MODEL INTEGRASI KESEDIAAN FORENSIK DIGITAL DAN PSIKOLOGI UNTUK KESELAMATAN SIBER

NORULZAHRAH BINTI MOHD ZAINUDIN

DOCTOR OF PHILOSOPHY
(COMPUTER SCIENCE)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

2024

MODEL INTEGRASI KESEDIAAN FORENSIK DIGITAL DAN PSIKOLOGI UNTUK KESELAMATAN SIBER

NORULZAHRAH BINTI MOHD ZAINUDIN

Thesis submitted to the Centre for Graduate Studies, Universiti Pertahanan Nasional Malaysia, in fulfilment of the requirements for the Degree of Doctor of Philosophy (Computer Science)

2024

Thesis submitted to the Centre for Graduate Studies, Universiti Pertahanan Nasional Malaysia, in fulfilment of the requirements for the Degree of Doctor of Philosophy (Computer Science)

ABSTRAK

Ancaman penipuan dalam talian dan insiden pelanggaran keselamatan yang semakin meningkat menimbulkan cabaran besar kepada agensi penguatkuasaan dan individu yang terlibat dengan forensik digital di seluruh dunia. Kesediaan forensik digital (KFD) membolehkan individu bersiap sedia untuk melaksanakan penyiasatan dengan lebih cekap. Meskipun pelbagai faktor telah dikaji berkaitan model KFD, antaranya faktor perundangan, kakitangan, sokongan pengurusan dan dasar, namun setakat kajian ini dilakukan, faktor kesediaan psikologi yang merupakan faktor penting bagi individu untuk bersedia melaksanakan forensik digital kurang diberi perhatian. Berdasarkan kajian literatur, terdapat jurang dalam penyelidikan mengenai faktor-faktor yang mempengaruhi KFD. Antaranya termasuk kekurangan kajian yang khusus kepada KFD di negara ini, serta kurangnya integrasi faktor psikologi. Selain itu, belum ada kajian yang melibatkan kumpulan besar profesional forensik digital dan kajian kuantitatif mengenai KFD, menunjukkan keperluan untuk model penyelidikan yang

lebih mendalam dan sistematik. Justeru, objektif utama kajian ini adalah untuk membangunkan model baharu KFD melalui integrasi faktor kesediaan psikologi iaitu konstruk daripada Indeks Kesediaan Teknologi (TRI 2.0) dan konstruk sedia ada dalam model KFD. Kajian ini berasaskan pendekatan kuantitatif yang menggunakan tinjauan melalui soal selidik tadbiran sendiri. Sejumlah 160 data berjaya dikumpul daripada pelbagai agensi keselamatan siber awam dan swasta di sekitar Lembah Klang (Januari hingga Oktober 2022). Kajian ini melakukan analisis deskriptif terhadap data demografi, manakala analisis *Partial Least Squares Structural Equation Modelling* (PLS-SEM) terhadap model baharu KFD. PLS-SEM juga digunakan untuk analisis pengantaraan bagi konstruk mediator dan moderator untuk menentukan konstruk siginifikan dalam kajian ini. Hasil analisis menunjukkan empat daripada sepuluh konstruk menghasilkan hubungan yang signifikan. Secara keseluruhannya, dapatan akhir kajian ini boleh membantu agensi keselamatan siber, organisasi dan penggubal dasar mengenali konstruk utama yang perlu dipertimbangkan semasa proses penyediaan forensik digital supaya pelaksanaan penyiasatan forensik digital dapat dilaksanakan dengan lebih berkesan pada masa hadapan.

Kata kunci: kesediaan forensik digital, keselamatan siber, penyiasatan forensik, bukti digital, kesediaan

ABSTRACT

The growing threat of online fraud and incidents of security breaches poses a major challenge to law enforcement agencies and individuals involved in digital forensics around the world. Digital forensic readiness (DFR) enables individuals to prepare and perform investigations more efficiently. Although various factors have been studied in relation to the DFR model, including legal factors, personnel, management support and policy, but as far as this study is concerned, the psychological readiness factor which is an important factor for individuals to be ready in carrying out digital forensics has received little attention. Based on the literature review, there is a gap in research on the factors that influence KFD. Among them are the lack of studies specific to KFD in this country, as well as the lack of integration of psychological factors. In addition, there has not been a study involving a large group of digital forensic professionals and a quantitative study on KFD, indicating the need for a more in-depth and systematic research model. Therefore, the main objective of this study is to develop a new DFR model through the integration of psychological readiness factors which are constructs from the Technology Readiness Index (TRI 2.0) and existing constructs in the DFR model. This study is based on a quantitative approach that uses surveys through self- administered questionnaires. A total of 160 pieces of data were successfully collected from various public and private cyber security agencies around the Klang Valley (January to October 2022). Descriptive analysis was performed on demographic data, while Partial Least Squares- Structural Equation Modelling (PLS-SEM) analysis on the new model of DFR. PLS-SEM was also used for mediation and moderation analysis of mediator constructs to determine the significant constructs in

this study. The results of the analysis showed that four out of ten constructs produced a significant relationship. Overall, the final findings of this study can help cyber security agencies, organisations and policy makers to recognise the key constructs that need to be considered during the digital forensics preparation process so that the implementation of digital forensics investigations can be carried out more effectively in the future.

Key words: digital forensic readiness, cybersecurity, forensic investigation, digital evidence, preparedness

PENGHARGAAN

Bismillahirahmanirrahim,

Segala puji bagi Allah yang Maha Esa kerana telah memberikan kesihatan dan kekuatan untuk menyiapkan kajian Ph.D ini. Pertama, jutaan terima kasih diucapkan kepada pasukan penyelia saya Ts. Dr. Asiakin Hasbullah, Dr. Muslihah Wook dan Prof. Madya Ts. Dr. Suzaimah Ramli atas sokongan, cadangan dan kesabaran yang tidak terhingga di sepanjang perjalanan PhD ini. Saya juga ingin merakamkan ucapan terima kasih kepada suami Mohd Tarmizi Haji Mat Zin atas sokongan yang tidak pernah luntur, juga terima kasih atas sokongan dan pengorbanan anak-anak Arissa, Naufal, Atiyyah dan Aafiyah. Tidak lupa ibu saya, Bidah Jantan dan ahli keluarga serta rakan-rakan saya yang dikasihi terutamanya Prof. Madya Ts. Dr. Noor Afiza dan Lt. Kol Dr. Roziyah atas sokongan, motivasi dan dorongan dalam melalui setiap fasa perjalanan Ph.D saya. Juga terima kasih kepada Dr. Shima atas bantuan yang dihulurkan dalam menyelesaikan penghantaran tesis. Ucapan terima kasih juga ditujukan kepada semua panel penilai dan responden yang telah menyertai kajian ini. Terima kasih tidak terhingga saya ucapkan.

KELULUSAN

The Examination Committee has met on **16 July 2024** to conduct the final examination of **Norulzahrah binti Mohd Zainudin** on his degree thesis entitled **'Model Integrasi Kesediaan Forensik Digital dan Psikologi untuk Keselamatan Siber'.**

The committee recommends that the student be awarded the of Doctor of Philosophy (Computer Science).

Members of the Examination Committee were as follows.

Prof. Madya Dr. Mohd Fahmi bin Mohamad Amran
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Chairman)

Prof. Madya Dr. Mohd Rizal bin Mohd Isa
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Internal Examiner)

Prof. Madya Ts. Dr. Nik Zulkarnaen bin Hj Khidzir
Fakulti Teknologi Kreatif dan Warisan
Universiti Malaysia Kelantan
(External Examiner)

Ts. Dr. Siti Hajar binti Othman
Faculty of Engineering
Universiti Teknologi Malaysia
(External Examiner)

APPROVAL

This thesis was submitted to the Senate of Universiti Pertahanan Nasional Malaysia and has been accepted as fulfilment of the requirements for the degree of **Doctor of Philosophy (Computer Science)**. The members of the Supervisory Committee were as follows.

Ts. Dr. Nor Asiakin Hasbullah
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Main Supervisor)

Dr. Muslihah Wook
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Co-Supervisor)

Associate Professor Ts. Dr. Suzaimah Ramli
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Co-Supervisor)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

PENGISYTIHARAN TESIS

Student's full name : NORULZAHRAH BINTI MOHD ZAINUDIN

Date of birth : 29/11/1978

Title : Model Integrasi Kesediaan Forensik Digital dan Psikologi untuk Keselamatan Siber

Academic session : 2024/2025

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

I further declare that this thesis is classified as:

☐ **CONFIDENTIAL** (Contains confidential information under the official Secret Act 1972)*

☐ **RESTRICTED** (Contains restricted information as specified by the organisation where research was done)*

☐ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

I acknowledge that Universiti Pertahanan Nasional Malaysia reserves the right as follows.

1. The thesis is the property of Universiti Pertahanan Nasional Malaysia.
2. The library of Universiti Pertahanan Nasional Malaysia has the right to make copies for the purpose of research only.
3. The library has the right to make copies of the thesis for academic exchange.

Signature	**Signature of Supervisor/Dean of CGS
Click here to enter text.	Click here to enter text.
IC/Passport No.	**Name of Supervisor/Dean of CGS
Date:	Date:

*If the thesis is CONFIDENTAL OR RESTRICTED, please attach the letter from the organisation with period and reasons for confidentiality and restriction.

** Witness

ISI KANDUNGAN

TAJUK	HALAMAN
ABSTRAK	**ii**
ABSTRACT	**iv**
PENGHARGAAN	**vi**
KELULUSAN	**vii**
APPROVAL	**viii**
PENGISYTIHARAN TESIS	**ix**
ISI KANDUNGAN	**x**
SENARAI JADUAL	**xiii**
SENARAI RAJAH	**xv**
SENARAI SINGKATAN	**xvii**
SENARAI SIMBOL	**xviii**
SENARAI LAMPIRAN	**xix**
BAB 1 PENGENALAN	**1**
1.1 Pendahuluan	1
1.2 Latarbelakang Kajian	2
1.3 Pernyataan Masalah	4
1.4 Persoalan Kajian	7
1.5 Objektif Kajian	8
1.6 Skop Kajian	9
1.7 Kepentingan Kajian	9
1.8 Organisasi Tesis	10
1.9 Kesimpulan	11
BAB 2 KAJIAN LITERATUR	**12**
2.1 Pengenalan	12
2.2 Definisi konsep	12
2.2.1 Forensik Digital	13
2.2.2 Model Penyiasatan Forensik Digital	15
2.2.3 Kesediaan Forensik Digital (KFD)	27
2.3 Isu berkaitan Kesediaan Forensik Digital	31
2.4 Model Kesediaan Forensik Digital Terdahulu	33
2.5 Faktor-faktor yang Mempengaruhi Kesediaan Forensik Digital (KFD)	40
2.5.1 Strategi Kesediaan	41
2.5.2 Pihak Berkepentingan Teknikal	42
2.5.3 Pihak Berkepentingan Bukan Teknikal	43
2.5.4 Teknologi Forensik	44
2.5.5 Seni Bina Sistem	44
2.5.6 Polisi Forensik	45
2.5.7 Latihan	46
2.5.8 Budaya	47

2.5.9 Sokongan Pengurusan 48
2.5.10 Tadbir Urus 48
2.5.11 Prosedur 49
2.5.12 Perundangan dan Peraturan 50
2.5.13 Kakitangan 51
2.5.14 Pengalaman 52
2.6 Faktor Psikologi dalam Kesediaan Forensik Digital 53
2.7 Teori berkaitan Kesediaan dan Kaitannya dengan Forensik Digital dalam Keselamatan Siber 54
2.8 Jurang dan Analisis Model Kesediaan Forensik Digital Terdahulu 59
2.9 Kesimpulan 63

BAB 3 METODOLOGI KAJIAN 64
3.1 Pengenalan 64
3.2 Falsafah Penyelidikan 64
3.3 Metodologi Kajian (Kuantitatif) 66
3.4 Reka bentuk Kajian 67
3.4.1 Fasa 1: Pernyataan Masalah dan Rekabentuk Kajian 68
3.4.2 Fasa 2: Mengenal pasti Teori Asas 68
3.4.3 Fasa 3: Pembangunan Model Kajian 69
3.4.4 Fasa 4: Pembangunan Instrumen Kajian 104
3.4.5 Fasa 5: Pengumpulan Data 125
3.4.6 Fasa 6: Analisis Data dan Pengesahan Model 131
3.5 Kesimpulan 133

BAB 4 ANALISIS DAN INTERPRETASI DATA 135
4.1 Pengenalan 135
4.2 Langkah 1: Analisis Awal Data Kajian 135
4.2.1 Analisis Kadar Pulangan Data 137
4.2.2 Pembersihan Data 137
4.2.3 Pengujian Varians Kaedah Sepunya (VKS) 138
4.2.4 Pengujian Taburan Normal Data 141
4.3 Langkah 2: Analisis Deskriptif 143
4.3.1 Analisis Deskriptif Demografi Sampel 143
4.4 Langkah 3: Analisis Model Persamaan Struktural 145
4.4.1 Langkah 3.1: Analisis Model Pengukuran 146
4.4.2 Langkah 3.2: Analisis Model Struktural 154
4.5 Langkah 4: Analisis Mediator dan Moderator 161
4.5.1 Analisis Pengujian Mediator 161
4.5.2 Analisis Pengujian Moderator 162
4.6 Analisis dan Interpretasi Keputusan Pengujian Hipotesis 163
4.7 Kesimpulan 168

BAB 5 PERBINCANGAN DAN KESIMPULAN 169
5.1 Pengenalan 169
5.2 Ringkasan Kajian 169

5.3 Jawapan kepada Persoalan Kajian 172
5.3.1 Persoalan Kajian 1 (PK1) 172
5.3.2 Persoalan Kajian 2 (PK2) 173
5.3.3 Persoalan Kajian 3 (PK3) 173
5.4 Sumbangan Kajian 174
5.4.1 Sumbangan Teoritikal 174
5.4.2 Sumbangan Praktikal 176
5.5 Batasan Kajian dan Cadangan Masa Hadapan 177
RUJUKAN **179**
LAMPIRAN **198**
BIODATA PELAJAR **232**
SENARAI PENERBITAN **233**

SENARAI JADUAL

NO. JADUAL	TAJUK	HALAMAN
Jadual 1.1	Padanan persoalan dan objektif kajian	8
Jadual 2.1	Definisi-definisi Forensik Digital	14
Jadual 2.2	Model-model utama forensik digital daripada kajian lampau	16
Jadual 2.3	Istilah dan definisi Kesediaan Forensik Digital (KFD)	28
Jadual 2.4	Rumusan Model Terdahulu	34
Jadual 2.5	Klasifikasi Kesediaan Teknologi	58
Jadual 2.6	Pemetaan KFD	59
Jadual 3.1	Falsafah Penyelidikan Positivism	65
Jadual 3.2	Faktor yang mempengaruhi KFD	74
Jadual 3.3	Latar belakang Pakar	82
Jadual 3.4	Analisis pakar dalam menentusah model konseptual awal	84
Jadual 3.5	Rumusan Hipotesis Kajian	101
Jadual 3.6	Rumusan Hipotesis Kajian dan Hubungan antara Konstruk	105
Jadual 3.7	Definisi Konstruk	107
Jadual 3.8	Indikator Pengukuran Konstruk	109
Jadual 3.9	Panel Pakar bagi Kesahan Kandungan	113
Jadual 3.10	Pindaan soal selidik selepas pengesahan pakar	114
Jadual 3.11	Hasil Analisis Kajian Rintis	120
Jadual 3.12	Senarai akhir kontruk dan indikator	121
Jadual 3.13	Rumusan Hipotesis Kajian Dikemaskini	123
Jadual 3.14	Perbandingan kaedah pengumpulan data melalui teknik soal selidik	130
Jadual 3.15	Ringkasan analisis data	132

Jadual 4.1 Keputusan Pengujian bias Varians Kaedah Sepunya (VKS) 139

Jadual 4.2 Keputusan Pengujian Kepencongan dan Kurtosis 143

Jadual 4.3 Analisis Deskriptif Pemboleh Ubah Demografi 144

Jadual 4.4 Jenis Penilaian dan Had nilai bagi penilaian model pengukuran reflektif 147

Jadual 4.5 Ringkasan Keputusan Model Pengukuran 151

Jadual 4.6 Kadar Heterotrait-Monotrait (HTMT) 154

Jadual 4.7 Had nilai penilaian model struktural 155

Jadual 4.8 Penilaian Keseluruhan Model Struktural 157

Jadual 4.9 Analisis Relevan Ramalan (Q2) 161

Jadual 4.10 Pengujian Hipotesis terhadap Mediator 162

Jadual 4.11 Efek moderator ke atas pembolehubah eksogenus 163

Jadual 4.12 Keputusan pengujian hipotesis 165

SENARAI RAJAH

NO. RAJAH	TAJUK	HALAMAN
Rajah 2.1	*Technology Readiness Index* (TRI)	55
Rajah 2.2	Graf kekerapan faktor Kesediaan Forensik Digital (KFD)	60
Rajah 2.3	Jurang Kajian Berkaitan Faktor Mempengaruhi KFD	61
Rajah 3.1	Reka bentuk Kajian	67
Rajah 3.2	Proses Pembangunan Model Konseptual	70
Rajah 3.3	Faktor yang mempengaruhi KFD diadaptasi daripada TRI	73
Rajah 3.4	Faktor-faktor daripada Model / Kerangka KFD dan Kajian Lampau	80
Rajah 3.5	Cadangan Model Konseptual Awal	81
Rajah 3.6	Pengubahsuaian model berdasarkan komen dan cadangan panel pakar	86
Rajah 3.7	Model Konseptual Kajian	87
Rajah 3.8	Model konseptual kajian (Hipotesis)	102
Rajah 3.9	Proses Pembangunan Instrumen	104
Rajah 3.10	Model konseptual kajian (Hipotesis) dikemaskini	124
Rajah 3.11	Analisis Kuasa Priori Menggunakan G*Power	128
Rajah 4.1	Proses Analisis Data	136
Rajah 4.2	Perisian WebPower untuk mengira nilai kepencongan dan kurtosis	142
Rajah 4.3	Output daripada perisian pengiraan nilai kepencongan dan kurtosis	142
Rajah 4.4	Proses Analisis *Partial Least Squares- Structural Equation Modelling* (PLS-SEM)	146
Rajah 4.5	Langkah penilaian model pengukuran reflektif	147
Rajah 4.6	Keputusan algoritma PLS-SEM	150
Rajah 4.7	Proses penilaian model struktural	155

Rajah 4.8 Hasil analisis Model KFD 167

SENARAI SINGKATAN

KFD	-	Kesediaan Forensik Digital
KPDNHEP	-	Kementerian Perdagangan Dalam Negeri dan Hal Ehwal Pengguna
PLS-SEM	-	*Partial Least Squares-Structural Equation Modelling*
SEM	-	*Structural Equation Modelling*
SKMM	-	Suruhanjaya Komunikasi dan Multimedia Malaysia
TRI	-	*Technology Readiness Indeks*
UKM	-	Universiti Kebangsaan Malaysia
UPNM	-	Universiti Pertahanan Nasional Malaysia
UTM	-	Universiti Teknologi Malaysia

SENARAI SIMBOL

β - Beta

α - Alpha

λ - Lambda

SENARAI LAMPIRAN

LAMPIRAN	TAJUK	HALAMAN
Lampiran A	Borang Penilaian Model Konseptual Awal	218
Lampiran B	Borang Pengesahan Kandungan Soal Selidik Kajian	229
Lampiran C	Borang Soal Selidik	240

BAB 1

PENGENALAN

1.1 Pendahuluan

Bab ini memberikan perbincangan mendalam mengenai latar belakang kajian berkaitan kesediaan forensik digital (KFD) dalam organisasi. Pada awalnya, bab ini menerangkan isu-isu utama yang dihadapi dalam KFD, khususnya bagaimana organisasi bersedia dalam menghadapinya. Masalah yang timbul dalam KFD dikupas dengan teliti melalui kajian literatur yang telah dijalankan, memberikan gambaran menyeluruh tentang cabaran dan kekurangan yang ada dalam bidang ini.

Seterusnya, persoalan kajian dan objektif kajian dihuraikan dengan jelas. Persoalan kajian yang dikemukakan bertujuan untuk memahami lebih mendalam aspek-aspek tertentu dalam KFD, manakala objektif kajian menetapkan apa yang ingin dicapai melalui penyelidikan ini. Bab ini juga membincangkan skop kajian, yang menjelaskan batasan serta lingkungan kajian yang akan dijalankan, memastikan bahawa fokus penyelidikan adalah tepat dan relevan.

Kepentingan kajian turut diketengahkan dalam bab ini, menunjukkan nilai dan sumbangan kajian terhadap bidang forensik digital dan amalan organisasi. Akhir sekali, organisasi tesis dijelaskan, memberikan panduan tentang bagaimana kajian ini disusun. Bab ini diakhiri dengan kesimpulan yang merangkumi keseluruhan kandungan bab, memastikan pembaca memahami konteks kajian dengan jelas.

1.2 Latarbelakang Kajian

Penggunaan teknologi maklumat dan komunikasi dalam kehidupan seharian di pelbagai sektor, sama ada dalam bidang komersial, perbankan, pendidikan atau pentadbiran kerajaan, bukan sahaja telah meningkatkan produktiviti tetapi juga kecekapan pengguna. Pada masa yang sama, penjenayah juga telah mengenal pasti jenayah konvensional boleh diadaptasi dengan menggunakan teknologi dan kebolehcapaian kepada maklumat. Dalam jenayah siber sebegini, teknologi digunakan terutamanya sama ada sebagai alat untuk melakukan aktiviti jenayah atau sebagai repositori bukti yang berkaitan dengan jenayah

Forensik digital telah melalui satu evolusi yang panjang dengan bermula daripada alatan dan teknik untuk mengesan bukti digital, bukannya daripada proses saintifik sepertimana sains forensik tradisional lain (Reith, Carr, & Gunsch, 2002). Perkara ini menjadi salah satu cabaran utama dalam forensik digital untuk memastikan bukti elektronik ditemui boleh diterima dan menggunakan kaedah saintifik. Tanpa kaedah saintifik, bukti tersebut boleh dipersoalkan oleh pelbagai pihak seperti hakim, peguambela, juga oleh pihak tertuduh, antaranya (Carrier & Spafford, 2003b).

Dalam usaha meningkatkan kepercayaan bukti digital yang melibatkan penguatkuasaan jenayah siber, pelbagai model dan kerangka proses-proses utama forensik digital telah dibangunkan. Pembangunan model dan kerangka proses forensik digital pada permulaan evolusi telah dipelopori oleh sekurang-kurang tiga model perintis iaitu *The Abstract Digital Forensic Model* (Reith, Carr, & Gunsch, 2002), *The Integrated Digital Investigation Model* (Carrier & Spafford, 2003b) dan *The Enhanced Integrated Digital Investigation Model* (Baryamureeba & Florence, 2004). Sehingga kini pelbagai model dan kerangka forensik digital telah dibangunkan mengikut kemajuan teknologi dan perkembangan aktiviti jenayah (Agarwal et al., 2011; Beebe et al., 2004; Ciardhuáin, 2004; Freiling & Schwittay, n.d.; Kohn et al., 2013a; Montasari, 2016b; Valjarevic & Venter, n.d.).

Tan (2001a) telah mempelopori satu bahagian penting dalam forensik digital dengan memperkenalkan konsep kesediaan forensik digital (KFD). Merujuk kepada definisi yang diberi oleh Tan (2001a), KFD merupakan keupayaan organisasi untuk memaksimumkan persekitaran untuk mengumpul bukti digital yang boleh dipercayai; dan meminimumkan kos forensik dalam tindak balas insiden. KFD melibatkan penubuhan dan pelaksanaan dasar, prosedur dan langkah teknikal yang membolehkan pengumpulan, pemeliharaan, analisis dan pembentangan bukti digital yang berkesan dan cekap sekiranya berlaku insiden (Bankole et al., 2022). Matlamat KFD adalah untuk memastikan organisasi bersedia untuk bertindak balas terhadap insiden digital, meminimumkan kesan ketidakpatuhan keselamatan dan memudahkan proses penyiasatan. Berdasarkan matlamat tersebut, kajian ini membangunkan satu model KFD yang boleh dijadikan sebagai panduan dan dasar dalam persediaan untuk kemungkinan berlaku jenayah berkaitan teknologi maklumat. Seperti yang dijelaskan

oleh Shin (2008), jenayah berkaitan teknologi maklumat bukan sahaja melibatkan penggunaan komputer semata-mata tetapi termasuk berbagai bentuk peranti berteknologi maju juga. Untuk kajian ini, istilah digital akan digunakan sebagai istilah umum untuk merujuk kepada peranti elektronik yang mungkin digunakan untuk melakukan jenayah.

1.3 Pernyataan Masalah

Perlaksanaan kesediaan forensik digital (KFD) dalam penyiasatan adalah penting pada masa kini berikutan peningkatan jumlah kes jenayah digital dan keperluan untuk menyelesaikannya dalam tempoh yang singkat dengan kos yang minimum (Chernyshev et al., 2019; Kebande et al., 2018b; Mouhtaropoulos et al., 2011). Kajian oleh Microsoft pada 2018 mendedahkan potensi kerugian ekonomi di Malaysia akibat insiden keselamatan siber telah menelan kos AS$12.2 bilion (Gnaneswaran, 2018). Disebabkan peningkatan bilangan insiden serangan siber, organisasi keselamatan siber perlu mempunyai satu pelan persediaan menghadapi situasi tersebut. Laporan oleh Point Software (n.d.) menyatakan bahawa pelbagai ancaman dan serangan siber telah berlaku termasuk berjuta-juta pelanggaran data, kata laluan terdedah, penggodaman syarikat anti-virus, perisian tebusan, serangan siber perkhidmatan awan serta data perubatan kes yang telah digodam. Laporan itu juga meramalkan lebih banyak lagi kejadian akan meningkat pada masa hadapan. Microsoft juga menerbitkan laporan yang dipanggil *Microsoft Digital Defense Report* yang menunjukkan peningkatan ancaman siber berkembang dengan pantas (Digital & Report, 2020). Pandemik COVID-19 global dimanipulasi oleh penyerang untuk menyasarkan pengguna Internet dengan vektor ancaman baharu dan eksploitasi

baharu. Justeru, pengamal keselamatan siber harus bersedia untuk menghadapi kejadian yang tidak diduga. Tanpa proses sistematik ketika melaksanakan penyiasatan forensik akan mengakibatkan kehilangan masa, kos, dan juga bukti berpotensi (Alenezi et al., 2017a).

Adil (2015) yang mengetuai Jabatan Forensik Digital bagi Keselamatan Siber Malaysia menekankan dalam pembentangannya bahawa proses keselamatan maklumat sentiasa tertumpu kepada pencegahan dan pengesanan, dengan pengumpulan bukti digital yang sangat sedikit. Dengan adanya panduan dalam KFD, bukti dapat diperolehi dengan optimum, maka ia dapat membantu mengurus risiko dalam penyiasatan, menyediakan proses undang-undang dan pembelaan, selain menyokong tindakan tatatertib peringkat dalaman (Elyas et al., 2014a).

Sesi temu bual semasa pengesahan model konseptual awal yang dijalankan bersama beberapa pegawai agensi penguatkuasaan mengesahkan bahawa Malaysia tidak mempunyai sebarang pelan yang bertumpu kepada KFD sebagai dasar yang boleh dijadikan rujukan oleh organisasi keselamatan siber. Walau pun pihak kerajaan telah mengeluarkan satu garis panduan bernama Strategi Keselamatan Siber Malaysia pada tahun 2020, dokumen tersebut hanya menekankan program kesediaan keselamatan siber yang merangkumi satu siri latihan direka bentuk untuk menguji keberkesanan prosedur di bawah Pelan Pengurusan Krisis Siber Kebangsaan (National Security Council, 2020). Program ini khusus untuk menilai kesediaan dan kesediaan agensi infrastruktur negara yang kritikal terhadap serangan siber di mana ia lebih menekankan persediaan langkah-langkah yang jelas dalam mempertahankan