BAB II
LANDASAN TEORI

2.1. Tinjauan Umum

Sebelum membahas *digital forensic readiness*, harus dipahami konsep*digital forensic*. Grobler dan Lowrens (2007) menyampaikan bahwa *digitalorensic rediness* sebagai sebuah komponen dalam keamanan sisteminformasi. Selain itu Sommer (2012) dari *Information Assurance AdvisoryCouncil* juga mengemukakan pentingnya pemahaman akan *Cybercrime*danundang-undang tentang *Cybercrime*. Selanjutnya Bates (2011) dari CumbriaPartnership NHS Foundation Trust mengkombinasikanya semua hal tersebutmenjadi sebuah audit*digital forensic readiness*. Untuk detail komponen model *digital forensicreadiness* secara jelas dan spesifik disampaikan olehBarskeetal. (2010) serta Rowlingson (2004).

2.2. Digital Forensik

Digital Forensik merupakan perluasan dari ilmu forensik. Ilmu forensikdidefinisikan sebagai penggunaan ilmu fisika pada hukum untuk mencarikebenaran dari sipil, kriminal, atau masalah lingkungan sosial dengan tujuanagar ketidakadilan tidak menimpa masyarakat (ECCouncil, 2008). Dariilmu forensik inilah lahir berbagai cabang ilmu forensik lainya, sepertiforensika medis, *digitalforensic* / *computer forensic*. *Digitalforensic* adalah rangkaian metode dari teknik dan prosedur untuk mendapatkan barang bukti dari peralatan komputer, berbagai media penyimpanan dan media digital yang dapat dipresentasikan di pengadilan dengan format yang dapat dipahami dan memiliki arti (ECCouncil, 2008).

Digital *Forensic readiness*

*Digital forensic readiness*adalah kemampuan sebuah organisasi untukmemaksimalkan potensi mereka dalam menggunakan barang bukti digital dan meminimalisir biaya investigasi yang dikeluarkan organisasi (Rowlingson, 2004).

Tujuan dari *digital forensic readiness*adalah untuk memaksimalkan penggunaan data sebagai barang bukti ketika terjadi insiden dan meminimalisir biaya investigasi ketika merespon insiden (Tan, 2001). Tujuan dari *digital forensic readiness*menurut Rowlingson (2004) adalah

1. Agar organisasi dapat mendapatkan barang bukti secara legal tanpa mengganggu proses bisnis dari organisasi.
2. Untuk memperoleh barang bukti yang mengarah pada tindak kriminal yang potensial dan perselisihan.
3. Untuk mengijinkan investigasi *computer forensic* untuk melanjutkan proporsi pada insiden.
4. Untuk meminimalisir intrupsi pada bisnis dari berbagai investigasi
5. Untuk menjamin bahwa barang bukti memiliki dampak positif ketika dihasilkan dari berbagai aksi legal.

2.3. Tahapan-tahapan Digital *Forensic readiness*

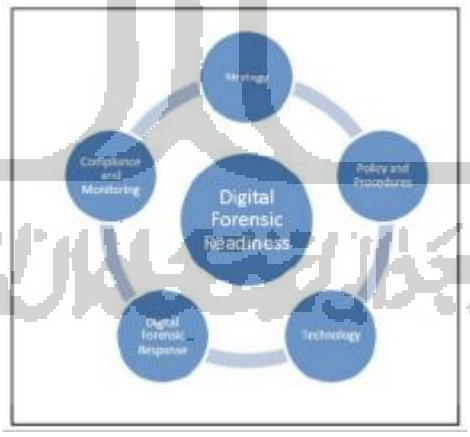
Selanjutnya, untuk mencapai tujuan-tujuan *digital forensic readiness* tersebut, dipelukan tahapan-tahapan. Tahapan-tahapan implementasi *digital forensic readiness*(Rowlingson, 2004) antara lain:

1. Mendefinisikan skenario organisasi yang dapat berpotensi menghasilkan barang bukti digital.
2. Mengidentifikasi sumber-sumber dan perbedaan tipe dari barang bukti yang potensial dalamorganisasi.
3. Menentukan barang bukti yang perlu dikumpulkan.
4. Membuat kecakapan didalam organisasi untuk mengumpulkan barang bukti secara aman dan dapat dijadikan bukti legal yang dibutuhkan organisasi.

5. .Membuat kebijakan-kebijakan untuk mengamankan media penyimpanan dan menangani barang bukti yang potensial.
6. Memastikan bahwa sumber-sumber sistem informasi terawasi untuk mendeteksi insiden.
7. Identifikasi keadaan ketika investigasi normal dilakukan pada saat kejadian.
8. Melatih anggota organisasi dalam kepedulian insiden sehingga semua anggota terlibat memahami tanggungjawab mereka pada proses barang bukti digital dan isu-isu legal yang mengelilingi barang bukti digital.
9. Dokumentasi kasus-kasus berbasis barang bukti yang menggambarkan insiden dan dampaknya pada organisasi.
10. Memastikan telah dilakukan *review* secara legal untuk memfasilitasi berbagai tindakan untuk merespon insiden.

2.4. Model Digital *Forensic readiness*

Dari beberapa telaah, model *digital forensic readiness*secara spesifikdikemukakan oleh Barske et al. Model *digital forensic readiness*menurut Barske et al. memuat lima komponen utama *digital forensic readiness*, yang dapat terlihat pada Gambar 4



Gambar 5 Komponen Digital *Forensic readiness(Sumber: Barske et al., 2010)*

Komponen-komponen tersebut Menurut Barske dkk adalah (Barske et al., 2010):

1. Strategi

Keputusan untuk mengimplentasikan program *digital forensic readiness*harus menjadi keputusan strategis bagi organisasi, dan memastikan bahwa *digitalforensic readiness*merupakan strategi penting yang berhubungan langsung bagi tujuan organisasi.

2. Kebijakan dan prosedur

Setiap organisasi membutuhkan kebijakan-kebijakan dan prosedur sebagai petunjuk bagi angota organisasi berkenaan tindakan dan aktivitas. Untuk memastikan *digital forensic readiness*dalam organisasi, harus disiapkan kebijakan dan prosedur untuk memastikan pelaksanaanya.

3. Teknologi

Organisasi ketika mengimplementasikan *digital forensic readiness* membutuhkan penggunaan software atau hardware sebagai pendukung proses *digital forensic*, seperti memperoleh barang bukti digital dan melakukan pengujian terhadap barang bukti digital tersebut.

4. Respon digital forensic

Digital Forensic Response dibutuhkan untuk menangani dan menindak berbagai isu terkait tindakan *Cybercrime*, investigasi kriminal, perbaikan insiden keamanan komputer dan mendukung setiap proses *digital forensic*.

5. Pelaksanaan dan pengawasan

Program *digital forensic readiness*harus selalu dimonitor dan diawasi, dan mampu menangani resiko ketika terjadi kegagalan program *digital forensic readiness*. Semua dapat tercapai ketika semua anggota organisasi memiliki pengetahuan akan kebijakan-kebijakan dan prosedur yang dilaksanakan sesuai regulasi. Model *digital forensic readiness*yang dibuat Barske dkk tersebut ditujukan bagi institusi usaha kecil menengah (UKM), sehingga masih harus dilakukan penyesuaian untuk kajian agar bisa dan sesuai diterapkan pada instansi.

2.5. *Cybercrime* (Kejahatan Dunia Maya)

Pada tahun 2001 Department of Justice (DOJ) Amerika Serikat mendefinisikan *computer crime* sebagai pelanggaran hukum pidana yang melibatkan pengetahuan teknologi computer untuk perbuatan, penyelidikan, atau

penuntutan (Ghosh et al., 2010). Dengan demikian, kejahatan komputer termasuk dan termasuk sejumlah kejahatan, termasuk *hacker*, menulis virus, pembajakan digital, *cyberstalking*, pembajakan e-*mail*, dan pencurian informasi digital, yang meluas ke pencurian identitas, penipuan bank, penipuan kartu kredit, pencurian rahasia dagang, spionase internasional (Ghosh et al., 2010). Pada Maret 2010, DOJ mengklasifikasikan, kejahatan yang menggunakan atau menjadikan jaringan komputer sebagai target termasuk kategori computer crime, *Cybercrime*, dan *network crime* (Ghosh et al., 2010). Di Indonesia, Pemerintah tidak mendefinisikan, menyebutkan atau menjelaskan tentang *Cybercrime*, *computer crime*, atau *network crime*. Dalam Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, pada Bab VII pasal 27 sampai 37, pemerintah hanya menjelaskan tentang perbuatan yang dilarang (UU ITE, 2008). Menurut Petrus Reinhard Golose, seperti yang dikutip Aldyputra (2012) jenis-jenis *Cybercrime*dapat dijabarkan sebagai berikut.

1. Unauthorized Access to Computer System and Service/Internet Intrusion

Jenis *Cybercrime*ini merupakan jenis kejahatan yang dimana perbuatan melawan hukumnya berupa tindakan memasuki jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik jaringan tersebut. Contoh jenis *Cybercrime*ini adalah mengakses sebuah *website* dengan menggunakan *username* orang lain.

2. Illegal Content

Illegal content merupakan jenis *Cybercrime*yang dimana perbuatan melawan hukumnya berupa tindakan mentrasmisikan data atau menyebarkan informasi tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Contoh dari *Cybercrime*ini adalah pencemarannama baik (*defamation*), penyebaran pornografi, penyebaran rahasia negara, ataupun penyebaran data bajakan (*distribution ofpirated softwar*.

3. Data Forgery

Jenis *Cybercrime*ini merupakan jenis kejahatan yang dimana perbuatan melawan hukum berupa tindakan memalsukan data yang terdapat dalam jaringan

ataupun tindakan memasukan data yang dapat menguntungkan pelaku atau orang lain dengan melawan hukum. Kejahatan ini biasanya berupa pemalsuan dokumen-dokumen *e-commerce* yang digunakan untuk mendapatkan informasi dari si korban atau memasukan data gaji pegawai melebihi seharusnya.

4. Cyber Sabotage and Extortion

Jenis *Cybercrime*ini merupakan jenis kejahatan yang dimana perbuatan melawan hukumnya berupa tindakan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau jaringan komputer yang terhubung dengan internet. Kejahatan ini dilakukan dengan menyusupkan suatu program yang dapat mengakibatkan kerusakan pada data, program komputer atau sistem jaringan komputer yang ditarget.

5. Offense Against Intellectual Property

Jenis *Cybercrime*ini merupakan jenis kejahatan yang dimana perbuatan melawan hukumnya ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain. Misalkan seperti peniruan tampilan dari sebuah *website* secara ilegal, penyebaran data yang merupakan rahasia dagang seseorang, dan sebagainya.

6. Infringements of Privacy

Jenis *Cybercrime*ini merupakan jenis kejahatan yang dimana perbuatan melawan hukumnya berupa tindakan penyalahgunaan atau penyebaran dari informasi pribadi yang dimiliki seseorang yang dimana dapat mengakibatkan kerugian terhadap orang tersebut baik secara materiil maupun immateriil. Misalnya informasi seperti nomor kartu kredit, nomor PIN Anjungan Tunai Mandiri (ATM), cacat atau penyakit tersembunyi, dan sebagainya.

7. Cracking / Hacking

Jenis *Cybercrime*ini merupakan jenis kejahatan yang dimana perbuatan melawan hukumnya berupa tindakan perusakan terhadap sistem keamanan suatu sistem komputer dan biasanya dilakukan dengan maksud untuk melakukan pencurian data atau tindakan anarkis.

8. Carding

Jenis *Cybercrime*ini merupakan jenis kejahatan yang dimana perbuatan melawan hukumnya berupa tindakan menggunakan kartu kredit orang lain tanpa sepengetahuan atau persetujuannya sehingga dapat merugikan orang tersebut baik secara materil maupun non-materiil.

9. Defacing

Jenis *Cybercrime*ini merupakan jenis kejahatan yang dimana perbuatan melawan hukumnya berupa tindakan mengubah halaman situs / *website* pihak lain.

10. Phising/Identity Theft

Jenis *Cybercrime*ini merupakan jenis kejahatan yang dimana perbuatan melawan hukumnya berupa tindakan mencuri informasi mengenai identitas dari pengunjung sebuah situs.

11. Spamming/Harassment Through E-mails

Jenis *Cybercrime*ini merupakan jenis kejahatan yang dimana perbuatan melawan hukum berupa tindakan pengiriman informasi melalui *e-mail* yang dimana informasi tersebut tidak diinginkan oleh penerima.spam sering disebut juga sebagai *bulk e-mail* atau *junk e-mail*.

12. Transmitting Malware

Jenis *Cybercrime*ini merupakan jenis kejahatan yang dimana perbuatan melawan hukum berupa tindakan menyebarkan *malware*. Yang dimaksud dari hal tersebut adalah suatu jenis program komputer yang fungsinya mencari kelemahan dari *software* pada sebuah komputer yang kemudian melalui kelemahan tersebut dilakukan tindakan penyalahgunaan seperti perusakan sistem, *spam*, ataupun pencurian informasi.

13. Cyber-child Pornography

Jenis *Cybercrime*ini merupakan jenis kejahatan yang dimana perbuatan melawan hukum berupa tindakan menyebarkan informasi dengan muatan pornografi anak (*child pornography*).

2.6. Barang Bukti Digital Dalam Perspektif Hukum

Seiring dengan berkembangnya tindak kejahatan, metode, alat dan media yang menggunakan berbagai teknologi informasi dan komputer, maka barang bukti digital/elektronik dapat dijadikan alat bukti yang sah, sebagaimana ditegaskan dalam Undang-undang (UU) Republik Indonesia (RI) No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) pasal 5 angka 1 dan angka 2 (Perpustakaan Nasional Republik Indonesia, 2013) yang berbunyi:

1. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakanalat bukti hukum yang sah.
2. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaksebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

Adapun yang dimaksud dengan informasi elektronik ataupun dokumen elektronik juga ditegaskan pada UU yang sama pada pasal 1 angka 1 dan angka 4 (Perpustakaan Nasional Republik Indonesia, 2013) yang berbunyi:

1. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
2. Dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Untuk memahami UU ITE tersebut dibutuhkan keterangan yang lebih detail dan jelas dari berbagai pakar. Secara sepesifik, Mount dan Denmark menjelaskan berbagai barang bukti digital (Mount, tt) antara lain:

1. Komputer dan komponen-komponen digitalnya.
2. Peralatan audio digital seperti pemutar mp3, Ipod, peralatan pengenalan suara, dan perangkat pengawasan suara.
3. Peralatan video digital seperti kamera digital, peralatan pengawaan video digital.
4. Peralatan kombinasi *audio/video* seperti CD, DVD, disket, dan penyimpanan USB.
5. Peralatan komunikasi seperti telepon selular, blackberry, iPhone, dan lainlain.

Selain itu masih banyak sekali barang bukti digital lainya. Terutama barang bukti yang berasal dari jaringan komputer ataupun internet. Sommer (2012) menyebutkan antara lain:

1. Barang bukti dari *keylogger* (aplikasi pencatat ketikan *keyboard*).
2. Jaringan komputer perusahaan.
3. *Email.*
4. *Personal Digital Assistants* (PDA) / Tablet.
5. Telepon pintar / telepon selular.
6. Peralatan navigasi satelit.
7. Data dan isi telekomunikasi.
8. Alamat IP (*internet protocol*).
9. Data dari penyedia layanan internet.
10. Barang bukti dari *website.*
11. Barang bukti dari *web server.*
12. Peralatan CCTV (*closed-circuit television*).

2.7. Keamanan Aset dan Infrastruktur Teknologi Informasi (TI)

Keamanan jaringan dapat dikatakan optimal jika dapat mengakomodir berbagai aspek (Gregg, 2006), yaitu:

1. Dapat mencegah serangan/ancaman dari luar organisasi

Serangan dari luar ini bisa berupa serangan *hacker*, *cyberterrorism*, serangan virus atau malware, dapat mencegah serangan *denial of services* (DoS) atau*distributed denial of services* (DDoS). Untuk mengantisipasi

ancaman/serangan ini dapat digunakan *firewall* ataupun antivirus. *Firewall* adalah *hardware* atau*software* yang didesain untuk membatasi dan menyaring antara jaringan terpercaya dan jaringan tidak terpercaya. *Firewall* juga digunakan untuk mengontrol trafik dan membatasi aktivitas yang spesifik. Selain itu juga dapat digunakan IDS, yaitu sistem yang tersusun dari sensor-sensor jaringan, sistem*monitoring*, sistem analisa dan laporan, komponen *database* dan *storage*, dan juga kotak respon. IDS merupakan sistem peringatan ketika terjadi serangan terhadap jaringan/sistem.

2. Dapat mencegah serangan/ancaman dari dalam organisasi

Serangan dari dalam bisa berupa pencurian data atau informasi oleh pihak dalam organisasi, atau penyalahgunaan infrastruktur organisasi untuk kepentingan kejahatan. Serangan dari dalam ini adalah serangan yang paling berbahaya. Oleh karena itu, organisasi harus menyediakan mekanisme autentikasi dan pengamanan terhadap aset-aset organisasi, sehingga menjamin sistem dan aset digunakan oleh pihak yang sah dan punya hak.

3. Dapat pulih secepat mungkin jika terjadi serangan/gangguan

Hal lain yang harus diperhatikan oleh ahli keamanan IT adalah *disaster recovery*, yaitu sistem dan organisasi dapat segera pulih jika terkena serangan atau bencana. Seorang *administrator* dapat menyediakan backup sistem dan data, membuat*disaster recovery plan*, dan mengadakan audit Sistem Informasi maupun sumber daya manusia.

4. Dapat merekam setiap aktivitas didalam jaringan

Setiap aktivitas dalam jaringan dan sistem merupakan aset yang penting.Bagi seorang *administrator*, catatan aktivitas merupakan bahan/materi untuk menyempurnakan sistem menjadi lebih baik, karena dalam setiap aktivitas, dapat ditemukan kelemahan dari sistem, maupun catatan serangan dan metodenya. Dalam hal ini dapat digunakan *honeypot*, yaitu *tool* yang memiliki kemampuan merekam setiap aktivitas *hacker*, termasuk aktivitas jaringan, *malware* yang di *upload*, catatan *chat* dengan *hacker* lain, dan semua tipe *command*. Kemampuan ini memungkinkan admin jaringan untuk mempelajari apasaja yang *hacker* lakukan, dan bagaimana *hacker* melakukanya.

5. Dapat menjaga kenyamanan *user*

Untuk menjamin kinerja organisasi berjalan maksimal, sistem harus dapat menciptakan iklim kerja yang nyaman dan mudah, tetapi tetap aman dan terkontrol. Meskipun aspek kenyamanan sangat berbalik dengan kenyamanan, seorang administrator harus dapat menciptakan keseimbangan antara kenyamanan dan keamanan, sehingga pelaku organisasi dapat nyaman dan betah dalam bekerja.