

<sup>1</sup> Khalilul Nishad Abdullah<sup>2</sup> Siti Nur-Ila Mat Kamal\*<sup>3</sup> Othman Ibrahim<sup>4</sup> Yan-Ling Tan<sup>5</sup> Nurkhairany Amyra  
Mokhtar<sup>6</sup> Mohd Shamsul Mohd  
Shoid

## Adoption of Digital Forensic Practice: A Framework Development for Malaysian Organizations



**Abstract:** - The rise in global digitization has made organizations more vulnerable to cyber threats and digital incidents, emphasizing the importance of digital forensics (DF) as a tool for collecting and obtaining reliable digital evidence. Malaysia has seen a 50% increase in cyber incidents among companies in the past year, leading to a higher demand for digital forensics in incident response. However, companies like Desktop Support Project Company (DSPC) struggle to keep up with DF implementation. Their reliance on a central agency for incident response results in inefficiencies and delays. This study investigates the current state of digital forensics in Malaysia, focusing on DSPC. The objective is to create an initial framework for the use of digital forensics. Using the HOT-fit model and Technology-Organization-Environment (TOE) frameworks, this study identifies technological, organizational, and human factors as key drivers of DF adoption. The findings aim to provide a theoretical basis for related companies to evaluate DF adoption, enabling decision-makers to enhance the innovation adoption process and improve their ability to manage digital incidents effectively.

**Keywords:** Digital Forensic, Desktop Support Project Company, Innovation Adoption, Technology Adoption, IS Theories.

### I. INTRODUCTION

The rise in global digitization has made organizations vulnerable to cyber threats and digital incidents. Digital forensics (DF) has become widely acknowledged as a crucial innovation for organizations, aiding in the collection and acquisition of reliable digital evidence through thorough investigations. According to [54] in Malaysia, 50% of companies experienced a cyber-incident within the previous year, leading to an increasing demand for digital incident response using digital forensic. To address these challenges, there is a significant call for the creation of guidelines, frameworks, or models that can aid organizational decision-makers in assessing digital forensics practices. Efficiently discovering and preserving reliable digital evidence from digital sources is crucial, particularly for potential prosecution purposes

In Malaysia, the Desktop Support Project Company (DSPC) faces challenges in staying abreast of the implementation of DF [30]. These companies depend on the focal agency to handle and implement digital incident response for reported cases. However, the increase in demand for forensic analysis has worsened the inefficiencies in DF investigations, leading to delays in addressing reported incidents and disruptions in business operations during the investigation process. To address these challenges, it is crucial for organizations

<sup>1</sup> Information Science Studies, College of Computing, Informatics and Mathematics, Universiti Teknologi MARA Cawangan Johor, Kampus Segamat, Johor, Malaysia. khalilulabdullah@gmail.com

<sup>2</sup> Information Science Studies, College of Computing, Informatics and Mathematics, Universiti Teknologi MARA Cawangan Johor, Kampus Segamat, Johor, Malaysia. sitin509@uitm.edu.my

<sup>3</sup> Faculty of Management, Universiti Teknologi Malaysia, Skudai, Johor, Malaysia. othmanibrahim@utm.my

<sup>4</sup> Faculty of Business and Management, Universiti Teknologi MARA Cawangan Johor, Kampus Segamat, Johor, Malaysia. tanya163@uitm.edu.my

<sup>5</sup> Mathematical Sciences Studies, College of Computing, Informatics and Mathematics, Universiti Teknologi MARA Cawangan Johor, Kampus Segamat, Johor, Malaysia. nurkhairany@uitm.edu.my

<sup>6</sup> Information Science Studies, College of Computing, Informatics and Mathematics, Universiti Teknologi MARA Cawangan Selangor, Kampus Puncak Perdana, Selangor, Malaysia. shamsulshoid@uitm.edu.my

\* Corresponding Author Email: sitin509@uitm.edu.my

to acknowledge the significance of DF in their operational setting and integrate this technology. Timely and effective digital forensic investigations are crucial for promptly addressing incidents and delivering forensic findings without unnecessary delays. The structure of this paper is organized as follows: The following section will address the statement of the problem. The literature review section provides an indepth understanding of the current research field. The fourth section provides an overview of the study's methodology. The fifth section of the paper presents the findings and conclusions of the study. The study's conclusion is presented at the end of the paper.

## II. STATEMENT OF PROBLEM

As shown in Figure (a) that the rise in cyber incidents has had a substantial effect on organizations, resulting in the loss of valuable and sensitive data, damage to the organization's reputation, and financial losses [3], [12], [14], [30], [32]. In order to tackle these difficulties, DF has been acknowledged as a valuable resource for organizations to effectively address, manage, and resolve incidents that are connected to these challenges [1], [5], [17], [20], [33]. Nevertheless, a major obstacle exists in the insufficient grasp, preparedness, and consciousness required to steer DSPC towards the utilization of DF [33]. In the Malaysian context, the issue of DF has been thoroughly examined, particularly in relation to understanding the factors that influence the decision of the DSPC to implement DF [33]. According to [8] research examined the adoption and implementation of DF (data fusion) specifically within an American Police Agency, with a particular emphasis on environmental and organizational factors. When examining the adoption of innovation within organizations, it is crucial to consider the comprehensive aspects of technological, organizational, and environmental factors [37]. By considering these factors, one can gain a more thorough comprehension of the attributes of innovation, particularly in developing nations [9], [28]. Hence, when considering developing countries, it is crucial to investigate the factors that consider the distinct characteristics of DF, as this can greatly contribute to the promotion of its utilization by DSPC. This study aims to align with the recommendations made by [24], which advocate for expanding research in the field of DF to encompass various perspectives and promote the ongoing development of this discipline.

As shown in Figure (a), the rise in cyber incidents has had a significant impact on organizations, resulting in the loss of valuable and sensitive data, damage to the organization's reputation, and financial losses [3], [12], [14], [30], [32]. To address these challenges, DF has been recognized as a valuable resource for organizations to effectively address, manage, and resolve incidents related to these issues [1], [5], [17], [20], [33]. However, a major obstacle exists in the insufficient understanding, preparedness, and awareness required to guide DSPC towards the utilization of DF [33]. In the Malaysian context, the issue of DF has been thoroughly examined, particularly in relation to understanding the factors that influence the decision of the DSPC to implement DF [33]. According to [8] research examined the adoption and implementation of DF (data fusion) specifically within an American police agency, with a particular emphasis on environmental and organizational factors. When examining the adoption of innovation within organizations, it is crucial to consider the comprehensive aspects of technological, organizational, and environmental [37]. By considering these factors, one can gain a more thorough understanding of the attributes of innovation, particularly in developing nations [9], [28]. Therefore, when considering developing countries, it is essential to investigate the factors that consider the unique characteristics of DF, as this can greatly contribute to the promotion of its utilization by DSPC. This study aims to align with the recommendations made by [24], which advocate for expanding research in the field of DF to encompass various perspectives and promote the ongoing development of this discipline.

The implementation of digital forensics in a company is crucial for effectively addressing the intricate challenges posed by cyber threats. By utilizing digital forensics, companies dealing with such issues can expedite and optimize the resolution process, thereby indirectly mitigating losses and safeguarding the company's reputation. However, the limited knowledge and proficiency in this field have led to the underutilization of digital forensics in numerous small organizations [33].

[31] study conducted a comprehensive analysis of organizational incident management policies, models, and frameworks for computer forensics investigations. The study emphasized the significance of these policies and provided recommendations on effectively integrating computer forensics into incident management. [33] found that the utilization of digital forensics in DSPCs in Malaysia remains limited. This is due to a lack of

awareness, knowledge, and expertise in this field, and the costs associated with implementation can pose a significant barrier.

Large companies recognize the importance of implementing digital forensics in security risk management. Nevertheless, smaller DSPC companies frequently fail to recognize the importance of preserving data and evidence for potential future digital investigations [31].

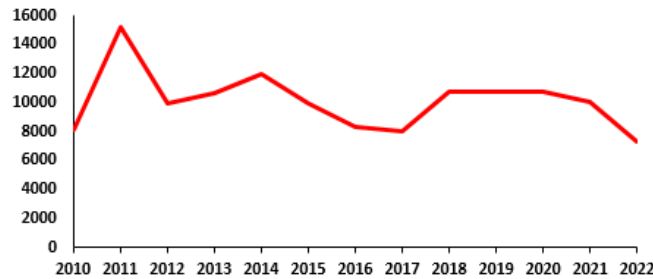


Fig. (a). Summary of Reported Cyber Incidents from 2010 to 2022 (MyCERT, 2024)

Businesses that have incorporated forensic capabilities into their operations gain the advantage of being able to gather, retain, analyze, and assess data or evidence to determine the condition of their systems and ascertain if personal and sensitive data has been compromised. Digital forensics techniques and methodologies can be utilized not only for forensic investigations but also for analyzing operational and security incidents and recovering previously implemented systems [27].

However, there is a lack of discussion in Malaysia regarding issues related to the practice of digital forensics. Most studies have focused on assessing Malaysia's preparedness for digital forensic practice, specifically examining the readiness of the country, companies, and institutions. The scarcity of a comprehensive framework has resulted in a lack of guidance for decision-makers in organizations, particularly DSPC in Malaysia, when exploring, assessing, and evaluating the factors that impact the adoption of digital forensics innovation in their operational environment.

The research model proposed in this study aims to aid decision-making regarding the adoption of digital forensics and help anticipate potential influences that can enhance the process of innovation adoption. Therefore, this study has the potential to lay the groundwork for implementing digital forensics practices within relevant organizations in Malaysia. By providing guidance on the adoption of digital forensic practices, this study aims to enhance our understanding of the successful adoption of digital forensics. This, in turn, may encourage more agencies, including modern organizations from various sectors, particularly the DSPC, to adopt digital forensics as part of their work practices.

A problem was encountered in the DSPC. The extensive dependence of society on information technology has not only driven notable technological progress but has also led to more intricate types of digital incidents in organizational contexts. Specifically, Malaysia has experienced a significant increase in cyber-criminal activity. The Malaysian Threat Landscape Report for 2018, published by Cyber Security Malaysia, revealed that 10,699 incidents were reported to the Malaysian Computer Emergency Response Team (MyCERT) in 2018. This represents a notable 34% surge compared to the previous year. The diagram in Figure (a) presents a summary of cyber incidents reported between 2010 and 2022, while Table I provides a summary of reported incidents based on general incident classification statistics from 2010 to 2022.

Table I: Summary of reported incidents based on general incident classification statistics from 2010-2022

Cyber General Incident	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	Total Incident
Content Related	39	59	20	54	35	33	50	46	1805	298	170	91	50	2750
Malicious Codes	1199	1012	645	1751	716	567	435	814	342	738	593	648	1023	10483
Denial of Service	66	78	23	19	29	38	66	40	356	19	16	22	17	789

<b>Intrusion</b>	2160	3699	4326	2770	1125	1714	2476	2011	111	1359	1444	1410	755	25360
<b>Intrusion Attempt</b>	685	734	67	76	1302	303	277	266	1700	104	116	159	180	5969
<b>Spam</b>	1268	3751	526	950	3650	3539	545	344	92	129	145	102	478	15519
<b>Fraud</b>	2212	5328	3991	4485	4477	3257	3921	3821	1160	7774	7593	7098	4741	59858
<b>Vulnerabilities Report</b>	42	98	78	19	34	22	35	60	5123	91	117	69	48	5836
<b>Cyber Harassment</b>	419	459	300	512	550	442	529	560	10	260	596	417	-	5054
<b>Total Incident</b>	8090	15218	9976	10636	11918	9915	8334	7962	10699	10772	10790	10016	7292	

### III. LITERATURE REVIEW

#### 3.1 Desktop Support Project Company

Desktop Support Project Companies, also referred to as IT companies, manage the transmission, storage, and retrieval of information. They utilize a variety of concrete tools, systems, and procedures, including computers, storage devices, networks, and other technology, to store and manage information. In short, IT companies monitor the transmission, storage, and retrieval of data across various media.

IT companies play a crucial role in the current business landscape by helping organizations leverage technology to improve productivity, efficiency, and overall performance. They may offer services such as software development, system integration, cloud computing solutions, IT infrastructure management, and cybersecurity services. Leading IT companies such as Google, Apple, IBM, and Microsoft are widely recognized for their contributions to the industry. To remain competitive in the rapidly evolving IT industry, companies often adapt to emerging technologies and market trends. They offer a wide range of services and products to meet the diverse needs of their clients, continuously innovating to stay ahead in the fast-growing IT market.

The DSPC industry in Malaysia is growing rapidly, with a wide variety of companies offering specialized services and solutions. Software development companies lead the way, specializing in creating custom software solutions to meet various individual and business needs. Leading multinational IT giants such as TCS, Infosys, Accenture, IBM, and Microsoft have established a significant presence in Malaysia. These businesses provide a diverse range of IT products and services by leveraging their vast resources and expertise, driving technological progress and stimulating the nation's economy. Overall, the amalgamation of these various fields underscores Malaysia's position as a growing hub for IT innovation and advancement.

#### 3.2 Digital Forensic in Malaysia

DF has been defined by multiple experts, each offering a nuanced viewpoint on its extent and objectives. [25] laid the groundwork by defining DF as the application of scientific and engineering principles to address legal issues related to digital evidence—a combination of scientific knowledge and legal principles. At its core, it requires careful examination of digital information with the ultimate goal of generating legally acceptable results. [23] provides a well-known definition of DF as the use of scientifically derived techniques to protect, collect, verify, examine and present digital evidence.

To establish a solid foundation for knowledge advancement and theory formulation, it is important to conduct a comprehensive examination of previous research [2], [15]. Therefore, we conducted an extensive review of prior DF studies to gain a thorough understanding of the current state of DF in Malaysia and to clearly outline the background and problems discussed in the research literature. There is a notable lack of research specifically focusing on DF within the context of DSPC, particularly in Malaysia. Current research primarily addresses the benefits of DF and organizations' willingness to adopt and use it. However, there is a scarcity of studies presenting models or frameworks specifically designed to investigate the factors that impact the use of DF in organizations

## IV. METHODOLOGY

This paper investigates the use of the current body of literature on relative advantage, complexity, compatibility, top management support, infrastructure, culture, agency competition, and perceived technical competence. The goal is to create a conceptual framework that identifies the motivational factors affecting organizations' decision-making processes when adopting DF into their operations. This study uses a variety of scholarly sources, including journal articles, conference papers, dissertations, and cited websites, to enhance understanding of innovative work behaviors. In addition, the literature search utilizes online databases such as Google Scholar, Emerald, Web of Science, and IEEE. Table II presents the findings of the literature review and integrates them to create a conceptual framework examining the factors that drive organizations to adopt DF.

**Table II:** Summary of variables from the literature review of studies on technology adoption

Author(s)	Type of Variables/ Variables	Technologies Studied
Ching, Teoh, Amran (2020)	Relative Advantage	InsurTech Adoption
Kotni, et al. (2023)	Complexity	Adoption of ChatGPT in Higher Education
Kotni, et al. (2023)	Compatibility	Adoption of ChatGPT in Higher Education
Ali et al.(2022)	Top Management Support	Information technology (IT) innovation adoption
Hossein et al. (2017)	Infrastructure	HIS
Ali et al.(2022)	Culture	Information technology (IT) innovation adoption
Abied, Ibrahim (2021)	Agency Championship	Cloud Service Adoption
Abied, Ibrahim (2021)	Perceived Technical Competence	Cloud Service Adoption

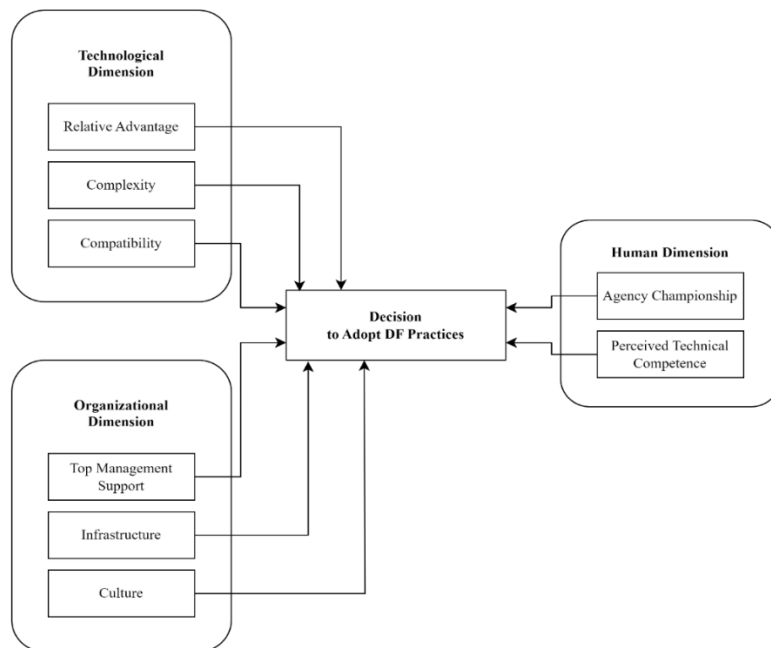
## V. RESULT AND DISCUSSION

A preliminary framework was developed through a comprehensive analysis of previous research on organizational innovation adoption and adoption of DF. The review's conclusion aligns with the HOT-fit model and the TOE framework, which consider technological, organizational, and fundamental human dimensions. Unlike other IS theories, this comprehensive framework allows for the use of multiple measures for each dimension, tailored to the specific requirements and circumstances of the innovation [37]. Therefore, in accordance with contextual requirements and utilizing research technology, this study aims to predict and elucidate the factors influencing the TOE dimensions. Past researchers have identified technological, organizational, environmental, and human contextual factors as primary challenges in the adoption of DF among DSPCs.

A theory for the adoption of DF must consider technological and organizational factors that influence a company's readiness to explore and adopt new ideas within its unique context. Therefore, the TOE framework is logical, providing a robust theoretical structure for examining contextual and dimensional factors [35]. However, in our developed model, we excluded the environmental aspect as it did not significantly contribute to this study. Characteristics associated with this dimension include vendor support, normative pressure, and coercive pressure, which do not impact DF adoption among DSPCs. DSPCs, as vendors themselves, require less external support compared to other entities. Similarly, coercive and normative pressures do not influence DF adoption in DSPCs. This is illustrated in Figure (b).

In addition, [16] utilized the TOE framework and the Hot-Fit model in his study on the implementation of DF in the Malaysian Law Enforcement Agency (MLEA), as these variables are closely related to the framework. Tornatzky and Fleischer developed the TOE framework in 1990, which examines the organizational, technological, and environmental factors influencing technology adoption in businesses. However [52] introduced the Hot-Fit model, emphasizing the importance of aligning technology with organizational factors for successful implementation. By integrating these frameworks, this study aims to achieve a comprehensive

understanding of the challenges involved in effectively integrating new technologies, organizations, and individuals in the context of DF deployment in DSPCs. Figure (b) illustrates the variables influencing the decision to adopt DF, focusing on the technological, organizational, and human dimensions. This new model is the result of the study's findings.



**Fig. (b).** Initial integrated framework of DF practices adoption for DSPC

## VI. HYPOTHESIS

### 6.1 *Relative Advantage*

Based on [29], relative advantage is defined as the extent to which an innovation offers superior benefits and opportunities compared to its predecessor. In this study, "relative advantage" refers to how agency decision-makers perceive the usefulness of DF. [49] found in their study that relative advantage is a compelling factor motivating companies to adopt new information technology. Similarly, [18] provided evidence of the significance of relative advantage, showing significant test results related to technology adoption factors. This study encompasses various benefits associated with DF adoption, including cost savings, faster response times, improved performance in forensic tasks, reduced operational disruptions, and other related advantages. [33] anticipate agencies adopting DF technology due to its superior advantages over traditional investigative and scientific problem-solving approaches.

Therefore, considering the importance of relative advantage in evaluating the adoption of DF by DSPCs in Malaysia, we propose the following hypothesis: The use of digital forensics by DSPCs in Malaysia is positively impacted by relative advantage

### 6.2 *Complexity*

[7] found that complexity hinders the acceptance and implementation of innovation. [51] defines complexity as the perceived level of difficulty associated with the use of innovation. Organizations often perceive DF, even in its early stages, as a complex innovation that requires adoption, understanding, and implementation due to the challenges it poses. [11] have identified several challenges contributing to DF's complexity, such as the lack of standardized protocols for implementation, the necessity for new and updated procedures, and the lack of uniformity among forensic tools. Addressing technical compatibility issues often requires the use of advanced and expensive digital forensic tools, necessitating expertise for effective application of DF.

A significant constraint in DF complexity arises from the dynamic nature of digital technology, which exacerbates the aforementioned difficulties. Therefore, recognizing this issue as a significant additional factor

influencing DF adoption, we propose the following hypothesis: The use of digital forensics by DSPCs in Malaysia is negatively impacted by complexity.

### 6.3 *Compatibility*

Prior research has consistently demonstrated that compatibility plays a positive role in the acceptance of innovation, as shown by [37] and supported by multiple studies on innovation adoption [48]. Compatibility is perceived to have a positive impact on the implementation of digital forensics (DF). In this study, [29] defines compatibility as the degree to which a technology aligns with the goals, values, current practices, and infrastructure of the agency.

In this context, "infrastructure" refers to the organizational systems and networks, including laboratory setups that support digital forensic operations and [6]. Therefore, the following hypothesis is proposed: The use of digital forensics by DSPCs in Malaysia is positively impacted by compatibility).

### 6.4 *Top Management Support*

Based on the majority of the reviewed literature, top management buy-in is identified as a significant factor influencing the adoption of new technologies, particularly in the context of innovation adoption [7], [9], [19], [22], [48]. Top management support plays a crucial role in promoting the adoption of DF within an organization. Beyond providing strategy, vision, resources, and commitment, top management can create an environment conducive to implementing DF initiatives [4].

In this study, top management support refers to the level at which a group of individuals engaged in strategic decision-making recognizes the importance of adopting innovative technologies, which significantly influences the adoption of DF in agencies. Therefore, the following hypothesis is proposed: Top management support has a positive effect on the DSPCs' in Malaysia adoption of digital forensics

### 6.5 *Infrastructure*

Infrastructure, as defined by [21], refers to the collection of tools and physical resources that an organization uses to facilitate its operations. The infrastructure of an organization plays a crucial role in fostering innovation adoption, as indicated by previous research on technology acceptance [10], [18], [37], [48]. According to [44], to conduct digital forensic operations effectively, it is essential to have the requisite organizational infrastructure. In this study, "infrastructure" specifically pertains to the physical framework of forensic science, comprising a network of meticulously designed laboratories and well-equipped facilities that include hardware, software, and other tools. These resources enable agencies to perform both investigative and non-investigative digital forensics activities.

Therefore, to justify an agency's decision to implement DF, it is crucial to have adequate and appropriate forensic technology infrastructure [6], [14]. Consequently, the following hypothesis is proposed: Infrastructure has a positive effect on the use of DF towards DSPC in Malaysia.

### 6.6 *Culture*

In this study, culture is defined as a set of shared values, beliefs, assumptions, and practices that influence the motivation of organizational members towards DF and, consequently, the readiness of the agency to embrace innovation. Due to its recent emergence and limited exposure in society, there is a scarcity of literature on the relationship between culture and DF [4]. [6] argue that culture directly impacts the implementation of DF.

To effectively prioritize DF, organizations must foster a forensic culture, often necessitating a cultural shift. Establishing and managing forensic programs helps enhance member understanding and adapt existing values, beliefs, conventions, assumptions, and practices to incorporate new technologies, as education significantly influences culture. [18] have identified culture as a key determinant of technology adoption, supported by empirical data. Thus, the following hypothesis is proposed: Culture has a positive effect on the use of DF towards DSPC in Malaysia.

### 6.7 *Agency Championship*

The concept of agency championship refers to the presence of agency members who actively lead DF adoption initiatives and inspire others within the organization to positively embrace DF. This study views agency championship as a motivating attribute of employees that facilitates innovation adoption. According to [43], internal employees who comprehend innovation and its benefits play a critical role in an agency's adoption of innovations. In IT organizations, User and Technical champions, as described by [45], fulfill specific roles: Technical champions focus on operational aspects to ensure the effectiveness of innovation, while User champions motivate and guide users to adopt innovation through promotion and guidance. A champion is an organizational member with strong peer-persuasion skills.

This study particularly focuses on employees within direct dissemination organizations. Therefore, the following hypothesis is proposed: Agency Championship has a positive effect on the DSPCs' adoption of digital forensics.

#### 6.8 *Perceived Technical Competence*

Technical competence is a crucial factor in the adoption of innovation, as highlighted by numerous previous studies [22]. [47] emphasize that technical competence signifies the proficiency of an agency's technical staff, encompassing their skills and knowledge of cutting-edge technology [50]. To expedite innovation adoption, [46] argue that agencies must systematically develop their employees' technological skills and knowledge. Before deciding on innovation adoption, agencies should assess the technical competence of their organizational members to ensure they can effectively utilize new technologies.

In the context of this investigation, technical competence refers specifically to staff members' expertise and knowledge in DF, enabling them to perform forensic duties and achieve forensic objectives. Therefore, possessing technical proficiency and meeting all requirements are crucial for an organization to successfully implement DF. Therefore, the following hypothesis is proposed: Perception of Technical Competence has a positive effect on the use of digital forensics on DSPC in Malaysia.

### VII. CONCLUSION AND RECOMMENDATION

This paper aims to investigate the determinants influencing an organization's decision to implement DF. These determinants include relative advantage, motivation, complexity, compatibility, top management support, infrastructure, culture, agency championship, and perceived technical competence. Understanding these factors is crucial for DSPCs as they help identify key considerations for adopting DF within their organizations.

Moreover, this study will benefit future scholars by providing insights into the factors influencing DSPCs' decisions to implement DF. The framework proposed in this paper synthesizes findings from prior research to guide future investigations into DF adoption factors specifically tailored for DSPCs.

Further research is recommended to empirically examine these proposed factors and their impact on DF adoption in DSPCs, thereby contributing to a deeper understanding of how organizations can effectively integrate DF into their operational strategies.

### VIII. ACKNOWLEDGEMENTS

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

### REFERENCES

- [1] P. G. Altbach, AswamiAriffin, Jill, S., and HusinJazri. (2012). Digital forensics institute in Malaysia: the way forward. *Digital Evidence and Electronic Signature Law Review*, 9(8), 51–57.
- [2] Bhattacharjee, A. (2012). *Social Science Research: principles, methods, and practices*. (2nd). Florida: Creative Commons Attribution.
- [3] ElfadilSabeil Mohamed Ali. (2013). *Digital forensics professional competency-based curriculum procedures*. (Doctoral thesis), Universiti Teknologi Malaysia, Malaysia.
- [4] Elyas, M., Maynard, S. B., Ahmad, A., and Lonie, A. (2014). Towards a systematic framework for digital forensic readiness. *Journal of Computer Information System*, 54, 70-89.
- [5] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years digital forensics research: The next 10 years. *Digital Investigation*, 7, 64–73.



- [6] Grobler, C. P., Louwrens, C. P., and Von Solms, S. H. (2010). A framework to guide the implementation of proactive digital forensics in organizations. In *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*. 677–682.
- [7] Grover, V. (1993). An empirically derived model for the adoption of customer-based inter organizational systems. *Decision Sciences*, 24(3), 603–640.
- [8] Hamdi, Y. (2011). *The Response of American Police Agencies to Digital Evidence*. (Doctoral thesis), University of Central Florida, USA.
- [9] Hemlata, G., Hema, D., and Raoot A. D. (2014). Review on IT adoption: insights from recent technologies. *Journal of Enterprise Information Management*. 27(4), 488–502.
- [10] K. Zhu, K.L. Kraemer, V. Gurbaxani, S.X. Xu, Migration to open-standard inter organizational systems: Network effects, switching costs, and path dependency, *MIS Quarterly: Management Information Systems*, 2006, doi: 10.2307/25148771.
- [11] Karie, N. M., and Venter, H. S. (2015). Taxonomy of challenges for digital forensics. *Journal of Forensic Sciences*, 60(4), 885–893.
- [12] Khuram, M., Ahmer, U., Kamran, A., and Nadeem, M. (2014). Digital forensic models: A comparative study based in large enterprises of Pakistan. *Research Journal of Recent Sciences*, 3(8), 103–110.
- [13] M.M. Yusof, J. Kuljis, A. Papazafeiropoulou, L.K. Stergioulas, An Evaluation Framework for Health Information Systems: Human, Organization and Technology-Fit Factors (HOT-Fit ), *International Journal of Medical Informatics* 77(6) (2007) 386–398. DOI: <https://doi.org/10.1016/j.ijmedinf.2007.08.011>
- [14] Mankantshu, M. A. (2013). *Investigating the Factors that Influence digital Forensic Readiness in a South African Organization*. Master of Commerce in Information Systems, University of Cape Town.
- [15] Marian C., Eileen D., and Gerard C. (2018). An analysis of systematic literature review (SLR) approach in the field of IS management. *Proceeding of the 17th European Conference on Research Methodology for Business and Management Studies*. 12-13 July 2018. Rome, Italy, 78-85.
- [16] Mat Kamal, S.N.I. (2019). *Digital Forensics Adoption Model for Malaysian Law Enforcement Agencies* [PhD Thesis, Universiti Teknologi Malaysia]. <http://eprints.utm.my/98109/1/SitiNuurIlaPSC2019.pdf>
- [17] Mohay, G. (2005). Technical challenges and directions for digital forensics. In *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering*. 2005, 155–161.
- [18] Mumtaz, A. H., Steve, C., and Stephen, S. (2012). A conceptual model for the process of IT innovation adoption in organizations. *Journal of Engineering and Technology Management*, 29(3), 358–390.
- [19] N. Schillewaert, M.J. Ahearne, R.T. Frambach, R.K. Moenaert, “The adoption of information technology in the sales force,” *Industrial Marketing Management*, 34(2), 323–336, 2005, doi:10.1016/j.indmarman.2004.09.013.
- [20] Nordiana, R., Wahid, A. W. A., Idna, I. M. Y., and Laiha, M. kiah M. (2014). Digital forensics: An overview of the current trends. *International Journal of Cryptology Research*, 4(2), 2–13
- [21] Oliveira T & Martins Mf. 2010. Information technology adoption models at firm level: review of literature. *European Conference on Information Management and Evaluation* pp. 312.
- [22] Oliveira, T., Faria, M., Thomas, M.A. &Popovič, A. (2014). Extending the understanding of mobile banking adoption: When UTAUT meets TTF and ITM. *International Journal of Information Management*, 34 (5), 689-703.
- [23] Palmer, G. (2001). *A Road Map for Digital Forensic Research*. Utica, NewYork.
- [24] Pangalos, G., and Katos, V. (2010). Information assurance and forensic readiness. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, 26, 181–188.
- [25] Pollitt, M. M. (2007). An ad hoc review of digital forensic models. In *Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering*. IEEE. 43-54.
- [26] Pollitt, M. M. (2007). An ad hoc review of digital forensic models. In *Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering*. IEEE. 43-54.
- [27] Radack, S., 2009. *Forensic Techniques: Helping Organizations Improve their Responses to Information Security Incidents* (NIST Publications).
- [28] Riyadh, A. N., Akter, Md. S. and 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.
- [29] Rogers, E. M. (1995). *Diffusion of Innovations*, (4th). New York: The Free Press.
- [30] Sarah K.Taylor, Miratun M. Saharuddin and Zabri A. Talib (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.
- [31] 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](https://doi.org/10.1016/s1361-3723(02)00610-3)
- [32] Sommer, P. (2009). *Directors and Corporate Advisors' Guide to Digital Investigations and Evidence* (2nd). UK: Information Assurance Advisory Council.

- [33] Suhaila, I., Arniyati, A., and MohdAfizi, M. S. (2011). New method of forensic computing in a small organization. *Australian Journal of Basic and Applied Sciences*, 5(9), 2019–2025.
- [34] Taylor, C., Endicott-Popovsky, B., and Frincke, D. A. (2007). Specifying digital forensics: A forensics policy approach. *Digital Investigation*, 4, 101–104.
- [35] Tornatzky, L. and Fleischer, M. (1990). *The process of technology innovation*. Lexington: Lexington Books.
- [36] Willassen, S. Y. and S. F. Mjølunes (2005). Digital forensics research. *Teletronik*, 1, 92-97.
- [37] Yang, Z., Sun, J., Zhang, Y., and Wang, Y. (2015). Understanding SaaS adoption from the perspective of organizational users: A tripod readiness model. *Computers in Human Behavior*, 45, 254–264.
- [38] Yaser Hasan Salem Al-Mamary, Alina Shamsuddin, NorAziati A. H. (2015). Investigating the key factors influencing on management information systems abiedoption among telecommunication companies in Yemen: The conceptual framework development. *International Journal of Energy, and Communications*, 6(1), 59–68.
- [39] Abied, O., & Ibrahim, O. (2021). Cloud service adoption model in the Libyan e-government implementation. 2021 International Congress of Advanced Technology and Engineering (ICOTEN). <https://doi.org/10.1109/icoten52080.2021.9493534>
- [40] Ali, O., Murray, P. A., Muhammed, S., Dwivedi, Y. K., & Rashiti, S. (2022). Evaluating Organizational Level IT Innovation Adoption Factors among Global Firms. *Journal of Innovation & Knowledge/Journal of Innovation and Knowledge*, 7(3), 100213. <https://doi.org/10.1016/j.jik.2022.100213>
- [41] K. H. Ching, A. P. Teoh and A. Amran, "A Conceptual Model of Technology Factors to InsurTech Adoption by Value Chain Activities," 2020 IEEE Conference on e-Learning, e-Management and e-Services (IC3e), Kota Kinabalu, Malaysia, 2020, pp. 88-92, doi: 10.1109/IC3e50159.2020.9288465.
- [42] Kotni, V. D. P., Ungarala, D. P., Peri, P. P., Nitcharla, S., Nagaraj, K., & Mustafa, M. (2023). Adoption of ChatGPT in Higher Education-Application of IDT Model, Testing and Validation. *Researchgate*. <https://doi.org/10.1109/ictacs59847.2023.10390323>
- [43] Asli Yagmur Akbulut. (2003). *An Investigation of the Factors That Influence Electronic Information Sharing between State and Local Agencies*. Doctoral thesis), Louisiana State University. United State.
- [44] Carrier, B. D., and Spafford, E. H. (2004). An event-based digital forensic investigation framework. In *Proceedings of the Fourth Digital Forensics Research Workshop*. 1–12.
- [45] Garfield, M. (2000). Critical success factors for state telemedicine policy. In *Proceeding of Americas Conference on Information Systems* (pp.1573-1578). Long Beach.
- [46] Ghobakhloo, M., Arias-aranda, D., and Benitezamado, J. (2011). Adoption of e-commerce applications in SMEs. *Industrial Management & Data Systems*, 111(8), 1238–1269.
- [47] Jiunn, woei L., David, C. Y., and 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.
- [48] 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.
- [49] Premkumar, G., and Roberts, M. (1999). Adoption of new information technologies in rural small businesses. *The International Journal of Management Science*, 27, 467–484.
- [50] Rahayu, R., and 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.
- [51] Thong, J. Y. L. L. (1999). An integrated model of information systems adoption in small businesses. *Journal of Management Information Systems*, 15(4), 187–214.
- [52] Yusof, M. M., Kuljis, J., Papazafeiropoulou, A., and Stergioulas, L. K. (2008a). An evaluation framework for Health Information Systems: human, organization and technology-fit factors (HOT-fit). *International Journal of Medical Informatics*, 77(6), 386–398.
- [53] Hossein Ahmadi, Mehrbakhsh Nilashi, Leila Shahmoradi, and Othman Ibrahim. (2017). Hospital information system adoption: Expert perspectives on an adoption framework for Malaysian Public Hospital. *Computers in Human Behavior*, 67, 161-189.
- [54] MyCERTHomepage, <https://www.cybersecurity.my/en/index.html>, last accessed 2024/6/11.