IMPLEMENTASI DIGITAL FORENSIK BRUNEI DARUSSALAM DALAM MEMBANGUN KEAMANAN SIBER

IMPLEMENTATION OF DIGITAL FORENSIC BRUNEI DARUSSALAM IN BUILDING CYBER SECURITY

Aryo C.K. Wardana[1], Rodon Pedrason[2], Triyoga Budi Prasetyo[3]
Universitas Pertahanan
(aryo.ckwardana@gmail.com, rodonpedrason65@gmail.com, tri_yoga_budi@yahoo.co.id)

Abstrak - Tantangan dunia *cyber* bukan merupakan sesuatu yang baru, terlebih lagi di era informasi dimana semua terkoneksi melalui internet, dengan berkembangnya perangkat untuk menyambungkan manusia dengan satu sama lain, seperti computer, smartphone, tablet, dan lain sebagainya semakin membuka peluang bagi para pelaku kejahatan untuk melancarkan serangan melalui dunia siber. Agar dapat mengatasi ancaman tersebut maka sangat diperlukan penanganan yang cepat dan tepat sasaran agar dapat segera diantisipasi. Salah satunya adalah dengan menggunakan *digital forensics*, sebuah acuan untuk menginvestigasi segala bentuk bukti digital yang dijadikan sebagai alat untuk melakukan *cybercrime*. Dalam tulisan ini, penulis melihat bagaimana pemerintah Brunei Darussalam mengimplementasikan *Digital Forensics* untuk meningkatkan *Cyber Security* di Brunei Darussalam. Dengan bekerja sama dengan pihak swasta dan beberapa lembaga lainnya yang terkait dengan penanggulangan *cybercrime* pemerintah Brunei Darussalam telah menciptakan sebuah struktur dan acuan yang cukup baik untuk dapat menghadapi berbagai ancaman *cyber* yang ada di Brunei Darussalam. Dengan demikian pemerintah Indonesia dapat mempelajari hal tersebut agar dapat menciptakan sebuah struktur dan acuan yang baik pula untuk dapat menghadapi ancaman *cyber* di Indonesia.
Kata kunci: Siber, Kejahatan Siber, Keamanan Siber, Forensik Digital

Abstract - *The challenges of the cyber world is not something new, especially in the information age where all connected via the Internet, with the development of devices to connect people with each other, such as computers, smartphones, tablets, and so the more opportunities for criminals to launch attacks through cyber world. In order to overcome such threats so it will need a fast and precise handling goals that can be anticipated. One of them is to use a digital forensics, a reference to investigate all forms of digital evidence that is used as a tool to commit cybercrime. In this paper, the authors look at how the government of Brunei Darussalam to implement Digital Forensics to boost Cyber Security in Brunei Darussalam. By working closely with the private sector and other institutions associated with cybercrime prevention Brunei government has created a structure and references were good enough to be able to deal with cyber threats that exist in Brunei Darussalam. Thus the government of Indonesia can learn it in order to create a structure and a good reference as well to be able to confront cyber threats in Indonesia.*
Key Words: *Cyber, Cybercrime, Cybersecurity, Digital Forensics*

[1] Penulis adalah Mahasiswa Pasca Sarjana Program Studi Peperangan Asimetris Cohort-5 TA. 2017 Fakultas Strategi Pertahanan, Universitas Pertahanan. Penulis dapat dihubungi melalui *email penulis.*
[2] Dr. rer. pol. Rodon Pedrason, M.A adalah Dosen Prodi Peperangan Asimetris Universitas Pertahanan.
[3] Dr. Triyoga Budi Prasetyo, M.Si adalah Dosen Prodi Peperangan Asimetris Universitas Pertahanan.

Pendahuluan

Seiring dengan bertambah maraknya serangan dan ancaman-ancaman asimetris di dunia digital yang berupa *cybercrime* pemerintah global dan para penegak hukum kini mulai mencari cara untuk mengatasi hal tersebut, *cybercrime* saat ini tengah menjadi sorotan dunia. Secara garis besar *cybercrime* hampir sama dengan kejahatan konvensional, namun telah dikembangkan dengan menggunakan teknologi sebagai alat untuk melakukan kejahatannya di sebuah dunia baru yang bernama dunia digital.

Penipuan, pencucian uang, pembajakan, penghinaan, adalah beberapa kejahatan konvensional yang saat ini telah berkembang menuju ke ranah asimetris dan tengah terjadi di dunia digital. Dikarenakan bentuk dunia digital yang tidak dapat dilihat secara langsung, jejak dari para pelaku kejahatan ini semakin sulit dideteksi secara fisik, melainkan harus dideteksi secara digital, dimana sebagian besar barang bukti kejahatan berada di dalam sebuah atau beberapa *device*. Dikarenakan jenis penanganannya yang tidak dapat diselesaikan secara biasa maka *cybercrime* merupakan salah satu jenis serangan asimetris.

Peningkatan jumlah *cybercrime* saat ini telah dianggap sebagai permasalahan serius oleh beberapa negara di seluruh dunia, seiring dengan pengoptimalisasian hukum dan pengamandemenan undang-undang guna memenuhi kebutuhan penanganan *cybercrime*. Kemampuan para penegak hukum-pun juga mulai ditingkatkan dengan pembekalan mengenai *digital forensics*, dan berbagai penelitian mengenai keamanan komputer dan investigasi di dunia digital-pun juga sudah mulai dikembangkan oleh para ahli komputer.

Apabila ditelusuri secara mendalam, *computer forensics* yang merupakan cikal bakal dari *digital forensics* mulai dikembangkan sebagai respon dari meningkatnya kejahatan yang didedikasikan dengan menggunakan sistem komputer sebagai objek kejahatannya, alat yang digunakan untuk melakukan kejahatan. Istilah *computer forensics* berawal pada tahun 1984 ketika laboratorium FBI dan penegak hukum lainnya di Amerika mulai mengembangkan sebuah program untuk menganalisa bukti

kejahatan komputer. Beberapa grup peneliti seperti *Computer Analysis Response Team (CART), The Scientific Working Group on Digital Evidence (TWGDE),* dan *The National Institute of Justice (NIJ)* telah dibentuk guna mengembangkan disiplin ilmu *computer forensics* termasuk berbagai kebutuhan untuk membuat acuan standar pelaksanaannya.[4]

Computer forensics adalah nama yang diberikan kepada ilmu mengenai cara mendeteksi kejahatan digital dalam dunia siber tanpa batasan lokasi geografis. Dr. H.B. Wolfe mendefinisikan *computer forensics* sebagai sebuah metode mengenai serangkaian teknik dan prosedur untuk mengumpulkan barang bukti, dari perangkat computer dan beberapa jenis alat penyimpanan, media digital, yang dapat dihadirkan dalam pengadilan secara koheren dan format yang berarti".[5]

Computer forensics, seperti yang telah didefinisikan oleh Wolfe merupakan konsentrasi utama dalam jurnal ini. Fokus utama adalah untuk mencari tahu metode apa yang digunakan untuk mengidentifikasi dan mendeteksi kejahatan digital dengan menggunakan perangkat komuter dan bagaimana cara memperoleh data guna memperkuat proses hukum kejahatan.

Digital forensics didefinisikan sebagai salah satu penggunaan ilmu dan metode yang telah teruji untuk menganalisa sumber digital guna memfasilitasi atau memperdalam gambaran rekonstruksi dari kejadian yang diduga sebagai sebuah tindak kejahatan, *digital forensics* juga dapat membantu mengantisipasi aksi ilegal yang terlihat dapat merusak jalannya rencana operasi. Salah satu elemen penting dalam *digital forensics* adalah kredibilitas dari bukti digital tersebut. Bukti digital yang berbentuk bukti komputer, audio digital, video digital, handphone, mesin fax, dan lain sebagainya. Para penegak hukum mengharapkan bukti digital memiliki integritas, keaslian, dapat direproduksi, tidak terpengaruh, dan dapat difokuskan. [6]

Digital forensics merupakan salah satu cabang ilmu pengetahuan yang berurusan dengan informasi digital yang diproduksi, disimpan, dan kemudian disalurkan melalui

[4] Michael Noblett, Mark.M.Pollitt and Lawrence Presley. (2000) Recovering and Examining Computer Forensic Evidence, Forensic Science Communications, Volume 2, Number 4.

[5] H M Wolfe, "Web Solutions and Technologies After the Hack", presented at *ICE Conference*, 2003

[6] Gary L Palmer. (2001). A Road Map for Digital Forensic Research. Technical Report DTRT0010-01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS).

computer sebagai salah satu bukti dari seluruh investigasi dan proses hokum. *The Digital Forensic Research Workshop* telah mendefinisikan *digital forensics* sebagai penggunaan ilmu pengetahuan pasti dan metode yang telah teruji untuk melakukan proses preservation, validation, identification, analysis, interpretation, documentation, dan presentation dari seluruh bukti digital yang diperoleh dari sumber digital dengan kegunaan untuk memfasilitasi atau memperdalam rekonstruksi dari sebuah kejadian yang diduga sebagai sebuah tindak kejahatan, atau untuk membantu proses guna mengantisipasi terjadinya kejadian kejahatan tersebut.[7]

Berbagai metode *computer forensics* dan juga *digital forensics* dikembangkan demi menghadapi berbagai jenis metode ancaman siber yang terdiri dari berbagai tingkatan dan saluran, selain itu metode *digital forensics* juga dikembangkan guna menghadapi peningkatan jumlah serangan siber yang sekarang telah menjadi tren global. Meskipun sudah dikembangkan namun masih sedikit negara-negara yang mengimplementasikan hal tersebut guna meningkatkan *cyber security* di negaranya.[8]

Tulisan ini akan menggunakan metode kualitatif dalam penulisan makalah. Metode ini dilakukan dalam memperoleh data-data yang diperlukan melalui studi literature, studi pustaka, *online research*, setra studi lapangan yang telah dilakukan pada tanggal 12-18 Maret 2017 di Bandar Seri Begawan, Brunei Darussalam. Basis dari penelitian ini adalah data primer yang ditemukan dalam Buku Putih Pertahanan Indonesia baik yang dikeluarkan oleh Kementerian Pertahanan Republik Indonesia pada tahun 2003 dan 2008, serta perundang-undangan yang menjadi dasar kebijakan. Sementara data primer dari pihak Brunei Darussalam kami temukan dalam *Brunei Visions 2035, Brunei's E-Government Program, Brunei's National Security Policy, Defense Planning Guidance,* serta perundang-undangan yang berkaitan dengan upaya peningkatan *Cyber Security*. Di samping itu juga digunakan data sekunder yang diperoleh dari berbagai

[7] Ryan Harris – DFRWS 2006 conference proceedings, Arriving at an Anti-forensics consensus

[8] S. S. Basamh, H. A. Qudaih and J. B. Ibrahim, "An Overview on Cyber Security Awareness in Muslim Countries," *International Journal of Information and Communication Technology Research,* vol. 4, no. 1, pp. 21-24, 2014.

sumber informasi yang relevan mengenai karakteristik *cyber-threats* dan upaya *digital forensics* yang telah dan akan dilakukan oleh Brunei Darussalam di samping penggunaan landasan teoretis yang relevan.

Brunei Darussalam dalam usahanya untuk mengontrol tingkat *cybercrime* telah membentuk beberapa lembaga yang bertujuan untuk menyediakan acuan guna menyelamatkan informasi, dan menyelamatkan pengguna saat sedang menelusuri dunia digital. Paper ini akan terbagi menjadi tiga sub-bab dimana isi dari masing-masing sub-bab adalah, **Sub-Bab I** Tantangan dan Isu *Cyber Security* Brunei Darussalam, **Sub-Bab II** *Digital Forensics* ITPSS Brunei Darussalam, **Sub-Bab III** Cara meningkatkan *Cyber Security* Brunei Darussalam dengan menerapkan *Digital Forensics*. Jurnal ini diharapkan dapat menjadi rujukan pembelajaran Indonesia dalam meningkatkan kualitas *cybersecurity* di Indonesia, serta menjadi acuan untuk menyusun *code of conduct* dalam mengatasi maraknya kejadian *cybercrime* di Indonesia.

Tantangan dan Isu *Cyber Security* Brunei Darussalam

Cyber security Brunei Darussalam ditangani oleh sebuah himpunan yang terdiri dari beberapa lembaga seperti *IT Protective Security Service Sdn Bhd (ITPSS)* yang didirikan pada tahun 2003 dengan tujuan untuk menyediakan acuan untuk menyelamatkan informasi, *Digital Forensics, Secure Event Management, IT Security Training,* dan *Incident Response Team* yang didirikan pada tahun 2004 dengan nama *Brunei Computer Emergency Response Team (BruCERT).* Di bawah ini merupakan persentase serangan *cyber* yang telah dialami oleh Brunei Darussalam dalam kurun waktu 2011 hingga 2015.

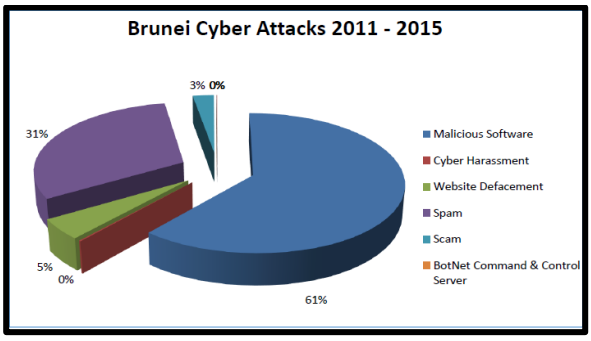

Figure 1: Serangan Cyber di Brunei

Source: BruCERT

Dalam kurun waktu lima tahun tersebut persentase kasus *cybercrime* di Brunei Darussalam terus menerus meningkat. Terlebih lagi setelah dikeluarkannya perundangan yang telah

dibuat oleh pemerintah Brunei Darussalam guna melindungi para korban dari *cybercrime.* Berikut ini merupakan rekapan dari kasus *cybercrime* yang terdeteksi dan telah dijatuhi hukuman yang terhimpun dalam koran lokal Brunei:

Table 1: Rekap kejadian cybercrime yang terdeteksi dan telah dijatuhi hukuman

Cybercrime	Tahun	Masa Hukuman	Kejadian
***Hacking* dan pencurian data**	2010	28 Bulan Penjara	*Wireless Access Point* yang tidak terkunci menyebabkan pelaku kriminal berhasil memperoleh nomor kartu kredit dan menggunakannya untuk membayar pembelian *online* sebesar $ 2720.00
Cyber bullying	2012	10 Bulan Penjara	Mantan kekasih mengunggah gambar dan video rahasia dengan kekasih lamanya dengan tujuan untuk mempermalukan.
Ancaman Teroris	2015	Dalam Pembahasan	Pelaku mengemukakan keinginannya untuk bergabung dengan organisasi teroris melalui *social media.*

Source: BruneiTimes

Selain *cybercrime* yang sudah tercatat, masih banyak ancaman-ancaman *cyber* lainnya di Brunei Darussalam, hingga pada tanggal 5 Februari 2015, *Royal Brunei Technical Service (RBTS)* mengadakan sebuah forum guna memberikan pemahaman kepada masyarakat Brunei terutama korporasi mengenai ancaman *cyber* agar tercipta kesadaran korporasi tersebut terhadap *cyber security* dan memastikan organisasi korporasi tersebut telah dibekali pengetahuan dasar tentang *cyber security.* Forum yang bertema *Combating Cyber Security Threats* membahas mengenai berbagai masalah ketergantungan dalam ranah *cyber* yang dapat menjanjikan berbagai peluang baik, sekaligus menjadi ancaman yang sangat berbahaya. Forum yang diadakan oleh RBTS tersebut juga mencatat bahwa ancaman di dunia *cyber* di Brunei Darussalam terus meningkat setiap tahunnya seiring dengan terus meningkatnya perkembangan penggunaan teknologi informasi. [9]

Ancaman Kejahatan

Kejahatan *cyber* yang paling berbahaya adalah kejahatan dengan menyamar sebagai orang lain dengan menggunakan IP *address* dan tanpa disadari telah melakukan berbagai kerusakan. Untuk melacak jenis pelaku kejahatan seperti ini tidaklah mudah dan sangat menantang. *The Industrial*

[9] RBTS (2015). Combating Cyber Security Threats, *Cyber Security Forum Brunei*

Control Systems Cyber Emergency Response Team (ICS-CERT) mengategorikan pelaku kejahatan *cyber* kedalam tiga kategori kelompok. Pada intinya ancaman yang diberikan dari tiga kelompok tersebut hampir serupa, namun apa yang membedakan dari ketiga kelompok ini adalah niat dan sumber yang mereka peroleh. Grup pelaku kejahatan yang pertama (1) merupakan grup umum, dimana mereka merupakan individu atau kelompok yang memiliki pengetahuan teknis mengenai *cyber*, dan melakukan kejahatan hanya demi memperoleh ketenaran *(notoriety).* Grup pelaku kejahatan yang kedua (2) merupakan grup sindikat, dimana mereka adalah pelaku kejahatan yang bekerja secara berkelompok, seperti *hacker, hacktivist,* dan orang dalam yang membuka *backdoor* untuk memberikan akses kepada pelaku serangan *cyber*. Dan grup pelaku kejahatan yang ketiga (3) merupakan grup pelaku kejahatan berat, mereka tergolong kedalam jenis teroris dan para pengancam keamanan negara melalui perang *cyber*.[10]

Keabsahan Data/Informasi (Hoax)

Tantangan dan isu bagi keabsahan data bukanlah sesuatu yang baru, namun tetap saja menjadi permasalahan yang tidak dapat dibiarkan. Semakin cepat teknologi informasi, semakin mudah dan cepat informasi dibagikan di dunia *cyber*. Sebagai contoh, penggunaan mesin pencari *Google* yang paling sering diakses oleh para pengguna internet, memiliki banyak sekali risiko dikarenakan begitu banyaknya informasi yang terdapat di dalam mesin pencari tersebut. Oleh karena itu diperlukan beberapa hal yang perlu diantisipasi, diantaranya:

1. Memastikan Informasi yang diperlukan adalah valid dan akurat.
2. Memastikan informasi yang dibaca itu tidak menyesatkan dan membelokkan pengguna untuk mempercayainya, seperti menyesatkan agama, kepercayaan, dan ras.
3. Kesalahan dalam menelusuri *link* atau *website* yang terbuka di *search result Google.*

Selain *Google,* berbagai *media digital* lain seperti *email, WhatsApp, Facebook* juga termasuk dalam tantangan ini. Sekarang *Facebook* atau *WhatsApp* dapat diistilahkan sebagai informasi yang tidak stabil.

[10] Edward. F. (2015). Cyber Security Challenges: Protecting your transportation management center. *ITE Journal.*

Informasi apa saja yang actual seperti kecelakaan, informasi mengenai acara hiburan, dan keramaian akan dapat dengan mudah dan cepat disebarkan di *media digital* untuk dinikmati oleh pengguna *media* tersebut. Tanggapan dari masing-masing penggunapun akan beragam, ada yang akan menekan *"like"* di *Facebook* untuk berita tersebut dan tidak sedikit yang akan menyebarkan informasi-informasi ini. Apabila informasi tersebut merupakan informasi yang baik maka tidak akan ada masalah yang terjadi dari penyebaran informasi tersebut, namun apabila informasi yang disebarkan merupakan informasi tidak baik, seperti foto kecelakaan di jalan raya yang tidak sepatutnya disebarkan tanpa sensor terlebih dahulu, maka seharusnya informasi tersebut disaring terlebih dahulu sebelum disebarkan.

Salah satu ancaman lain bagi *cyber security* adalah ancaman dari *"Trolling". Trolling* merupakan istilah ancaman *cyber security* dimana pelaku dari *trolling* akan menyebarkan *statement* atau pernyataan yang dapat membangkitkan respon negative. Respon-respon negative tersebut pada akhirnya dapat membangkitkan keamanan dan dapat mengganggu kestabilan organisasi maupun kestabilan sebuah negara, seperti halnya yang terjadi di negara-negara Arab yang lebih dikenal dengan istilah *"Arab Spring".*[11] Stabilitas sebuah negara dapat terganggu hanya karena sebuah pergerakan politik dan pemberontakan sipil yang diakibatkan oleh sebuah propaganda jahat yang disebarkan melalui *digital media*.[12] Semua *trolling* yang dilakukan pada umumnya bermaksud untuk membelokkan persepsi, menyesatkan, dan mempengaruhi kemampuan berfikir pengguna dalam menyikapi suatu hal. Tempat-tempat operasi yang disasar oleh para pelaku *trolling* ini seringkali disebut sebagai *"Cognitive Hacking"*[13], *"Cognitive Malware"*[14], atau *"Social Cyber Attacks"*[15]

[11] Howard, PN, Duffy, A., Freelon, D., Hussain, M., Mari, W. & Mazaid, M. (2011). What was the role of Social Media During the Arab Spring? Opening Closed Regimes. *Project on Information Technology & Political Islam (PITPI).*

[12] Knott, B. (2014). Cyber Trust and Influence. *Proceedings of the Human Factors and Ergonoics Society annual Meeting,* 58 (1), 415-418. DOI: 10.1177 / 1541931214581985

[13] Cybenko. G., Giani, A., & Thompson, P. (2002). Cognitive Hacking: A Battle for the Mind. *Computer,* 35 (8), 50-56

[14] Finomore, V., Sitz, A .., Blair, E., Rahlil, K., Champion, M., Funke, G., Mancuso, V. & Knott, B. (2013). Effects of Cyber disruption in a Distributed Team Decision Making Task, *Proceedings of the Human Factors and ergonomics Society Annual Meeting,* 57, 394-398.

Tantangan-tantangan yang telah disebutkan di atas sangat dapat menimbulkan isu keamanan dimana penyalahgunaan *digital media* bisa mengundang bahaya terlebih lagi jika bertepatan dengan *websites* yang menjadi umpan para pelaku kejahatan. Tujuan dari beberapa kasus kejahatan di *digital media* adalah ingin menjadikan para pengguna internet sebagai korban dari pornografi, prostitusi, seks bebas, penculikan, dan perdagangan manusia. Atau yang lebih membahayakan adalah mempengaruhi dan menyesatkan para pengguna internet dengan berbagai macam tautan yang berisi propaganda untuk merusak suatu organisasi ataupun negara. Ini telah terbukti dengan munculnya berbagai grup-grup militant yang melakukan perekrutan anggota melalui *Facebook* dan *Twitter*, serta berkomunikasi dengan menggunakan enkripsi guna merencanakan dan melaksanakan serangan, hal tersebut secara singkat dapat disebut sebagai "*Cyber Terrorism*" yang secara langsung telah mengganggu kedaulatan suatu bangsa dan negara.

Invasi Sistem Keamanan

Invasi terhadap sistem keamanan juga menjadi salah satu tantangan *cyber security* dari negara Brunei Darussalam dimana hal tersebut dapat menjurus ke berbagai jenis *cybercrime.* Invasi terhadap sistem keamanan dapat terjadi melalui tiga tahap yaitu, manusia, sistem proses, dan teknologi seperti kelalaian pengguna yang tidak memperbarui kata sandi yang sangat disarankan guna mengurangi risiko invasi terhadap sistem keamanan atau kurangnya control terhadap keamanan perangkat serta media ICT. Pejabat senior operasi BruCERT melaporkan bahwa jenis kejahatan yang paling banyak teridentifikasi sejak tahun 2011 adalah *spams* dan *website defacement* dimana pada tahun 2011 saja, sebanyak 160 buah *websites* mengalami *defacement* karena kurangnya pengawasan dan kelalaian karena tidak menggunakan *security patch*. Pada tahun 2012 dan 2013, jumlah *websites defacement* meningkat dikarenakan penggunaan *3rd party website* yang tidak memiliki *security control*. Kejahatan tersebut telah menyebabkan berbagai kesulitan pengaksesan informasi dan menghalangi kinerja harian. Pada tahun

[15] Goolsby, R. (2013). On Cybersecurity, Crowdsourcing, and Social Cyber Attack. *commons Lab Policy Memo Series,* 1-9.

2014, serangan *DoS (Denial of Service)* tercatat telah terjadi pada lembaga keuangan dimana para peretas *(hacker)* telah mengancam dan melepaskan serangan guna memutus jaringan dari lembaga keuangan tersebut.

Tantangan *cyber security* Brunei Darussalam yang terakhir adalah tantangan melalui metode *IOT (Internet of Things)*[16]. Metode IOT dapat memungkinkan organisasi atau individu dapat mengontrol perangkat yang terhubung *"Connected Device"* hanya dengan menggunakan jari. FBI dalam *public service announcement* telah memperingatkan bahwa segala bentuk *connected devices* dapat menimbulkan risiko ancaman baru dikarenakan hal tersebut dapat membuka celah bagi para pelaku *cybercrime* untuk melakukan serangan. Segala perangkat tersebut mulai dari hal yang paling sederhana seperti lampu hingga *network connected printer*.[17][18]

Berbagai tantangan dan isu ancaman *Cyber Security* sangat memerlukan penanganan serius dari pihak pemerintah Brunei Darussalam, dibawah ITPSS dan BruCERT, pemerintah Brunei Darussalam telah menggunakan langkah antisipasi untuk menghadapi berbagai ancaman *cyber security* dari seluruh tantangan tersebut. Salah satunya adalah dengan menerapkan *Digital Forensics* sebagai suatu instrument untuk menginvestigasi segala macam ancaman *cyber security* di Brunei Darussalam.

Digital Forensics ITPSS Brunei Darussalam

Peningkatan jumlah pengguna *media digital* dalam kurun waktu dua decade terakhir telah merubah cakupan dari ranah kejahatan tradisional, sekaligus telah membentuk sebuah jenis ranah kejahatan tambahan. *Media digital* semakin sering digunakan sebagai alat untuk melakukan kejahatan atau sebagai alat bantuan untuk melakukan sebuah kejahatan dalam dunia *cyber*. Sedangkan bukti dari kejadian yang terjadi di dalam dunia *cyber* tersebut sangat sulit dilihat secara fisik dan terkadang sulit diakses oleh para penegak hukum, karena segala kejahatan terjadi di dalam dunia yang kasat mata sehingga sangat menyulitkan untuk penanganannya,

[16] Drubin. C. (2016). Booming Opportunities in IOT Cybersecurity. *Microwave Journal,* 59 (6), 52

[17] Hammond, B. (2015). FBI Issues Cybersecurity Alert for IOT Devices. *Cybersecurity Policy Report.*

[18] Higginbotham, S. (2015). The FBI warns citizens to beware of cybercrime and the Internet of things. *Fortune.*

sehingga ini amat sangat perlu diantisipasi agar tidak terus berkembang.

Bukti kejahatan dengan menggunakan *digital media* atau yang lebih sering disebut sebagai *digital evidence* hanya dapat di temukan dalam perangkat yang dilakukan oleh para pelaku kriminal seperti dalam perangkat *hard disk* atau *removable media, email,* atau *log file* yang menunjukkan akses terhadap suatu aktivitas tertentu yang dianggap mencurigakan.[19] *Digital evidence* terdiri dari semua perangkat *digital* dan bukti fisik terkait lainnya yang mungkin ada. *Digital device* mungkin mengandung banyak jejak digital yang dapat diproduksi menjadi sebuah *digital evidence* yang akan digunakan dalam pengadilan. Kualitas dari *digital evidence* ditunjang dari proses investigasi *digital forensics* yang kritis dan kredibel, sehingga dapat dipertanggung jawabkan di pengadilan.

Proses Investigasi *Digital Forensics*

Proses investigasi dari *digital forensics* dapat terbagi menjadi beberapa tingkatan yang terdiri dari empat (4) buah tingkatan kunci yaitu: *Preservation, Collection, Examination,* dan *Analysis*.[20][21]

a. *Preservation*

   Tahap *preservation* merupakan tahapan investigasi yang pertama kali dilakukan dimana penegak hukum membekukan semua aktivitas pada perangkat yang diduga sebagai tempat kejadian perkara. Pembekuan tersebut termasuk dengan menghentikan atau mengantisipasi segala kegiatan yang sekiranya dapat merusak *digital information* yang telah dikumpulkan. *Preservation* juga melakukan tindakan lain seperti mengantisipasi orang lain untuk menggunakan *computer* selama proses investigasi berlangsung, menghentikan segala proses penghapusan data, dan memilih jalan tercepat untuk mengumpulkan data.

b. *Collection*

   Tahap *collection* merupakan tahapan pencarian dan pengumpulan informasi digital yang terkait dan mungkin relevan dengan proses investigasi. Sejak informasi digital di dalam perangkat

[19] Hewling (2010), Digital Forensics: The UK Legal Framework, Published Masters dissertation, University of Liverpool, Liverpool UK.

[20] A roadmap for digital forensic research. Tech. rep., Digital Forensic Research Workshop, 2001.

[21] Reith, M., Carr, C., and Gunsch, G. An examination of digital forensic models. International Journal of Digital Evidence 1, 3 (2002).

digital, pengumpulan informasi digital berarti menyita berbagai perangkat yang diduga berisi informasi digital, atau memindahkan informasi kepada sebuah media tertentu. Proses pengumpulan dapat termasuk penyitaan computer dari tempat kejadian perkara, mengopi atau mencetak konten yang ada di dalam server, rekaman dari *network traffic,* dan lain sebagainya.

c. *Examination*

Tahap *examination* merupakan tahapan untuk menelaah secara lebih dalam guna mencari *digital evidence* yang terkait dengan kejadian yang sedang diinvestigasi. Hasil dari *examination* adalah data mengenai berbagai objek yang ditemukan dan juga informasi yang telah dikoleksi. Informasi yang dikoleksi tersebut mencakup *log file,* file data yang berisi kalimat-kalimat spesifik, *timestamps,* dan lain sebagainya.

d. *Analysis*

Tahapan penting terakhir adalah tahap *analysis* dimana dalam tahap ini proses investigasi akan berujung kepada penarikan kesimpulan berdasarkan segala jenis temuan yang berhasil dikumpulkan di lapangan.

ITPSS Brunei Darussalam

IT Protective Security Service Sdn Bhd (ITPSS) merupakan sebuah lembaga swasta yang diberikan kewenangan penuh oleh pemerintah Brunei Darussalam untuk melaksanakan pengawasan terhadap keamanan di dalam dunia *cyber*, *ITPSS* didirikan pada tahun 2003 sebagai pionir dan solusi untuk mengatasi permasalahan keamanan di bidang *cyber,* yang memberikan bantuan berupa berbagai informasi mengenai segala hal yang menyangkut *cyber security* dan *physical security service* mulai dari *penetration testing* dimana pihak ITPSS akan mengetes sistem keamanan jaringan suatu tempat untuk kemudian diberikan saran serta bantuan untuk meningkatkan keamanan sistem jaringan tersebut, *digital forensics* dimana pihak ITPSS menginvestigasi sebuah bukti dari perangkat yang diduga digunakan sebagai alat untuk melakukan *cybercrime, secure event management* dimana pihak ITPSS memberikan pelayanan jasa guna mengatur keamanan dalam sebuah event, dan yang terakhir adalah *IT security training* dimana pihak ITPSS memberikan pelayanan untuk melatih para

pengaman *cyber* agar dapat bekerja secara mandiri.

Para pengguna jasa dari ITPSS sangatlah beragam mulai dari perusahaan-perusahaan swasta hingga agensi-agensi pemerintahan terbesar yang ada di Brunei Darussalam. Para tim ahli yang dimiliki oleh ITPSS secara konsisten selalu disertifikasi secara berkala dengan menggunakan standar kualifikasi international dan telah memiliki pengalaman dengan berbagai jenis program keamanan di Brunei.

Salah satu kebanggaan ITPSS adalah kecakapan lembaga ini dalam merespon kejadian di dunia *cyber* melalui *Brunei Computer Emergency Response Team (BruCERT)* sebagai salah satu pokok utama pelayanannya. *BruCERT* didirikan pada tahun 2004, sebagai agensi pemerintahan yang dipercaya untuk mengatasi segala jenis ancaman *online* dan *computer security* di Brunei Darussalam.

Meningkatkan *Cyber Security* Brunei Darussalam dengan menerapkan *Digital Forensics*.

Brunei Darussalam merupakan sebuah negara kecil, namun penegakan hukum *cybercrime* sangat terstruktur di negara ini. Meskipun belum terlalu lama didirikan dan jumlah kasus *cybercrime* yang masih tergolong sedikit, pemerintah sangat menjadikan ini sebagai *concern* untuk mengatasi segala permasalahan tersebut. Dalam penanganan kasus *cybercrime* pemerintah menjadikan *Royal Brunei Police Force* sebagai ujung tombak, bekerja sama dengan pengacara public sebagai penunjang dari sisi legal. Mengikuti tren global dimana tiap negara mulai memperkenalkan dan memproduksi hukum *cyber* nya tersendiri yang biasa disebut sebagai *Computer Misuse Act.*[22] Hukum *cyber* tersebut akan menjadi pilar utama untuk menghadapi *cybercrime*.

Terdapat tujuh buah focus utama yang diatur dalam kebijakan hukum *cyber* ini, diantaranya adalah:

1. Akses kepada materi computer tanpa memiliki wewenang.
2. Mengakses jaringan dengan maksud dan tujuan untuk memfasilitasi serangan *cyber.*
3. Memodifikasi perangkat computer tanpa memiliki wewenang.
4. Menghalangi atau memakai layanan computer tanpa memiliki wewenang.

[22] Legislation, Attorney General Chambers, Brunei Darussalam.

5. Mengganggu kelancaran penggunaan computer tanpa wewenang.
6. Membongkar kode akses tanpa memiliki wewenang.
7. Meningkatkan hukuman untuk segala kegiatan yang berhubungan dengan computer yang terlindungi.

Namun dalam sudut pandang investigasi, Brunei Darussalam masih tergolong baru dalam hal ini, sebelumnya para penegak hukum di Brunei Darussalam masih memiliki sedikit sekali pengetahuan mengenai cara melakukan investigasi, sehingga pemerintah brunei hanya dapat mencontoh standar operasional prosedur investigasi yang telah dilakukan oleh investigator negara lain. Karena agar proses *digital forensics* dapat mencapai tujuannya untuk meningkatkan *cyber security*, maka diperlukan metode yang tepat agar investigasi yang dilakukan berintegritas. Sebelumnya pemerintah Brunei Darussalam menggunakan metode investigasi dengan berdasarkan *4-phase* model:

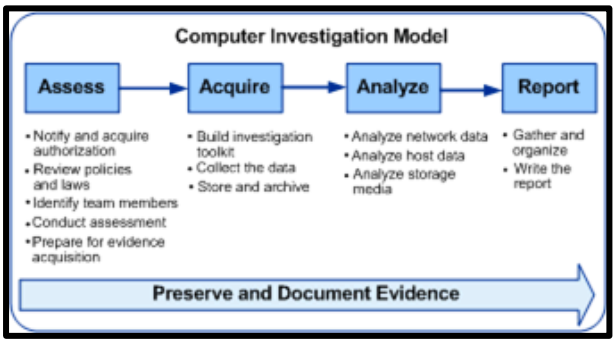

Figure 2 Brunei Last Computer Investigation Model

Sumber: ITPSS

Model investigasi *4-phase* tersebut merupakan model investigasi yang telah banyak dilakukan oleh *computer forensic field,* sebagai acuan dasar dalam menjalankan *digital forensic investigation.* Berikut merupakan acuan yang sebelumnya digunakan oleh pemerintah Brunei Darussalam untuk meningkatkan *Cyber Security*

1. *Assess*

- Penegak hukum Brunei membutuhkan surat penugasan, termasuk surat izin untuk melakukan pencarian dan investigasi. Meskipun hukum Brunei telah mengatakan bahwa penegak hukum memiliki kelebihan untuk melakukan hal tersebut tanpa memiliki izin, namun pihak yang berwenang tetap merekomendasikan agar para penegak hukum memiliki izin terlebih dahulu,

untuk menghindari kecurigaan dan kesalahpahaman prosedur.[23]

- Penegak hukum menyusun tim yang resmi untuk melakukan investigasi. Meskipun polisi Brunei merupakan penegak hukum dalam kasus *cyber crime* namun tetap direkomendasikan dan sangat penting untuk menyusun petugas investigasi yang memiliki pemahaman lebih dalam menangani *computer evidence*. Karena apabila tidak ditangani secara lebih serius, maka ditakutkan bukti dapat rusak, dan proses investigasi akan gagal.
- Hal ini juga penting mengikuti kebijakan dari lembaga dalam melakukan pemeriksaan di tempat dan mempertahankan kebijakan. Polisi Brunei sebagai penegak hukum harus bekerja sama dengan lembaga-lembaga yang terlibat dalam kasus ini. Privasi juga merupakan hal yang sangat penting untuk dipertahankan, dan polisi dapat melanggar salah satu kebijakan lembaga tanpa pengakuan dan otorisasi.
- Siapkan toolkit yang tepat sesuai dengan jenis kejahatan sebelum memulai investigasi. Hal ini juga penting untuk menelusuri tempat kejadian perkara dengan lebih efisien.
- Mendokumentasikan penyelidikan penting, termasuk langkah-langkah yang diambil, untuk menjaga integritas proses penyelidikan. Dokumen ini penting dan harus diperiksa oleh petugas hukum.

2. *Acquire*

- Toolkit disiapkan dari tahap pertama dengan benar sebelum mengambilnya bukti. Dikarenakan harus efisien dan memadai dalam memperoleh data yang diperlukan.
- Dalam pengumpulan data, penegak harus mengambil tindakan pencegahan yang ekstrem, jika penegak hukum sedang melakukan *digital forensic* secara langsung, penting bagi penegak hukum untuk memperoleh data *volatile* dari sistem sebelum menyita *hardware*, karena data ini akan menjadi hilang setelah sistem telah di *shutdown*.
- Dokumentasi harus dilakukan, seperti dalam kelanjutan dari tahap sebelumnya.

3. *Analyze*

- Hal ini penting dilakukan bagi para penegak hukum untuk tidak melakukan analisis secara langsung pada bukti asli

[23] Legislation, Attorney General Chambers, Brunei Darussalam.

(perlu disimpan di lokasi yang aman) karena bisa mengubah keaslian bukti. Analisis hanya boleh dilakukan pada file duplikasi.

- Sekali lagi, penting untuk penyidik untuk menggunakan alat yang tepat dalam menganalisis, dan ini juga perlu dipersiapkan dengan baik dari tahap pertama.
- Analisis harus dilakukan secara menyeluruh, untuk memperoleh informasi penting yang berkaitan dengan kasus tersebut.
- Semua langkah-langkah yang diambil dalam tahap ini juga harus dimasukkan kedalam dokumentasi, untuk merekam dan menjadi bukti. Penulis juga akan merekomendasikan untuk penyidik untuk memasukkan rekaman visual dari proses analisis untuk menghindari keraguan.
- Analisis bukti harus dilakukan di laboratorium yang terpisah, khusus dibuat untuk penyelidikan *digital forensics* untuk menghindari konflik dan bukti yang rusak.

4. *Report*

- Laporan hasil investigasi final harus dipersiapkan, termasuk catatan semua langkah yang diambil oleh penegak tersebut, alat yang digunakan, anggota tim dan bahan terkait lainnya. Hal ini juga penting untuk memperbarui dan menyelesaikan alur investigasi.
- Dokumentasi juga akan mencakup rekonstruksi kasus, seperti pada bagaimana penegak yang melihatnya, untuk memberikan pemahaman yang lebih baik kepada pihak hukum.

Meskipun model investigasi *4-phase* tersebut sudah cukup baik untuk digunakan dalam proses *digital forensic* ketika menangani permasalahan *cybercrime*, namun pemerintah Brunei Darussalam menyimpulkan bahwa model tersebut sangat menyulitkan para penegak hukum, dikarenakan terjadinya simpang siur posisi antara penegak hukum dengan para staf ahli yang mahir dalam bidang *digital forensic*, selain itu pemerintah Brunei juga mengetahui bahwa ancaman *cybercrime* akan selalu berkembang, sehingga penanganan di Brunei Darussalam-pun juga masih sangat diperlukan pengembangan, untuk mengembangkan ilmu dan memberikan acuan lebih mendasar dalam melaksanakan *digital forensic*, maka pemerintah Brunei Darussalam turut

menunjuk pihak swasta guna mengembangkan konsep *digital forensics* sebagai acuan dasar investigasi untuk meningkatkan *cyber security* di Brunei Darussalam.

Pihak swasta tersebut adalah ITPSS, dimana dalam pelaksanaan *digital forensic* ITPSS memiliki sebuah divisi khusus guna menangani *Digital Forensic*, divisi *digital forensic* ITPSS yang bertujuan untuk menjadi salah satu agensi yang dapat menjadi panutan bagi para penegak hukum di Brunei Darussalam dalam melaksanakan *digital forensic,* berbagai langkah yang dilakukan oleh divisi *digital forensic* ini adalah dengan memfasilitasi para agensi penegak hukum dan juga membantu pekerjaan penegak hukum dalam memerangi *cybercrime* di Brunei Darussalam. Divisi ini juga turut memberikan berbagai pembekalan kepada penegak hukum dan non-penegak hukum mengenai berbagai macam kapabilitas dalam melakukan investigasi baik melalui pemberian materi ilmu, kerja sama, maupun pelatihan. Sejak didirikan, divisi ini langsung ditunjuk oleh pemerintah Brunei Darussalam untuk menjadi salah satu ujung tombak dalam pelaksanaan *digital forensics* sekaligus menjadi representasi dari Brunei Darussalam saat melaksanakan kerjasama di dunia Internasional.

Langkah-langkah keamanan yang saat ini telah dan terus dilaksanakan adalah dengan menyusun beberapa sub divisi dan pelayanan guna menunjang kebutuhan akan *cybersecurity*, seperti *Digital Forensics, Data Recovery, Media Sanitization,* dan *Expert Witness Testimony*.

1. *Digital Forensics*
   - Komputer, Jaringan, Database, Email *Forensics*
   - *Mobile Forensics*
   - *Malware Analysis*
2. *Data Recovery*
   - *Hard Drive,* RAID, SSD, Pemulihan Data Server.
3. *Media Sanitization*
   - Mengganti dan menghapus segala data media dengan menggunakan *software Mobile Forensics*
   - *Degaussing,* atau menghapus data magnet dari perangkat magnet
   - *Destruction,* menggunakan pendekatan secara fisik untuk menghancurkan dan membinasakan data yang merugikan.
4. *Expert Witness Testimony*

- Divisi *Digital Forensics* juga memberikan pelayanan berupa kesediaan untuk menjadi saksi ahli di persidangan, dengan memberikan para ahli di bidang analysis guna memberikan kesaksian teknis terhadap sebuah kasus yang sedang dipersidangkan.

Dalam melaksanakan *digital forensics* divisi ini menggunakan proses *digital forensics* dasar yang telah dilakukan oleh pemerintah Brunei Darussalam sebelumnya, hanya saja kali ini proses yang dilaksanakan telah disempurnakan, dimana dalam melaksanakan *digital forensics* divisi ini kini memakai lima tahapan mulai dari *identification, preservation, collection/acquisition, examination* & *analysis,* hingga tahap terakhir yaitu *reporting and presentation.* Tahapan tambahan dalam proses ini adalah *identification,* dimana sebelumnya pemerintah Brunei Darussalam hanya menunggu laporan dari para pengguna *cyber,* namun sekarang pemerintah turut berperan aktif dalam mengantisipasi terjadinya *cybercrime* secara cepat dan tepat sasaran.

Kesimpulan

Berdasarkan penjabaran di atas, dapat disimpulkan bahwa maraknya kejadian *cybercrime* yang terjadi, telah memicu pemerintah untuk terus meningkatkan keamanan di dalam dunia *cyber*, salah satu cara yang dapat digunakan oleh pemerintah untuk mengatasi permasalahan tersebut adalah dengan cara melakukan proses secepatnya pada saat kejadian *cybercrime* terjadi sehingga hasil dari proses dapat dianalisis dan dijadikan sebagai pedoman untuk mengantisipasi terjadinya *cybercrime* serupa di kemudian hari, oleh karena itu *digital forensics* sangatlah penting untuk terus dikembangkan, karena sangat berguna bagi para penegak hukum agar dapat segera mengatasi segala bentuk *cybercrime* yang terjadi.

Pemerintah Brunei Darussalam sebagai penentu kebijakan dalam peningkatan *cyber security* di Brunei telah melakukan langkah antisipasi terbaik dengan mengeluarkan kebijakan *Computer Misuse Act* yang sangat membantu para penegak hukum dalam menentukan langkah apa yang harus diambil dalam menghadapi *cybercrime*, selain itu

pemerintah Brunei Darussalam juga sangat memahami bahwa kemampuan yang dimiliki oleh pemerintah saat ini tidak akan mampu menghadapi terpaan dari *cybercrime* yang terus berkembang setiap harinya, oleh karena itu pemerintah Brunei memutuskan untuk bekerja sama dengan pihak swasta guna membantu pemerintah dalam mengembangkan *cybersecurity* dan memproduksi acuan dalam melakukan *digital forensics* agar segala kejadian *cybercrime* dapat segera diselesaikan.

Kesigapan pemerintah Brunei Darussalam dalam menghadapi *cyber threats* sangat berbanding terbalik dengan pemerintah Indonesia yang tergolong masih belum terlalu serius dalam menangani permasalahan ini, dapat dilihat perbandingan yang cukup signifikan dimana pemerintah Brunei Darussalam mengupayakan segala cara agar negara tersebut mampu menghadapi ancaman dari *cyber*, bahkan tidak segan untuk mengajak seluruh pihak untuk membantu pemerintah. Sedangkan di Indonesia, pemerintah belum terlalu serius menyikapi hal ini, dapat dilihat dari kesimpang siurannya aturan dan lembaga yang mengatasi permasalahan ini, bahkan *code of conduct* dalam penanganan masalah *cyber* pun masih belum jelas dan tidak terstruktur secara rapi, sehingga sangat membingungkan masyarakat Indonesia apabila ingin melaporkan suatu kejadian *cybercrime*.

Masih banyak sekali tumpeng tindih wewenang dan ego sectoral di dalam pemerintah Indonesia, masing-masing pihak terkesan berlomba-lomba untuk membuat kebijakan mengenai *cyber* dibawah wilayah kewenangannya. Pemerintah Indonesia seharusnya mengoptimalkan *Badan Cyber Nasional* karena dengan adanya lembaga tersebut, pemerintah dapat secara penuh mengontrol segala kebijakan mengenai *cyber* dibawah kewenangannya. Namun yang sangat disayangkan pemerintah terkesan lambat dengan terus menerus mengulur waktu peluncuran *Badan Cyber Nasional* ini sehingga langkah Indonesia dalam mengatasi ancaman *cyber* menjadi tertinggal.[24]

Digital Forensics merupakan kunci utama dalam penanganan kasus *cybercrime* yang ada di tiap negara, semakin maju dan

[24]http://semarang.bisnis.com/read/20160815/16/88875/pembentukan-badan-cyber-nasional-diprediksi-molor-lagi. Diakses Pada 6 April 2017

cepat proses *digital forensics* dilakukan, maka penanganan *cybercrime* di suatu negara akan semakin cepat juga, selain itu data yang diperoleh dari hasil investigasi *digital forensics* juga dapat segera digunakan sebagai bahan acuan untuk memperbaiki sistem keamanan, sehingga *cyber security* dapat terus ditingkatkan.

Daftar Pustaka

A roadmap for digital forensic research. (2001). Tech. rep., Digital Forensic Research Workshop.

Cybenko. G., Giani, A., & Thompson, P. (2002). Cognitive Hacking: A Battle for the Mind. *Computer,* 35 (8), 50-56

Drubin. C. (2016). Booming Opportunities in IOT Cybersecurity. *Microwave Journal,* 59 (6), 52

Edward. F. (2015). Cyber Security Challenges: Protecting your transportation management center. *ITE Journal.*

Finomore, V., Sitz, A .., Blair, E., Rahlil, K., Champion, M., Funke, G., Mancuso, V. & Knott, B. (2013). *Effects of Cyber disruption in a Distributed Team Decision Making Task*, Proceedings of the Human Factors and ergonomics Society Annual Meeting, 57, 394-398.

Gary L Palmer. (2001). *A Road Map for Digital Forensic Research*. Technical Report DTRT0010-01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS).

Goolsby, R. (2013). *On Cybersecurity, Crowdsourcing, and Social Cyber Attack*. commons Lab Policy Memo Series, 1-9.

H M Wolfe. (2003). *"Web Solutions and Technologies After the Hack"*, presented at *ICE Conference*, 2003

Hammond, B. (2015). FBI Issues Cybersecurity Alert for IOT Devices. *Cybersecurity Policy Report.*

Hewling. (2010). Digital Forensics: The UK Legal Framework, Published Masters dissertation, University of Liverpool, Liverpool UK

Higginbotham, S. (2015). The FBI warns citizens to beware of cybercrime and the Internet of things. *Fortune.*

Howard, PN, Duffy, A., Freelon, D., Hussain, M., Mari, W. & Mazaid, M. (2011). What was the role of Social Media During the Arab Spring? Opening Closed Regimes. *Project on Information Technology & Political Islam (PITPI).*

Pembentukan Badan Cyber Nasional Diprediksi Molor Lagi. (2017). *Online Article:* http://semarang.bisnis.com/read/20160815/16/88875/pembentukan-badan-cyber-nasional-diprediksi-molor-lagi. Diakses Pada 6 April 2017

Knott, B. (2014). Cyber Trust and Influence. *Proceedings of the Human Factors and Ergonoics Society annal Meeting,* 58 (1), 415-418. DOI: 10.1177 / 1541931214581985

Legislation, Attorney General Chambers, Brunei Darussalam

Michael Noblett, Mark.M.Pollitt and Lawrence Presley. (2000). Recovering and Examining Computer Forensic Evidence, Forensic Science Communications, Volume 2, Number 4.

RBTS. (2015). Combating Cyber Security Threats, *Cyber Security Forum Brunei*

Reith, M., Carr, C., and Gunsch, G. (2002). *An examination of digital forensic*

models. International Journal of Digital Evidence 1, 3.

Ryan Harris – DFRWS. (2006). *Conference proceedings, Arriving at an Anti-forensics consensus*

S. S. Basamh, H. A. Qudaih and J. B. Ibrahim. (2014). "An Overview on Cyber Security Awareness in Muslim Countries," *International Journal of Information and Communication Technology Research,* vol. 4, no. 1, pp. 21-24.