FASA KESEDIAAN DIGITAL FORENSIK BAGI KERAJAAN NEGERI JOHOR

RUZANA BINTI JAFFAR

UNIVERSITI TEKNOLOGI MALAYSIA

FASA KESEDIAAN DIGITAL FORENSIK BAGI KERAJAAN NEGERI JOHOR

RUZANA BINTI JAFFAR

Laporan projek ini dikemukakan sebagai memenuhi
sebahagian daripada keperluan tujuan
penganugerahan Ijazah Sarjana Sains Komputer (Keselamatan Maklumat)

Fakulti Komputeran
Universiti Teknologi Malaysia

JUN 2013

ABSTRAK

Pada masa kini terdapat banyak insiden yang membabitkan peranti digital perlu dititikberatkan oleh penjawat awam Kerajaan Negeri Johor. Terdapat banyak salahlaku membabitkan maklumat digital yang dipandang ringan oleh pihak pengurusan dan tiada garis panduan atau polisi jika penjawat awam menggunakan internet untuk kegunaan peribadi, melakukan jenayah yang berkaitan dokumen elektronik sebagai bukti, mencuri maklumat daripada komputer pejabat, gangguan seksual menggunakan mel elektronik, penggunaan telefon bimbit untuk urusan rasmi dan pelbagai aktiviti menggunakan rangkaian Kerajaan Negeri Johor. Kerajaan Negeri Johor tidak mempunyai sebarang polisi untuk berhadapan dengan senario begini terutama apabila membabitkan prosiding perundangan. Kajian projek dijalankan ke atas permasalahan ini dengan objektif untuk mengenalpasti fasa dan aktiviti kesediaan digital forensik bagi Kerajaan Negeri Johor, mencadangkan fasa dan aktiviti kesediaan digital forensik dan deraf panduan maklumat bagi polisi kesediaan digital forensik Kerajaan Negeri Johor serta pengesahan fasa dan aktiviti kesediaan digital forensik dan deraf panduan maklumat bagi polisi kesediaan digital forensik Kerajaan Negeri Johor. Untuk mencapai matlamat kajian ke atas projek ini, pendekatan saintifik penyelidikan perlu dilaksanakan. Metodologi penyelidikan yang dilaksanakan bagi membantu mencapai matlamat kajian bagi projek ini adalah mengenalpasti masalah melalui pemerhatian, teori dan model, pengumpulan data, analisa data, hipotesis dan hasil penyelidikan. Hasil akhir kajian projek ini adalah fasa kesediaan digital forensik bagi Kerajaan Negeri Johor dan deraf panduan maklumat bagi polisi kesediaan digital forensik Kerajaan Negeri Johor. Kedua-dua hasil akhir projek ini dapat membantu Kerajaan Negeri Johor mempunyai garis panduan awal apabila berlaku insiden membabitkan bukti digital.

ABSTRACT

In reason years, there are many incidents involving digital devices which need to be taken seriously by the Johor State Government. There are numerous misconduct involving digital information taken lightly by the management and there are no guidelines or policies for the civil servants if they abuse the Internet for personal usage, committing cyber related crimes, stealing information from the office computers, sexual harassments using electronic mail, the usage of mobile phones for personal purposes and other unauthorized activities using the government's networking. Johor State Government has no policies to deal with this incidents especially those involving legal proceedings. Research projects are carried out on this problems with the objectives to identify, propose, draft guidelines policies and confirm the phases and digital forensic readiness activities for the Johor State Government. To achieve this objectives, a scientific approach to research must be implemented. The research methods apply are by identifying the problems through observations, theories and models, collecting and analyzing data, making hypothesis and research findings. The research will finally produce the phases of implementation and draft guidelines policies for digital forensic readiness. These will hopefully assist the Johor State Government should there be incidents involving digital evidence.

ISI KANDUNGAN

BAB	PERKARA	HALAMAN
	PENGAKUAN	ii
	DEDIKASI	iii
	PENGHARGAAN	iv
	ABSTRAK	v
	ABSTRACT	vi
	KANDUNGAN	vii
	SENARAI RAJAH	xiii
	SENARAI JADUAL	xv
	SENARAI LAMPIRAN	xix
1	**PENGENALAN**	1
	1.1 Pengenalan	1
	1.2 Latarbelakang Masalah	2
	1.3 Pernyataan Masalah	3
	1.4 Matlamat Kajian	5
	1.5 Objektif Kajian	5
	1.6 Skop Projek	5
	1.7 Signifikan Kajian	6
	1.8 Organisasi Laporan	7

2	**KAJIAN LITERATUR**		9
	2.1	Pengenalan	9
	2.2	Komputer Forensik	10
	2.3	Perbezaan Pakar Komputer dan Pakar Forensik	11
	2.4	Digital Forensik	14
	2.5	Kajian Kes Jenayah Digital Forensik	17
	2.6	Kajian Digital Forensik Di Sektor Awam dan Swasta di Malaysia	20
	2.7	Penyiasatan Digital Forensik	32
	2.8	Teknik Anti Forensik	34
	2.9	Model Penyiasatan Digital Forensik	36
	2.10	Kesediaan Digital Forensik	42
	2.11	Model Kesediaan Digital Forensik	48
	2.12	Faedah Kesediaan Digital Forensik	54
	2.13	Polisi Kesediaan Digital Forensik	55
	2.14	Kajian Polisi dan Garis Panduan Berkaitan Digital Forensik	57
		2.14.1 Negara Luar	57
		2.14.2 Kerajaan Negeri Johor	65
	2.15	Kesimpulan	66
3	**METODOLOGI PENYELIDIKAN**		67
	3.1	Pengenalan	67
	3.2	Rangka Kerja Kajian	68
		3.2.1 Fasa 1: Kenalpasti Masalah	71
		3.2.2 Fasa 2: Mencadangkan Fasa dan Aktiviti Kesediaan Digital Forensik	73
		3.2.3 Fasa 3:Pengesahan Fasa Kesediaan Digital Forensik dan deraf panduan maklumat	75

3.3 Kesimpulan 77

4 CADANGAN FASA KESEDIAAN DIGITAL FORENSIK 78

4.1 Pengenalan 78

4.2 Perancangan Menghasilkan Fasa Kesediaan Digital Forensik 79

4.2.1 Keperluan Fasa Kesediaan Digital Forensik 80

4.2.2 Pemilihan Fasa Kesediaan Digital Forensik 82

4.2.3 Pemilihan Aktiviti bagi Fasa Kesediaan Digital Forensik 82

4.2.4 Deraf Kandungan Fasa dan Aktiviti Kesediaan Digital Forensik 83

4.2.5 Pengesahan Deraf Cadangan Fasa Kesediaan Digital Forensik oleh Pakar 86

4.3 Perancangan Menghasilkan Deraf Panduan Maklumat Bagi Polisi Kesediaan Digital Forensik Kerajaan Negeri Johor 86

4.4 Kesimpulan 88

5 HASIL DAN PENEMUAN 89

5.1 Pengenalan 89

5.2 Analisis Hasil Temubual 90

5.3 Pakar Bagi Pengesahan Fasa dan Aktiviti Kesediaan Digital Forensik 94

5.4 Analisis Pengesahan Fasa dan Aktiviti oleh Pakar 95

5.5 Pengesahan Pakar Bagi Fasa Kesediaan Digital Forensik 96

5.6 Pengesahan Pakar Bagi Aktiviti Fasa Perancangan Dan Persediaan Sumber dan Peranan 99

5.6.1 Kenalpasti Peranan Pengurusan Atasan 100

5.6.2 Kenalpasti Tanggungjawab Penjawat Awam di Pentadbiran Kerajaan Negeri Johor 102

5.6.3	Kenalpasti Objektif	102
5.6.4	Kenalpasti Limitasi Skop	102
5.6.5	Kenalpasti Risiko Bukti Digital	104
5.6.6	Menguruskan Pasukan Kerja Bagi Kesediaan Digital Forensik	105
5.6.7	Dokumentasi Berkaitan Insiden Digital Forensik Dan Bukti Digital	106
5.7	Pengesahan Pakar Bagi Aktiviti Fasa Pengumpulan Elemen Kesediaan Digital Forensik	110
5.7.1	Kenalpasti Aset Digital	111
5.7.2	Tentukan Proses Kesediaan Digital Forensik	113
5.7.3	Kenalpasti Metodologi Penyiasatan Kesediaan Digital Forensik	115
5.7.4	Prosidur Penyerahan Bukti Digital	116
5.7.5	Pengurusan Rekod Bukti Digital	118
5.8	Pengesahan Pakar Bagi AKtiviti Fasa Latihan dan Penguatkuasaan	123
5.8.1	Kendalikan Program Latihan dan Kesedaran Bagi Penjawat Awam	124
5.8.2	Perundangan	125
5.8.3	Penguatkuasaan	125
5.9	Pengesahan Pakar Bagi Aktiviti Fasa Pematuhan Dan Pemantauan	127
5.9.1	Kemaskini Polisi	128
5.9.2	Dokumentasi	129
5.9.3	Polisi Yang Dikemaskini Kepada Pasukan Kerja dan Keselamatan	129
5.9.4	Audit Polisi	129
5.10	Cadangan Baru Fasa Kesediaan Digital Forensik Bagi Kerajaan Negeri Johor	132
5.11	Pengesahan Deraf Panduan Maklumat Bagi	

Polisi Kesediaan Digital Forensik 133

5.12 Kesimpulan 134

6 PERBINCANGAN DAN KESIMPULAN 135

6.1 Pengenalan 135

6.2 Perbincangan 135

6.2.1 Cadangan di Masa Hadapan 136

6.2.2 Cabaran dan Kekangan 136

6.3 Sumbangan 138

6.4 Kesimpulan 138

RUJUKAN 140

Lampiran A - M 145 - 235

SENARAI RAJAH

NO RAJAH	TAJUK	HALAMAN
2.1	Maklumat digital vs. Maklumat bukan digital	16
2.2	Anggaran bilangan kes merujuk komputer forensik di Mahkamah Perundangan Daerah Amerika, 2004-2010	19
2.3	Anggaran bilangan kes merujuk digital forensik di Mahkamah Perundangan Daerah Amerika , 2006-2010	19
2.4	Statistik kes jenayah digital 2002-2007 di Malaysia	20
2.5	Statistik kes jenayah digital 2002-2010 di Malaysia	21
2.6	Statistik kes jenayah digital Jan-Jun 2011 di Malaysia	22
2.7	Statistik kategori bukti digital 2007 di Malaysia	23
2.8	Statistik kategori jenayah digital forensik 2006 di Malaysia	24
2.9	Statistik kategori jenayah digital forensik 2008 di Malaysia	25
2.10	Statistik kategori jenayah digital forensik 2009 di Malaysia	25
2.11	Statistik kategori jenayah digital forensik 2010 di Malaysia	26
2.12	Statistik kategori jenayah digital forensik Jan-Jun 2011 di Malaysia	27
2.13	Statistik kes digital forensik mengikut jabatan 2002-2010 di Malaysia	29
2.14	Statistik kes digital forensik mengikut sektor	

	bagi pertengahan tahun 2011 di Malaysia	29
3.1	Rangka kerja kajian	69
4.1	Carta alir aktiviti merekabentuk polisi	80
4.2	Cadangan fasa kesediaan digital forensik bagi Kerajaan Negeri Johor	84

SENARAI JADUAL

NO JADUAL	TAJUK	HALAMAN
2.1	Perbandingan kemahiran teknikal	13
2.2	Perbandingan kemahiran undang-undang	14
2.3	Peratusan statistik jenayah membabitkan digital forensik 2007 sehingga pertengahan tahun 2011	31
2.4	Profil suspek di siasat	33
2.5	Teknik anti forensik positif	35
2.6	Teknik anti forensik negatif	35
2.7	Ringkasan senarai model penyiasatan digital forensik	37
2.8	Perbandingan kekuatan dan kelemahan bagi model penyiasatan digital forensik	38
2.9	Fasa kesediaan digital forensik di model penyiasatan digital forensik	43
2.10	Perbandingan fasa kesediaan digital forensik pada model penyiasatan digital forensik	46
2.11	Model kesediaan digital forensik	49
2.12	Perbandingan komponen pada model kesediaan digital forensik	51
2.13	Perbandingan aktiviti perlu ada dalam polisi kesediaan digital forensik	56
2.14	Senarai inisiatif berkaitan digital forensik di USA, UK, Australia dan Kanada	58
2.15	Senarai undang-undang siber di Malaysia	60

2.16	Senarai kandungan polisi kesediaan digital forensik merujuk kepada polisi yang telah dibangunkan	62
2.17	Perbandingan kandungan polisi yang telah dibangunkan	64
3.1	Objektif, aktiviti dan output kajian	70
4.1	Pemilihan aktiviti polisi kesediaan digital forensik	82
4.2	Cadangan fasa dan aktiviti kesediaan digital forensik bagi Kerajaan Negeri Johor	85
4.3	Cadangan deraf panduan maklumat bagi polisi kesediaan digital polisi Kerajaan Negeri Johor	87
5.1	Senarai responden bagi temubual	90
5.2	Data-data hasil temubual bersama Pegawai Tadbir Negeri Johor	91
5.3	Senarai pakar bagi pengesahan fasa dan aktiviti kesediaan digital forensik	94
5.4	Keputusan pengesahan bagi cadangan fasa kesediaan digital forensik	97
5.5	Keputusan pengesahan bagi susunan cadangan fasa kesediaan digital forensik	98
5.6	Keputusan pengesahan pakar bagi cadangan aktiviti fasa perancangan dan persediaan sumber dan peranan	100
5.7	Keputusan pengesahan cadangan elemen paling penting bagi aktiviti kenalpasti peranan pengurusan atasan	101
5.8	Keputusan pengesahan cadangan elemen bagi aktiviti kenalpasti limitasi skop	103
5.9	Keputusan pengesahan cadangan kriteria bagi aktiviti menguruskan pasukan kerja bagi kesediaan digital forensik	106
5.10	Keputusan pengesahan bagi susunan cadangan aktiviti fasa perancangan dan persediaan sumber dan peranan	107
5.11	Keputusan pengesahan bagi cadangan aktiviti fasa pengumpulan elemen kesediaan digital forensik	111

5.12	Keputusan pengesahan cadangan aset bagi aktiviti kenalpasti aset digital	112
5.13	Keputusan pengesahan cadangan kriteria bagi aktiviti tentukan proses kesediaan digital forensik	114
5.14	Keputusan pengesahan cadangan kriteria bagi aktiviti kenalpasti metodologi penyiasatan kesediaan digital forensik	115
5.15	Keputusan pengesahan cadangan kriteria bagi aktiviti prosidur penyerahan bukti digital	117
5.16	Keputusan pengesahan cadangan elemen bagi aktiviti kenalpasti pengurusan rekod bukti digital	119
5.17	Keputusan pengesahan bagi susunan cadangan aktiviti fasa pengumpulan elemen kesediaan digital forensik	121
5.18	Keputusan pengesahan bagi cadangan aktiviti fasa latihan dan penguatkuasaan	124
5.19	Keputusan pengesahan susunan cadangan aktiviti fasa latihan dan penguatkuasaan	126
5.20	Keputusan pengesahan bagi cadangan aktiviti fasa pematuhan dan pemantauan	128
5.21	Keputusan pengesahan cadangan tempoh audit bagi audit polisi	130
5.22	Keputusan pengesahan cadangan aktiviti fasa pematuhan pemantauan	131

SENARAI LAMPIRAN

LAMPIRAN	TAJUK	HALAMAN
A	Kajian kes jenayah digital forensik dan kesan ke atas organisasi dan individu	145
B	Senarai model penyiasatan digital forensik	153
C	Perbandingan aktiviti fasa model penyiasatan digital forensik	162
D	Senarai polisi dan garis panduan berkaitan kesediaan digital forensik yang digunapakai di Kerajaan Negeri Johor	166
E	Senarai pengesahan pegawai tadbir Negeri Johor yang ditemubual	172
F	Soalan temubual pegawai tadbir Negeri Johor	176
G	Pakar bagi pengesahan cadangan fasa dan aktiviti kesediaan digital forensik	180
H	Skrip pengesahan fasa kesediaan digital forensik	198
I	Contoh jawapan skrip pengesahan fasa kesediaan digital forensik	215
J	Ringkasan perubahan ke atas cadangan fasa dan aktiviti kesediaan digital forensik bagi Kerajaan Negeri Johor	232
K	Fasa kesediaan digital forensik bagi Kerajaan Negeri Johor	233
L	Deraf panduan maklumat bagi polisi kesediaan digital forensik Kerajaan Negeri Johor	234
M	Panduan maklumat bagi polisi kesediaan digital forensik Kerajaan Negeri Johor	235

BAB 1

PENGENALAN

1.1 Pengenalan

Di Malaysia terutamanya di agensi-agensi kerajaan sama ada kerajaan negeri atau persekutuan, pemahaman mengenai digital forensik adalah amat kurang walaupun kesedaran tentang digital forensik semakin meningkat. Kebanyakan penjawat awam di Kerajaan Negeri Johor tiada kesedaran kepentingan digital forensik dan bagaimana kerja seharian mereka di pejabat menyumbang kepada pendedahan jenayah membabitkan bukti digital.

Digital forensik adalah bidang yang luas melibatkan keselamatan komputer dimana matlamat utama adalah untuk mengenalpasti dan melindungi bukti digital yang dijadikan bukti apabila terdapat salahlaku dan aktiviti jenayah (Endicott dan Frincke, 2006). Dengan pertumbuhan teknologi digital yang ada di pasaran sekarang seperti tablet, ipad, storan yang lebih kecil, telefon pintar yang semakin canggih, storan di dalam pelbagai bentuk seperti jam tangan dan sebagainya begitu juga dengan kemajuan audio , video dan imej menyumbang kepada peningkatan jenayah digital forensik.

Satu polisi berkaitan kesediaan digital forensik adalah perlu bagi membolehkan penjawat awam dan agensi di Kerajaan Negeri Johor bersedia menghadapi kemungkinan jenayah digital yang membabitkan bukti digital.

Kesediaan digital forensik adalah satu proses kesediaan bagi penyiasatan digital sebelum sesuatu insiden berlaku. Ini bermakna bila insiden dikenalpasti, pasukan kerja, polisi, prosidur dan penjawat awam berada dalam keadaan yang bersedia dan profesional untuk memberikan maklumbalas dengan gangguan ke atas perkhidmatan berada di tahap minimum (QinetiQ, 2010).

Kesediaan digital forensik akan membantu Kerajaan Negeri dalam keadaan bersedia apabila bukti digital diperlukan untuk kes jenayah atau masalah disiplin melibatkan penjawat awam. Kesediaan digital forensik akan membantu Kerajaan Negeri menggunakan maklumat digital sebagai bukti digital secara maksima dengan kos yang minimum. Organisasi yang telah bersedia dengan potensi jika berlaku insiden membabitkan undang-undang dengan mengumpul dan melindungi data digital sebenarnya akan dapat mengurangkan kos apabila melibatkan prosiding undang-undang (Rowlinson, 2004).

1.2 Latarbelakang Masalah

Maklumat digital yang boleh dijadikan bukti digital banyak digunakan sama ada untuk kegunaan peribadi atau membabitkan urusan kerja di kalangan penjawat awam Kerajaan Negeri Johor. Walaupun kadar jenayah digital dilaporkan oleh Cybersecurity Malaysia menunjukkan peningkatan setiap tahun, namun tiada sebarang garis panduan atau polisi yang dibangunkan berkaitan digital forensik atau kesediaan bagi menghadapi sebarang insiden berkaitan maklumat digital oleh pihak Kerajaan Negeri Johor begitu juga Kerajaan Persekutuan. Kebanyakan polisi yang dibangunkan berkaitan penggunaan mel elektronik, internet dan keselamatan ICT tanpa pengkhususan mengenai kesediaan menghadapi jenayah digital forensik.

Pada masa kini terdapat banyak insiden yang membabitkan peranti digital perlu dititikberatkan oleh penjawat awam Kerajaan Negeri Johor . Terdapat banyak salahlaku membabitkan maklumat digital yang dipandang ringan oleh pihak

pengurusan , sebagai contoh terdapat garis panduan dan tindakan tatatertib yang perlu dilaksanakan jika seseorang penjawat awam tidak hadir kerja tetapi tiada garis panduan atau polisi jika penjawat awam menggunakan internet untuk kegunaan peribadi, melakukan jenayah yang berkaitan dokumen elektronik sebagai bukti, mencuri maklumat daripada komputer pejabat, gangguan seksual menggunakan mel elektronik, penggunaan telefon bimbit untuk urusan rasmi dan pelbagai aktiviti menggunakan rangkaian Kerajaan Negeri Johor. Kerajaan Negeri Johor tidak mempunyai sebarang polisi untuk berhadapan dengan senario begini terutama apabila membabitkan prosiding perundangan.

Oleh yang demikian, Kerajaan Negeri Johor perlu membangunkan polisi berkaitan dengan keseluruhan proses melibatkan digital forensik bagi memberikan satu panduan kepada penjawat awam dan mengurangkan kos serta risiko apabila berlakunya jenayah membabitkan digital forensik. Sebagai langkah awal, fasa kesediaan digital forensik dan deraf panduan maklumat bagi polisi kesediaan digital forensik perlu dibangunkan sebagai rujukan kepada semua penjawat awam di Kerajaan Negeri Johor. Kesediaan Digital Forensik adalah keupayaan Kerajaan Negeri Johor dan semua penjawat awam untuk memaksimakan potensi untuk menggunakan bukti digital dan pada masa yang sama mengurangkan kos penyiasatan (Tan, 2010).

1.3 Pernyataan Masalah

Kerajaan Negeri Johor tidak mempunyai sebarang polisi atau garis panduan berkaitan digital forensik. Adalah amat penting pada masa kini untuk membangunkan polisi sekurang-kurangnya berkaitan kesediaan digital forensik. Kesediaan digital forensik adalah kebolehan untuk mengumpul, melindungi dan menganalisa bukti digital yang boleh digunakan secara efektif dalam apa jua keadaan seperti tribunal pekerja, undang-undang mahkamah, penyiasatan keselamatan dan masalah disiplin. Alasan terbaik untuk menggunakan forensik di Kerajaan Negeri Johor adalah untuk membantu pengurusan insiden dan mengenalpasti fail yang

terlibat apabila sesuatu insiden berlaku. Terdapat banyak kes di Kerajaan Negeri Johor dimana penjawat awam menyalahguna peranti digital atau rangkaian dan infrastruktur Kerajaan Negeri untuk mendedahkan maklumat sulit kerajaan atau untuk kegunaan peribadi dan pelbagai ancaman lain. Polisi dan garispanduan sedia ada berkaitan keselamatan ICT dan pengurusan insiden tidak mencukupi untuk melindungi Kerajaan Negeri jika terdapat jenayah membabitkan digital forensik.

Oleh itu sebagai pendekatan awal , Kerajaan Negeri Johor perlu mengenalpasti fasa kesediaan digital forensik seterusnya membangunkan polisi kesediaan digital forensik bagi melindungi bukti digital sebelum sesuatu insiden berlaku. Bukti digital akan digunakan di dalam kes yang melibatkan proses formal dan perundangan. Kerajaan Negeri Johor perlu mempunyai capaian kepada bukti digital yang diperlukan untuk menyokong sebarang kes yang memerlukan prosiding perundangan atau bukti digital sebagai bukti sesuatu kes. Dengan itu terdapat kepentingan bagi Kerajaan Negeri Johor untuk melindungi bukti digital sebelum sesuatu insiden berlaku. Mengenalpasti fasa serta aktiviti kesediaan digital forensik yang bersesuaian akan membantu Kerajaan Negeri Johor untuk membangunkan polisi bagi memaksimakan keupayaan untuk menggunakan bukti digital dan mengurangkan kos apabila melibatkan penyiasatan maklumat digital dan prosiding undang-undang perlu dilakukan sama ada membabitkan penjawat awam atau pihak luar.

Fasa kesediaan digital forensik yang telah dikenalpasti akan membantu Kerajaan Negeri membangunkan polisi kesediaan digital forensik yang dapat memberikan amaran awal serta kesedaran kepada penjawat awam mengenai tindakan yang boleh diambil jika mereka menceroboh atau menyalahguna maklumat digital. Ini kerana ancaman paling bahaya adalah penjawat awam sendiri kerana mereka mempunyai capaian terus ke atas maklumat sulit Kerajaan Negeri Johor dan kurangnya kesedaran mengenai digital forensik juga boleh mengakibatkan ancaman jenayah membabitkan digital forensik daripada pihak luar.

1.4 Matlamat Kajian

Matlamat Kajian ialah untuk mengenaplasti fasa kesediaan digital forensik dan fasa yang diperolehi akan membantu di dalam penghasilan deraf panduan maklumat bagi polisi kesediaan digital forensik dan membolehkan Kerajaan Negeri Johor membangunkan polisi kesediaan digital forensik. Polisi kesediaan digital forensik membantu Kerajaan Negeri Johor bersedia di dalam pengumpulan dan penggunaan bukti digital dan juga memberikan faedah untuk melindungi maklumat digital daripada ancaman luaran dan dalaman.

1.5 Objektif Kajian

i. Mengenalpasti fasa dan aktiviti kesediaan digital forensik bagi Kerajaan Negeri Johor.
ii. Mencadangkan fasa dan aktiviti kesediaan digital forensik dan deraf panduan maklumat bagi polisi kesediaan digital forensik Kerajaan Negeri Johor.
iii. Pengesahan fasa dan aktiviti kesediaan digital forensik dan deraf panduan maklumat bagi polisi kesediaan digital forensik Kerajaan Negeri Johor.

1.6 Skop Projek

Skop projek adalah untuk mengenalpasti fasa serta aktiviti kesediaan digital forensik serta menghasilkan satu deraf cadangan panduan maklumat bagi polisi kesediaan digital forensik Kerajaan Negeri Johor. Projek ini hanya akan meliputi pengenalpastian fasa dan aktiviti kesediaan digital forensik serta cadangan deraf panduan maklumat polisi sebagai panduan kepada Kerajaan Negeri untuk

membangunkan polisi kesediaan digital forensik bagi mengumpul dan melindungi bukti digital sebelum sesuatu insiden jenayah membabitkan bukti digital berlaku. Kajian akan fokus kepada Unit Sains, Teknologi dan ICT Negeri Johor sebagai agensi induk di Kerajaan Negeri Johor yang membangunkan polisi bagi agensi-agensi Kerajaan Negeri Johor yang lain dan pegawai tadbir Negeri Johor sebagai responden.

1.7 Signifikan Kajian

Kajian projek ini dijalankan bagi membantu Kerajaan Negeri Johor membuat persediaan awal ke atas bukti digital sebelum sesuatu insiden berlaku. Kesediaan menghadapi insiden membabitkan bukti digital ini akan menjadi matlamat korporat Kerajaan Negeri Johor yang mengandungi tindakan teknikal dan bukan teknikal yang akan membantu memaksimakan keupayaan Kerajaan Negeri Johor menggunakan bukti digital. Sebarang maklumat digital berkemungkinan digunakan di dalam proses formal dan mempunyai kaitan dengan forensik. Keupayaan Kerajaan Negeri Johor melindungi dan menganalisa di peringkat awal bukti digital ini akan membantu pihak Kerajaan Negeri melindungi maklumat sulit kerajaan dalam bentuk digital dan seterusnya mengurangkan risiko berlakunya insiden membabitkan maklumat digital dan mempertingkatkan mutu perkhidmatan dan keyakinan rakyat terhadap Kerajaan Negeri Johor disamping memberikan banyak faedah kepada Kerajaan Negeri . Fasa dan aktiviti kesediaan digital forensik yang dicadangkan akan membantu Kerajaan Negeri Johor membangunkan polisi kesediaan digital forensik dimana Polisi Kesediaan Digital Forensik boleh memberikan faedah-faedah berikut kepada Kerajaan Negeri:

i. Mekanisma pertahanan membabitkan maklumat digital dapat dikenalpasti dan bertindak sebagai pencegahan kepada ancaman dalaman.

ii. Apabila berlaku insiden, gangguan ke atas perkhidmatan dapat diminimumkan dan kesinambungan dengan Pelan Kesinambungan Perkhidmatan dapat dilaksanakan dengan segera.

iii. Mengurangkan kos dan masa penyiasatan digital forensik di peringkat dalaman serta mempertingkatkan keselamatan maklumat daripada pelbagai ancaman jenayah siber.

iv. Mempetingkatkan imej Kerajaan Negeri Johor sebagai agensi kerajaan yang mempunyai ketelitian dan kawalan yang baik ke atas bukti digital.

v. Mempertingkatkan potensi untuk berjaya apabila melibatkan tindakan undang-undang.

vi. Mempertingkatkan keupayaan untuk tindakan undang-undang ke atas penjawat awam yang menyalahgunakan maklumat digital.

1.8 Organisasi Laporan

Bab ini menerangkan tentang pengenalan berkaitan dengan tajuk projek, matlamat, skop projek, pernyataan masalah serta latar belakang masalah dan faedah yang diperolehi daripada kajian projek ini. Bab yang seterusnya ialah kajian literatur. Bab 2 menerangkan mengenai kajian – kajian lepas yang telah dibuat serta garis panduan yang telah dibangunkan yang mempunyai kaitan dengan projek yang sedang dibangunkan. Bab ini juga meliputi model, statistik, kaedah atau teknologi yang telah diambil dalam melaksanakan projek. Bab 3 iaitu metodologi penyelidikan, melaporkan pendekatan dan rangka kerja secara menyeluruh yang perlu diambil sepanjang pelaksanaan kajian terhadap projek ini dibuat termasuk pendekatan justifikasi dan rangka kerja yang digunakan. Dalam Bab 4 adalah penemuan dan analisis awal mengenai kajian yang dibuat iaitu cadangan fasa dan aktiviti kesediaan digital forensik serta cadangan deraf panduan maklumat kesediaan digital forensik bagi Kerajaan Negeri Johor. Bab 5 iaitu hasil dan penemuan adalah analisis temubual dan pengesahan pakar ke atas fasa dan aktiviti kesediaan digital forensik serta cadangan baru fasa dan aktiviti kesediaan digital forensik serta deraf kerangka

maklumat polisi kesediaan digital forensik bagi Kerajaan Negeri Johor setelah dikajisemula dan diperbetulkan. Bab 6 meliputi kesimpulan dan perbincangan berkaitan sepanjang pelaksanaan projek.

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

Casey, E. (2004). Digital Evidence and Computer Crime 2nd Edition. *Elsevier Academic Press*

Ciardhuain, S. O. (2004) . An Extended Model of Cybercrime Investigation . *International Journal of Digital Evidence* . Volume 3(1), 1-22.

Cresson et.al. (1987). Computer Security: A Comprehensice Controls checklist. *John Wiley & Sons.*

CyberSecurity Malaysia. (2007). Digital Crimes Yearly Statistic 2007.

CyberSecurity Malaysia (2008). Digital Crimes Yearly Statistic 2008.

CyberSecurity Malaysia (2009). Digital Crimes Yearly Statistic 2009.

CyberSecurity Malaysia (2010). Digital. Crimes Yearly Statistic 2010

CyberSecurity Malaysia (2011). Digital Crimes Yearly Statistic 2011

Denning, D. E. (2000) . Hacktivitism: an emerging threat to diplomacy, American Foreign Service Association. http://www.afsa.org/sept00/Denning.cfm.

De Kloet, J. (2002). Digitisation and its Asian discontents: the Internet, politics and hacking in China and Indonesia. *First Monday.* http://firstmonday.org/issues/issue7_9/kloet/index.html.

Endicott-Popovsky B dan Frincke D. (2006). Embedding forensic capabilitiesinto networks: addressing inefficiencies in digital forensics investigations. *Proceedings of the 2006 IEEE workshop on information assurance: computer forensics*. West Point, NY.

Forte, D. dan Power, R. (2008). War & Peace in Cyberspace: Internal fraud – when system administrators leave. *Computer Fraud and Security***.**

Freiling, F.C. dan Schwittay, B. (2007) . Common Process Model for Incident and Computer Forensics. *Proceedings of Conference on IT Incident Management and IT Forensics,*. Stuttgard, Germany, 19-40.

Freiling, F. (2007) . A Common Process Model for Incident Response and Digital Forensic,. *Proceedings of the IMF2007.*

Freiling,F.C. dan Schwittay, B. (2010). A Common Process Model for Incident Response and Computer Forensics. *Journal of Computer Applications.*.Volume 1 (11).

Gorman S. (2010). Gorman S. U.S. aims to Bolster Overseas fight against cybercrime.*The Wall Street Journal*.

Grobler, C. P., & Louwrens, B. (2006). Digital Forensics: A Multi-Dimensional Discipline. *Proceedings of the ISSA 2006 from Insight to Foresight Conference. Pretoria*: University of Pretoria.

Hamzah, Z. (2005). E-Security Law & Strategy. *Malayan Law Journal Sdn Bhd* . 47301, 122.Reith , M. , Carr, C. dan Gunsch, G. (2002). An Examination of Digtal Forensic Models. *International Journal of Digital Evidence.*Volume 1 (Issue 3).

Hilley, Sarah. The corporation: the non-policed state**.** *Computer Forensic and Fraud* CBS. (2009). Cyberwar: sabotaging the system. Volume 60.

Howard, J.D. dan Longstaff T.A. A common language for computer security incidents . *Sandia National Laboratories,Tech. Rep.*

Imtiaz, F.(2006). Enterprise Computer Forensics. *Proceedings of the 4th Australian Digital Forensics Conference* .Perth: Edith-Cowan University, 29-35.

Jordaan, J.(2009). The case for digital forensic readiness. Unpublished.

Kohn, M. Eloff, J.H.P. , Olivier, M.S. (2006). Framework for a Digital Forensic Investigation. *Proceedings of the ISSA 2006 from Insight to Foresight Conference.* South Africa.

Kohn, M., Eloff , J . dan Olivier, M. . Framework for Digital Forensic Investigation: *Information and Computer Security Architectures Research Group (ICSA).* University of Pretoria.

Mandia , et al. (2003). Incident Response & Computer Forensics. (2nd Ed.) McGraw-Hill/Osborne, Emeryville

Meadaris, K.(20060. Grants to help develop ways to improve digital evidence collection.PurdueUniversity,<http://www.purdue.edu/UNS/html4ever/2006/061012RogersGrant.html>.

Mouhtaropoulos, A. dan Grobler, M. (2011). Digital Forensic Readiness: An insight into Governmental and Academic Initiatives. *European Intelligence and Security Informatics Conference. IEEE.*

Narayan, A.S. dan Ashik, M.M.. (2012). Computer Forensic First Responder Tools. *International Conference on Advances in Mobile Network, Communication and Its Applications.*

Nardoni D. (2005). Introduction to Computer Forensics. *Digital Investigation.* El sevier Ltd. Garfinkel, S.L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, Digital Forensic Research Workshop.* Elsevier

Ltd. Politt, M.M. (2004) . Six Blind Men From Indostan . *Digital Forensics Research Workshop.*

Palmer G. (2001). DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research. *Digital Forensics Workshop.*New York.

Perumall, S. (2009). Digital Forensic Model Based On Malaysian Investigation Process. IJCSNS *International Journal of Computer Science and Network 38 Security,*. Volume 9 (8).

Pilli, E.S., Joshi,R.C. dan Niyogi, R. (2010). Network Forensic frameworks: Survey and research challenges. *Digital Investigation* . Volume 7, 14-27.

Pilli, E.S. dan Joshi, R.C. (2011). A Generic Framework for Network Forensics. *International Journal of Computer Science & Information Technology (IJCSIT),*. Volume 3 .

Pollitt ,M.M. (1995) . Computer Forensics : An Approach to Evidence in Cyberspace . *Proceeding of the National Information Systems Security Conference.* Volume II, 487-491.

Pollitt, M.M. (2007). An Ad Hoc Review of Digital Forensic Models . *Proceeding of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering*. Washington, USA.

Pooe, A. dan Labuschagne, L. (2012). A conceptual model for digital forensic readiness. *IEEE.*

Reith, M., Carr, C., Gunsh, G. (2002) . An Examination of Digital Forensics Models. *International Journal of Digital Evidence*. Volume 1 (3).

Ricci, S.C. (2006) . FORZA – Digital forensics investigation framework that incorporate legal issues . *Digital Investigation .29-36* .

Ruibin, G. dan Gaertner, M. (2005) . Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework **.** *International Journal of Digital Evidence Spring*. Volume 4 (Issue 1).

Rogers, M.K.,et al. (2006). Computer Forensic Field Triage Process Model. *Conference on Digital Forensics, Security and Law*. 27-40

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence.*

Smith , F.C dan Bace, R.G. (2003). A Guide to Forensic Testimony : The Art and Practice of Presenting Testimony As An Expert Technical Witness. *Addison Wesley Professional*.

Sommer P. (2005) . Directors and Corporate Advisor's Guide to Digital Investigations and Evidence. *Information Assurance Advisory Council.*

Stephenson, P. (2003) . A Comprehensive Approach to Digital Incident Investigation. *Information Security Technical Report* . Volume 8 (2), 42-52.

Sundresan, P. (2009). Digital Forensic Model based on Malaysian Investigation Process.*International Journal of Computer Science and Network Security*. Volume 9 (8).

Tan, J. (2001). Forensic readiness. Cambridge USA.

Taylora, C., Popovskyb.B.E., Frinckec D.A. (2007) . Specifying digital forensics: A forensics policy approach. *Digital Investigation* . 4S (2007). 101-104.

U.S District (1996). *Gates Rubber Company v. Bando Chemical Industries, Ltd, et al.*Lexis Nexis 12423.

U.S Cert ,2008

Valjarevic, A. (2011) . Towards a Digital Forensic Readiness Framework for Public Key Infrastructure Systems. *IEEE*.

Yasinsac, A. and Manzano, Y. (2001). Policies to Enhance Computer and Network Forensics. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security.*

Yusoff , Y. , Ismail, R. , Hassan, Z. (2011). Common Phases of Computer Forensics Investigation Models . *International Journal of Computer Science & Information Technology*. Volume 3, (No.3).