2016). The PRISMA methodology used in this study is divided into four main phases. Phases 1 to 4 are identification, screening, qualification, and inclusion. Phase 1 activities include collecting papers, building a reference database, and conducting a literature search using keywords as descriptors.

Two online databases were selected based on their applicability to the disciplines of information systems and DF. Web of Science and Scopus were the online databases selected. "Computational Evidence, Computational Forensic*, Computational Investigation*, Computer Evidence*, Computer Forensic*, Computer Investigation*, Cyber Evidence*, Cyber Forensic*, Cyber Investigation, Digital Evidence*, Digital Forensic*, Digital Investigation*, Electronic Record* Evidence*, Electronic Record* Forensic*, Electronic Record* Investigation*, Forensic* Computer, Adapt, Adaptation, Adopt, Adoption, Organization*, Institution*, Firm*, Company*, Agency*, Organisation" are the keywords used to query the database.

Phase 2 and Phase 3 involve screening and selection of studies for eligible papers. Phase 2 screening focuses on removing redundant and duplicate papers from the sample. Removal of unnecessary studies is done during the same phase as screening on abstracts and titles. A manual removal process was used in Phase 3 to determine eligibility by examining the full-text papers retrieved from Phase 2.

The final stage of the methodology, known as Phase 4, involves data extraction and formulation. The remaining papers were sorted in this phase, and potentially important factors that reflect the basic ideas of the TOE framework were found. Screening, removal, and selection were performed according to the established inclusion criteria, as shown in Table 1, to ensure the quality value of the papers. Figure 1 shows the process of systematic review.

Table 1. Systematic Review Inclusion Criteria

Inclusion Criteria	The articles were collected from 2005 to the present (DF is a relatively new database, so there are no restrictions on the time ranges considered during the search).
	Only papers presented at international conferences and published in scholarly journals
	The use of a keyword in the abstract or title
	Full text article
	The articles were collected from 2005 to the present (DF is a relatively new database, so there are no restrictions on the time ranges considered during the search).

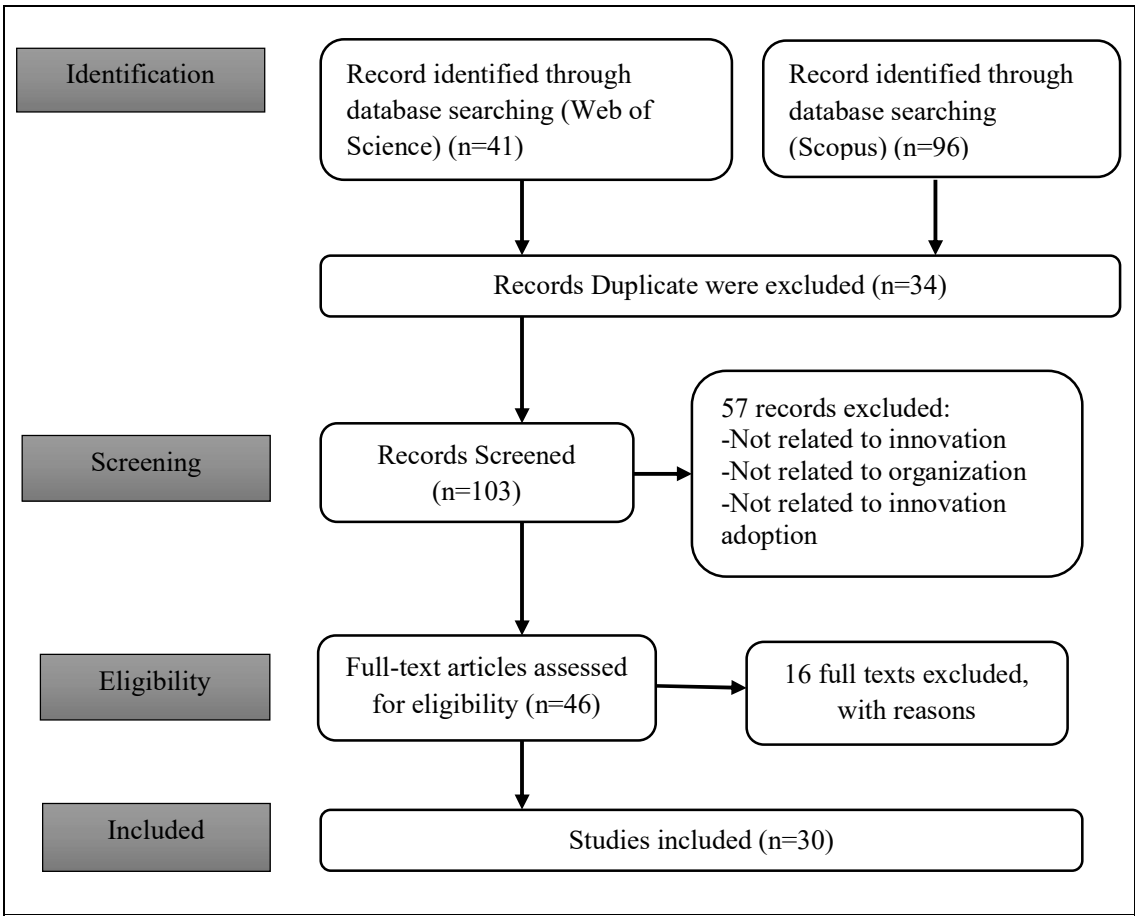

Fig 1. Flow chart of the systematic review

5.0 FINDINGS

A total of 137 scholarly articles were found throughout the search. The screening procedure was guided by exclusion criteria. After similar papers with duplicate information were eliminated, the screening process left with 103 potential articles. Abstract and title screening then formed the next step in the screening procedure. Titles and abstracts that were not related to innovation, organisational innovation, and innovation adoption were eliminated. However, manual full-paper skimming was conducted for 46 potentially relevant primary studies, guided by the inclusion and exclusion criteria.

The 30 articles that emerged from this review were ultimately used in the primary study. The first phase was to collect as much information as possible about technology use, focusing

on DF practices and adoption factors. Next, factors that impact adoption behaviour at the organisational level were identified through an analysis. Three dimensions of multiple perspectives reflecting the underlying assumptions of the TOE framework were used in the third phase of data extraction to examine relevant findings. Finally, a findings report was generated by suggesting and summarizing the extracted data. To ensure the reliability and validity of the rigorous discovery and review process, clear exclusion and inclusion criteria were used. Tables 2 and 3 present a summary of the overall study's conclusions regarding the likely factors influencing the MITO's decision to adopt DF as well as a brief description of each factor.

Table 2. Factors Influencing the Decision of DF Adoption by MITO

Author(s)	Innovation/ Tech Studied	Dimension/Variables									
		Technology				Organisation			Environment		
		RA	COMP	COMX	TMS	INF	CUL	GOV	CP	NP	VS
Ming et al (2010)	RFID	√		√	√						
Yu (2010)	RFID	√	√	√	√				√		
Liu (2010)	E-supply Chain Management								√	√	
Marques et al. (2011)	Medical Records System	√	√	√	√				√	√	
Ifinedo (2011)	E-Business	√	√	√	√						√
Low et al. (2011)	Cloud Computing	√	√	√	√						
Low et al. (2011)	Cloud Computing	√	√		√						
Chi et al (2012)	Health Level Seven (HL7)		√	√	√						
Currie (2012)	EHR System								√	√	
Makena (2013)	Cloud Computing	√	√	√	√					√	
Sila (2013)	E-Commerce			√	√				√	√	
Borgman et al. (2013)	Cloud Computing	√	√	√	√		√		√		
Sila (2013)	B2B E-Commerce			√	√						

Morgan and Conboy (2013)	Cloud Computing	√	√	√							
Hsiu (2014)	E-supply Chain Management				√						
Hui et al (2014)	RFID		√	√	√				√		
Jiunn et al. (2014)	Cloud Computing	√	√	√	√				√		
Nouf et al. (2014)	Cloud Computing	√	√	√	√					√	
Oliveira et al. (2014)	Cloud Computing	√	√	√	√				√		
Hui et al. (2014)	RFID	√	√	√	√				√		√
Klocker et al. (2014)	E-Health								√	√	
Ogan (2015)	Cloud Computing									√	
Yang et al. (2015)	Software as a Service (SaaS)	√	√		√						√
Hossein et al. (2015)	Hospital Information System	√	√	√	√	√			√		√
Abdullah and Clare (2015)	Cloud Computing	√	√	√	√				√		
Yi et al. (2016)	Mobile reservation systems	√	√	√	√						
Salim et al. (2016)	Cloud Computing	√	√		√	√					
Alam et al. (2016)	HRIS		√	√	√			√	√		√
Hossein et al. (2017)	HIS	√	√	√	√	√			√		√
Kamal (2019)	Digital Forensics	√	√	√	√	√	√	√	√	√	√

Frequency/Support	20	22	22	25	4	2	2	16	9	7

According to Grover (1993) and Yang et al. (2015), a thorough and inclusive understanding of the characteristics of innovation requires the integration of factors that consider comprehensive dimensions. So, in order to help MITOs' decision makers allocate organisational, technological, and environmental resources, the factors influencing DF adoption decisions are reviewed using the TOE framework.

Table 3. Description of Factors

Factors	Description
Relative Advantage (RA)	The extent to which people believe that DF technology is better to its predecessor and offers more benefits.
Compatibility (COMP)	The extent to which DF aligns with the existing agency infrastructure, including networks and laboratory systems, as well as the agency's needs, goals, corporate culture, and values.
Complexity (COMX)	The extent to which DF is thought to be comparatively hard to use and understand.
Top Management Support (TMS)	Senior management of an organisation endorsing DF.
Infrastructure (INF)	An infrastructure and system architecture that help the agencies make the most of the DF's capabilities.
Culture (CUL)	A collection of common values, presumptions, beliefs, and behaviours that influence and guide organisational members' attitudes and actions toward DF.
Governance (GOV)	The organisational procedures and frameworks that make forensics possible
Coercive Pressure (CP)	The official government's influence over a new innovation technology that will significantly impact the agency's adoption of DF
Normative Pressure (NP)	An influence from those working with professional organisations to get agencies to adopt similar innovations.
Vendor Support (VS)	The degree of assistance rendered by the outside DF vendor both during and following the adoption.

6.0 INITIAL MODEL

6.1 Technological Dimension

Technology encompasses both internal and external aspects that are relevant to the company, as stated by Oliveira and Martins (2011). Within the domain of DF, it denotes an aspect of the agency's technological infrastructure, such as an extremely specialised software tool or a piece of hardware intended expressly for forensic use.

Relative advantage, complexity, and compatibility are the factors taken into consideration under this dimension, which reflects the features of Digital Forensics technology with the systematic literature review in Table 2. The term "relative advantage" describes the extent to

which agency decision-makers perceive potential benefits from Digital Forensics. They characterise the greater advantage of Digital Forensics as the replacement of traditional investigative and scientific problem-solving approaches with new technologies (Mark, 2010; Suhaila et al., 2011). According to Kari and Venter (2015), complexity is defined as the inherently difficult nature of Digital Forensics, an aspect of the non-uniformity of forensic tools that necessitates the use of expensive and sophisticated Digital Forensics tools to solve technical incompatibility problems and a lack of standard operating procedures for conducting Digital Forensics, and the requirement for new and updated skills and expertise to perform Digital Forensics effectively. The degree to which a piece of technology is compatible with the agency's current infrastructure, goals, current practices, and values and beliefs is referred to as compatibility (Rogers, 1995).

6.2 Organisational Dimension

The term "organisational dimension" refers to an organisation's internally measurable attributes, such as infrastructure, culture, governance, size of agency, and support from top management. The degree to which a group of individuals involved in strategic decision making recognises the significance of implementing cutting-edge technology and subsequently has a significant impact on the adoption of Digital Forensics in the agencies is referred to as top management support.

According to Elyas et al. (2015) and Grobler et al. (2010), infrastructure is defined as forensic physical structure that consists of a well-architected network and a well-equipped laboratory with admissible and accepted hardware and software (tools) to enable the companies to conduct Digital Forensics activities, particularly for investigative and non-investigative purposes. Within the framework of this study, culture is defined as a collection of common values, beliefs, presumptions, and practices that influence and direct organizational members' motivation towards Digital Forensics. This, in turn, influences the degree to which the agencies are prepared to accept the innovation.

According to Mankantshu (2013), governance is the distribution of decision-making authority to oversee Digital Forensics operations. It has been determined that governance is a crucial component of the state of Digital Forensics within an organization. The term "size of the companies" refers to the range of resources that the companies own or are able to provide, such as their infrastructure and technical staff count.

6.3 Environmental Dimension

According to Olutoyin and Flowerday (2016), the term "environmental factors" refers to both internal and external elements that may exert pressure or support (Marimuthu et al., 2011) and originate from the environment, which includes the government, vendors, suppliers, and customers. Similarly, Hamdi (2011) argued that this aspect is the external force that has had the biggest influence on the use of Digital Forensics.

This dimension shows the current working environment that Malaysian IT companies are in, which could have an impact on how Digital Forensics are implemented there. Within the framework of this investigation, the external factors affecting the agencies comprise external normative and coercive pressures in addition to external vendor support. An external force that originated from government entities as an authorized body that controls the IT company and the companies' well-being is referred to as coercive pressure.

Given that the IT companies in this study are generally interrelated and directly under the jurisdiction of sovereigns, there may be normative pressure to adopt Digital Forensics. DiMaggio and Powell (1983) define normative pressure as the influence that vendors, consumers, and commercial, trade, and professional associations have on a company's

decision to embrace a particular innovation. According to Alsaad et al. (2014), Hamdi (2011), Oliveira and Martins (2011) and Yang et al. (2013), and other researchers, normative pressures on professionalism occur in the context of organisational adoption studies. These pressures subject an organisation's behaviours to shared values and the norms of other organisations through relational channels of their social network.

According to the current study, vendor support refers to the extent to which an external Digital Forensics vendor is able to offer services, such as comprehensive consulting engagements and technical and training support. Digital Forensics, as a relatively new and developing technology in the field, presented a number of difficulties for the practicing organisation (Hoss & Carver, 2009; Karie & Venter, 2015; Nance & Ryan, 2011). Consequently, it is essential to rely on vendors for such technical, training, and advisory support.

The company would rely on the vendor for specialised forensic skill and software training even though the vendor offered and supplied updates and new technical needs (Derek et al., 2008; Trenwith, 2013). According to Jiunn et al. (2014), perceived technical competence reflects both the technical staff members' abilities and their knowledge of cutting-edge technology (Hossein, Mehrbakhsh, & Othman, 2015; Jiunn et al., 2014; Rahayu & Day, 2015).

Perceived technical competence, as used in this study, refers to the extent to which employees have the specialised knowledge and understanding of Digital Forensics necessary to carry out forensic tasks and meet forensic objectives. Figure 2 show the initial model.

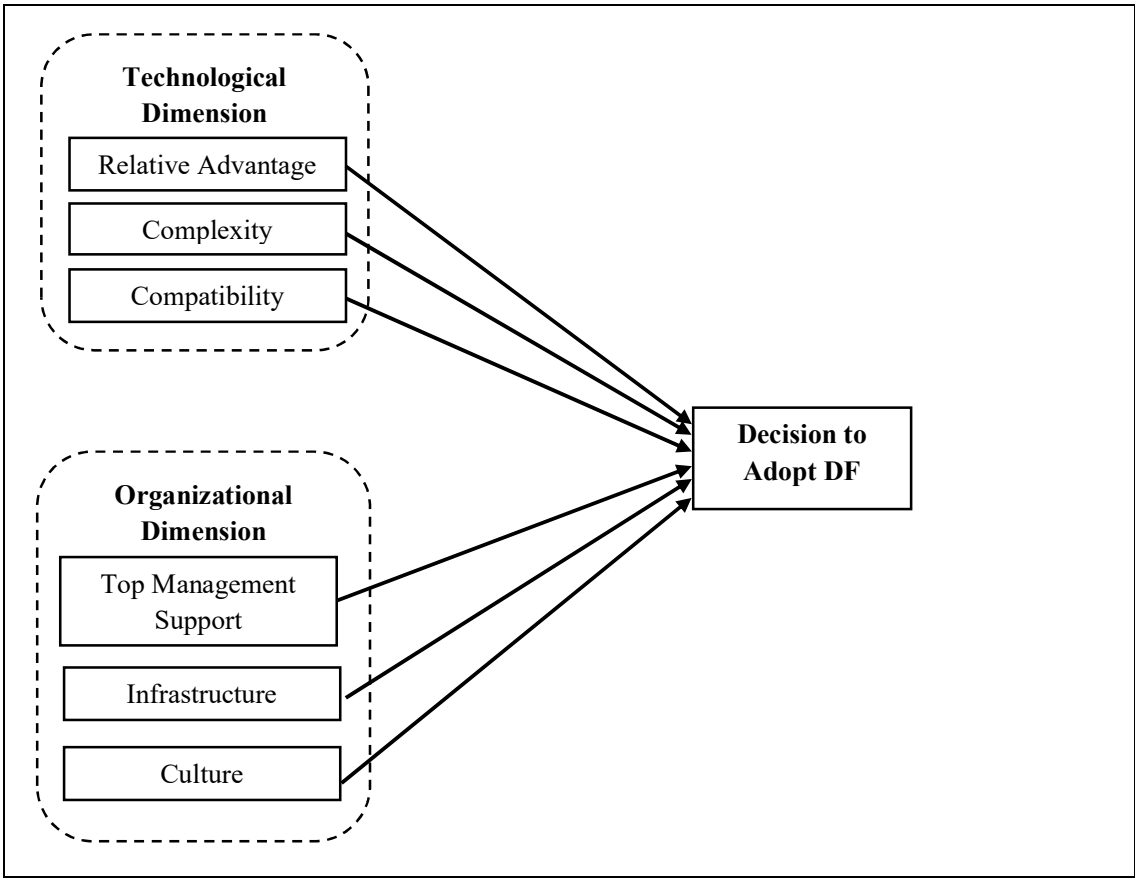

Fig 2. *Initial Digital Forensic adoption model*

7.0 CONCLUSIONS

This paper aims to provide the reader with a comprehensive understanding of the factors considered by the MITO when deciding whether to adopt Digital Forensics. The study identifies 6 factors that the agency's decision-makers need to consider when assessing whether to implement Digital Forensics in their organisation using the PRISMA approach. The first Digital Forensics adoption model was created by classifying these variables into two dimensions: technology and organisation.

The environmental dimension was not used in this model because it did not contribute significantly to this study. Among the characteristics for this dimension are vendor support, normative pressure, and coercive pressure. These characteristics do not influence MITO's decision to adopt DF. This is because MITO itself is a vendor and requires less support than other vendors. Organisations under MITO do not experience normative pressure because resource constraints and skill gaps make organisations focus on practical technological factors rather than mimetic pressure from competitors, making normative pressure insignificant. A Malaysian forensics study in 2022 found that normative pressure was not significant, indicating that organisations adopted based on internal capabilities amidst weak institutional enforcement (Abdullah et al., 2024). For coercive pressure, in developing countries, government regulations exist but face inconsistent implementation due to limited resources or bureaucratic inertia, making coercive pressure ineffective for innovations such as digital forensics (Lu & Wang, 2023). Organisations may comply symbolically without full acceptance because they prioritise cost-benefit analysis over mandate.

The governance in organisation dimension was not used because of it often appears to have limited impact on innovation adoption within a firm when internal operational factors such as resource availability and technological readiness dominate the decision-making process rather than formal structures (Malek et al., 2024). In MITO in developing countries including Malaysia, governance has less impact when institutional enforcement is weak and the organization relies too much on top management support or perceived benefits of innovation. Short-term market pressures that prioritize speed over structured governance thus reduce its influence on adoption decisions.

The first model will be created as a component of an ongoing research project using a quantitative descriptive research methodology with the IT organization serving as the unit of analysis. Research on technology adoption issues at the organizational level has shown that a quantitative approach is common (Choudrie & Dwivedi, 2005). For this reason, this study conducts a theoretical analysis as well as identifies the key elements that will influence the decision of Malaysian IT companies to adopt Digital Forensics. Finally, a survey instrument in the form of a questionnaire will be used to validate the proposed theoretical model among company decision-makers.

This paper contributes to the body of knowledge by examining the factors that influence the adoption of Digital Forensics innovations and helps to develop a framework that can be used as a guide or idea to help decision-makers in organisations better understand the decision to adopt Digital Forensics technologies.

ACKNOWLEDGEMENTS

This study was funded by Ministry of higher education (MOHe) through Fundamental Research Grant scheme (FRGS) (FRGS/1/2023/SS02/UITM/02/9).

REFERENCES

Aswami Ariffin, Jill, S., & Husin Jazri. (2012). Digital forensics institute in Malaysia: the way forward. *Digital Evidence and Electronic Signature Law Review, 9*(8), 51–57.

Abdullah Alhammadi, Stanier, C, & A. E. (2015). The determinants of cloud computing adoption in Saudi Arabia. In W. D. C. & Z. Jan (Eds.), *Second International Conference on Computer Science & Engineering* (CSEN 2015) (pp. 55–67). Dubai.

Abdullah, K. N., Mat Kamal, S. N. I., Ibrahim, O., Yan Ling, T., Mokhtar, N. A., & Mohd Shoid, M. S. (2024). adoption of digital forensic practice: a framework development for Malaysian organizations. *Journal of Electrical System, 20*(10). https://journal.esrgroups.org/jes/article/view/6437

Alam, M. G. R., Masum, A. K. M., Beh, L. S., & Hong, C. S. (2016). Critical factors influencing decision to adopt human resource information system (HRIS) in hospitals. *PLoS ONE, 11*(8), 1–22.

Al-Isma'ili, S., Li, M., Shen, J., & He, Q. (2016). *Cloud computing adoption determinants: an analysis of Australian SMEs*.

Alkhater, N., Wills, G., & Walters, R. (2014). Factors influencing an organisation's intention to adopt cloud computing in Saudi Arabia. In *2014 IEEE 6th international conference on cloud computing technology and science* (pp. 1040-1044). IEEE.

Alsaad, A. K. H., Mohamad, R., & Ismail, N. A. (2014). The moderating role of power exercise in b2b e-commerce adoption decision. *Procedia - Social and Behavioral Sciences, 130*, 515–523. http://doi.org/10.1016/j.sbspro.2014.04.060

Aswami, M. A. F., & Izwan, I. I. (2008). Digital forensics in Malaysia. Digital Evidence and Electronic Signature Law Review, 5, 161–165.

Borgman, H. P., Bahli, B., Heier, H., & Schewski, F. (2013). Cloudrise: Exploring cloud computing adoption and governance with the TOE framework. In P*roceedings of the Annual Hawaii International Conference on System Science*, 4425–4435.

Chen, S. J., & Chen, S. M. (2007). Fuzzy risk analysis based on the ranking of generalized trapezoidal fuzzy numbers. *Applied Intelligence, 26*(1), 1-11.

Chua, D. (2014, April 25). New wave of choreographers. *New Straits Times*, p.7.

Chi, H. L., I, C. L., Jin, S. R., *&* Jehn, S. Y. (2012). Critical factors influencing hospitals' adoption of hl7 version 2 standards: An empirical investigation. J*ournal of Medical Systems, 36*(3), 1183–1192.

Choudrie, J., & Dwivedi, Y. K. (2005). Investigating the research approaches for examining technology adoption issues. Journal of Research Practice, 1(1), 1–10.

Currie, W. L. (2012). Institutional isomorphism and change: The national pro gramme for IT 10 years on. *Journal of Information Technology, 27*(3), 236-248.

Daniels, D. J., & Hart, S. V. (2004). Forensic Examination of digital evidence: A guide for law enforcement. *U.S. Department of Justice Office of Justice Programs National Institute of Justice Special, 4*4(2), 634–111. http://doi.org/10.3408/jafst.7.95.

Derek, B., Francine, F., Ewa, H., & Oscar, B. (2008). Computer forensics - past, present, and future. *Journal of Information Science and Technology, 5*(3), 43–59.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Revie,* 147-160.

Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness expert perspectives on theoretical framework. *Journal of Computers & Security, 52*, 70–89.

Gomez, M.M., Sierra, J.M.C., Jabaloyes, J., & Zarozo, Manuel. (2010). A multivariate method for analyzing and improving the use of student evaluation of teaching questionnaires: A case study*. Quality Quantitative*. doi: 10.1007/s11135-010-9345-5.

Gunkel, M. (2008). *Guidelines for academic writing*. http://www.im.ovgu.de/im_media/down Loads/examinations/academic_paperwriting_MG.pdf

Grobler, C. P., Louwrens, C. P., & Von Solms, S. H. (2010a). A framework to guide the implementation of proactive digital forensics in organizations. In ARES 2010 - 5th I*nternational Conference on Availability, Reliability, and Security,* 677–682.

Grover, V. (1993). An empirically derived model for the adoption of customer-based interorganizational systems. Decision Sciences, 24(3), 603–640.

Hamdi, Y. (2011). *The Response of American police agencies to digital evidence* [Doctoral thesis University of Central Florida, USA].

Hemlata, G., Hema, D., & Raoot A. D. (2014). Review on IT adoption: insights from recent technologies. *Journal of Enterprise Information Management, 27*(4), 488–502.

Hoss, A. M., & Carver, D. L. (2009). *Weaving ontologies to support digital forensic analysis*.

Hossein, A., Mehrbakhsh, N., & Othman, I. (2015). Organizational decision to adopt hospital information system: An empirical investigation in the case of Malaysian public hospitals. I*nternational Journal of Medical Informatics, 84*(3), 166–188. http://doi.org/10.1016/j.ijmedinf.2014.12.004.

Hossein, A., Mehrbakhsh, N., Shahmoradi, L., & Othman Ibrahim. (2017). Hospital information system adoption: Expert perspectives on an adoption framework for Malaysian Public Hospital. *Computers in Human Behavior, 67*, 161- 189.

Hsiu, F. L. (2014). Understanding the determinants of electronic supply chain management system adoption: Using the technology-organization-environment framework. *Technological Forecasting and Social Change, 86*(2014), 80–92.

Hui, M. L., I-Chun, L., L., T. T. (2014). High-level managers' considerations for RFID adoption in hospitals: An empirical study in Taiwan. *Journal of Medical Systems, 38*(2).

Ifinedo, P. (2011). Internet/e-business technologies acceptance in Canada's SMEs: an exploratory investigation. I*nternet Research, 21*(3), 255–281. https://doi.org/10.1108/10662241111139309

Intan Salwani, M., Marthandan, G., Daud Norzaidi, M., & Choy Chong, S. (2009). E-commerce usage and business performance in the Malaysian tourism sector: empirical analysis. *Information Management & Computer Security, 17*(2), 166-185.9, doi:10.1108/09685220910964027

Jiunn, W. L., David, C. Y., & Yen, T. W. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management, 34*(1), 28– 36.

John, J. L. (2012). D*igital forensics and preservation*. Charles Beagrie Ltd.

Kahraman, C., Cevi, S., Ates, N. Y., & Gulbay, M. (2007). Fuzzy multi-criteria evaluation of industrial robotic systems*. Computer & Industrial Engineering*, 52, 414-433 (2007). doi: 10.1016/j.cie.2007.01.005

Karie, N. M., & Venter, H. S. (2015). Taxonomy of challenges for digital forensics. *Journal of Forensic Sciences, 60*(4), 885–893. http://doi.org/10.1111/1556-4029.12809.

Kasun, D. Z., Keerthi, G., & Ravith, B. (2016). Developing a Digital forensic framework for a third world country. In *International Conference on Advances in ICT for Emerging Regions*.

Khuram, M., Ahmer, U., Kamran, A., & Nadeem, M. (2014). Digital forensic models: A comparative study based in large enterprises of Pakistan. *Research Journal of Recent Sciences, 3*(8), 103–110.

Klöcker, P. N., Bernnat, R., & Veit, D. (2014b). Implementation through force or measure? how institutional pressure shape national e-health implementation programs. Ecis. (2007), 1–16.

Liu, H., Ke, W., Kwok, K.K., Gu, J., & H. C. (2010). The role of institutional pressures and organizational culture in the firm's intention to adopt internet-e*nabled supply chain management systems. Journal of Operations Management, 28*(5), 372–384.

Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial Management & Data Systems, 111*(7), 1006– 1023.

Lu, H., & Wang, J. (2023). Exploring the effects of sudden institutional coercive pressure on digital transformation in colleges from teachers' perspective. *Education and Information Technologies, 28*(12), 15991–16015. https://doi.org/10.1007/s10639-023-11781-x

Makena, J. N. (2013). Factors That affect cloud computing adoption by small and medium enterprises in Kenya. *International Journal of Computer Applications Technology and Research, 2*(5), 517–521.

Malek, W. A., Hussin, N., Ahmad, M. N., Samsudin, A. Z. H., & Jalil, A. (2024). *Corporate computer forensics investigation adoption antecedents in Malaysia's critical information infrastructure agencies* https://ir.uitm.edu.my/view/publication/Journal_of_Information_and_Knowledge_Management_=28JIKM=29.html>

Mankantshu, M. A. (2013). *Investigating the Factors that Influence digital Forensic Readiness in a South African Organisation*.

Marimuthu, M., Omar, A., Ramayah, T., & Mohamad, O. (2011). Readiness to adopt e-business among SMEs in Malaysia. *International Journal of E-Adoption*, 18–36. http://doi.org/10.4018/jea.2011070101.

Mark Pollit. (2010). *A history of digital forensics. IFIP Advances in Information and Communication Technology, 337 AICT*, 3–15. http://doi.org/10.1007/978-3-642-15506-2_1

Marques, A., Oliveira, T., Dias, S. S., and Martins, M. F. O. (2011). Medical records system adoption in European hospitals. *Electronic Journal of Information Systems Evaluation, 14*(1), 89-99.

Mat Kamal, S. N. I. (2019). *Digital forensics adoption model for Malaysian law enforcement agencies* [Doctoral Thesis, Universiti Teknologi Malaysia]. http://eprints.utm.my/98109/1/SitiNuurIlaPSC2019.pdf

Ming, C. T., Lee, W., & Hsin, C. W. (2010). Determinants of RFID adoption intention: Evidence from Taiwanese retail chains. *Information and Management, 47*(5–6), 255–261. http://doi.org/10.1016/j.im.2010.05.001.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2010). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *International Journal of Surgery, 8*, 336–341. http://doi.org/10.1016/j.ijsu.2010.02.007.

Morgan, L., & Conboy, K. (2013). Factors affecting the adoption of cloud computing: an exploratory study. In 2*1st European Conference on Information Systems 2013* (ECIS). Utrecht University. R http://eprints.maynoothuniversity.ie/6652/1/LMFactors-Cloud.pdf.

Mouhtaropoulos, A., & Panagiotis Dimotikalis & Li, C-T. (2013). Applying a Digital Forensic Readiness Framework: Three Case Studies. *IEEE,* 217–223.

Mouhtaropoulos, A., Li, C. T., & Grobler, M. (2014). Digital forensic readiness: Are we there yet?. *Journal of International Commercial Law and Technology, 9*(3), 173–179.

Nance, K., & Ryan, D. J. (2011). Legal aspects of digital forensics: A research agenda. In *Proceedings of the 44th Hawaii International Conference on System Sciences* (pp. 1–6). http://doi.org/10.1109/HICSS.2011.282.

Obwaya, M. (2011). Digital forensics framework for Kenyan Courts of laws [Master thesis, University of Nairobi, South Africa].

Oliveira, T., & Martins, M. (2011). Literature review of information technology adoption models at firm level. *The Electronic Journal Information Systems Evaluation, 14*(1), 110–121. http://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=15666379&AN=65267826&h=+3mBLgsH44TuP+Md6aBOWR03issM0HLuIC10e2bYsd573ACXyFRydASKNeJIVclRbeOPZqZtJv6cXzNTjE4tdA==&crl=c.

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information and Management, 51*(5), 497–510. http://doi.org/10.1016/j.im.2014.03.006

Olutoyin, O., & Flowerday, S. (2016). Successful IT governance in SMES: An application of the Technology – Organisation – Environment theory. S*outh African Journal of Information Management*, 1–8. http://doi.org/http://dx.doi.org/10.4102/sajim.v18i1.696 Copyr.

Palmer, G. (2001, August). A road map for digital forensic research. In *First digital forensic research workshop*, Utica, New York (pp. 27-30).

Pangalos, G., & Katos, V. (2009, September). Information assurance and forensic readiness. In *International conference on e-democracy* (pp. 181-188). Springer Berlin Heidelberg.

Pangalos, G., Ilioudis, C., & Pagkalos, I. (2010). The importance of corporate forensic readiness in the information security framework. In *Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*(pp.12–16).

Pollitt, M. M. (2007, April). An ad hoc review of digital forensic models. In *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)* (pp. 43-54). IEEE.

Radack, S. (2009). Forensic techniques: *Helping organizations improve their responses to information security incidents*. NIST Publications.

Rafizah, A. M., & Aishah, M. N. (2013). *CyberCSI 2nd Half Year 2012 Report*. Cyber Security Malaysia.

Rahayu, R., & Day, J. (2015). Determinant factors of e-commerce adoption by SMEs in developing country: Evidence from Indonesia. *Procedia - Social and Behavioral Sciences, 195*, 142–150. http://doi.org/http://dx.doi.org/10.1016/j.sbspro.2015.06.423

Riyadh, A. N., Akter, Md. S., & Islam, N. (2009). The adoption of e-banking in developing countries: a theoretical model for SMEs. *International Review of Business Research Papers, 5*(6), 212-230.

Rogers, E. M. (1995). *Diffusion of Innovations* (4th). The Free Press.

Saleh, A. A. M. (2013). *A digital forensic readiness component for operational unit* [Master thesis, Universiti Teknologi Malaysia, Malaysia].

Sinangin, D. (2002). Computer forensics investigations in a corporate environment. *Computer Fraud & Security, 2002*(6), 11–14. https://doi.org/10.1016/s1361-3723(02)00610-3

Stephen, D. B., Darrin, J., & Alessandro, S. (2011). Bridging differences in digital forensics for law enforcement and national security. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–6.

Taylor, S. K., Saharuddin, M. M., & Talib, Z. A. (2018). An analysis of digital forensic laboratory development among Malaysia's Law Enforcement Agencies. *International Journal of Computer and Information Engineering, 12*(7), 546-550.

Ramli, N., & Mohamad, D. (2010). On the Jaccard index with degree of optimism in ranking fuzzy numbers. In E. Hullermeier, R. Kruse, & F. Hoffman (Eds.), *Information processing and management of uncertainty in knowledge-based system application* (pp. 383-391). Springer.

Rosen, K.H. (1988). *Discrete mathematics and its applications*. Random House, Inc.

Sila, I. (2013). Factors affecting the adoption of B2B e-commerce technologies. *Electronic Commerce Research,13*. http://doi.org/10.1007/s10660-013-9110-7

Trenwith, P. M., & Venter, H. S. (2013, August). Digital forensic readiness in the cloud. In *2013 Information Security for South Africa* (pp. 1-5). IEEE.

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. J*ournal of Nursing Education and Practice, 6*(5). https://doi.org/10.5430/jnep.v6n5p100

Willassen, S. Y., & S. F. Mjølsnes (2005). Digital forensics research. *Telektronik, 1*, 92-97.

Xu, S., Zhu, K., Gibbs.J.(2004). Global technology, local adoption: A cross-country investigation of internet adoption by companies in the United States and China. *Electronic Markets, 14*(1), 13–24, 2004, doi:10.1080/1019678042000175261

Yang, Z., Kankanhalli, A., Ng, B., Tuang, J., & Lim, Y. (2013). Analyzing the enabling factors for the organizational decision to adopt healthcare information systems. *Decision Support Systems, 55*(3), 764–776. http://doi.org/10.1016/j.dss.2013.03.002

Yang, Z., Sun, J., Zhang, Y., & Wang, Y. (2015). Computers in human behavior understanding SaaS adoption from the perspective of organizational users: A tripod readiness model. *Computers in Human Behavior, 45*, 254–264.

Yi, S. W., Hsie, T. L., Ci, R. L., & Ding, Z. Z. (2016). Factors affecting hotels' adoption of mobile reservation systems: A technology-organization-environment framework. *Tourism Management, 53*, 163–172. http://doi.org/10.1016/j.tourman.2015.09.021

Yu, M. W., Yi, S. W., & Yong, F. Y. (2010). Understanding the determinants of RFID adoption in the manufacturing industry. T*echnological Forecasting and Social Change, 77*(2010), 803–815. http://doi.org/10.1016/j.techfore.2010.03.006