



Jawaban Tugas Akhir Matrikulasi Semester Ganjil 2009/2010

Nama Mahasiswa : **Susanto**
e-Mail : ntbsanto@yahoo.com
Mata Kuliah : **Intro to Cyber Law and Ethics**
(Pengantar Etika dan Hukum Informasi dan Transaksi Elektronik)
Dosen : **Bobby Reza, S.Kom., MM**
e-Mail : bobbyreza@bobbygoblog.com

Jawablah beberapa pertanyaan ini dengan sistematis dan komprehensif.

1. Menurut Saudara, perlukah ada undang-undang yang mengatur pemanfaatan informasi dan transaksi elektronik, mengapa?

Jawab :

Teknologi informasi dan komunikasi telah mengubah perilaku dan pola hidup masyarakat secara global. Perkembangan teknologi informasi telah pula menyebabkan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial, budaya, ekonomi dan pola penegakan hukum yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Kenyataan saat ini hal yang terkait dengan pemanfaatan teknologi informasi tidak lagi dapat dilakukan pendekatan melalui sistem hukum konvensional, mengingat kegiatannya tidak lagi bisa dibatasi oleh teritorial suatu negara, aksesnya dengan mudah dapat dilakukan dari belahan dunia manapun, kerugian dapat terjadi baik pada pelaku internet maupun orang lain yang tidak pernah berhubungan sekalipun misalnya dalam pencurian dana kartu kredit melalui pembelian di internet. Di samping itu masalah pembuktian merupakan faktor yang sangat penting, mengingat data elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia, tetapi dalam kenyataannya data dimaksud juga ternyata sangat rentan untuk diubah, disadap, dipalsukan dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Sehingga dampak yang diakibatkannya pun bisa demikian cepat, bahkan sangat dahsyat. Teknologi informasi telah menjadi instrumen efektif dalam perdagangan global.

Dari paparan singkat di atas, maka diperlukan undang-undang yang mengatur pemanfaatan informasi dan transaksi elektronik.

2. Bahaya apa saja yang berpotensi menimpa komputer Saudara yg terhubung atau tidak terhubung dengan jaringan internet?

Jawab :

Apabila komputer kita terhubung atau tidak terhubung dengan jaringan internet, maka ada 3 (tiga) ancaman yang akan terjadi terhadap komputer kita yaitu :

a. Local attack

Local attack atau *console hacking* adalah usaha rekan kita sendiri untuk mengakses data kita secara tidak sah. Jadi si penyerang dapat mengakses komputer kita secara fisik dan berusaha masuk ke dalam penyimpanan data. Apabila komputer kita tidak diproteksi dengan password, maka data kita dapat dilihat oleh siapa saja. Hal ini dikarenakan, begitu kita terhubung ke Internet melalui ISP (Internet Service Provider) kita, maka kita akan mendapatkan identitas berupa IP address. IP address pada pemakai Internet biasa (*dial up*) biasanya merupakan IP dinamis, yaitu berubah-ubah setiap kali terhubung ke Internet. IP address komputer lokal yang tidak terhubung ke Internet adalah 127.0.0.1, sedangkan apabila terhubung ke Internet akan mendapatkan lagi satu IP address, misalnya 203.125.33.90 (atau lainnya tergantung ISP anda). IP address kita dapat terlihat oleh pihak lain di luar, sehingga dapat menjadi obyek serangan.

Apabila komputer kita merupakan bagian dari LAN (*local area network*), dan koneksi ke Internet secara bersama sama melalui satu komputer (disebut *proxy server*), maka IP address komputer kita ditetapkan secara lokal oleh administrator, biasanya IP address lokal ini formatnya 192.168.x.x atau sejenisnya. IP address ini tidak terlihat oleh pihak luar, sehingga komputer kita terlindung oleh *proxy server* tadi.

b. Bahaya Berinternet

Bahaya sewaktu berinternet sudah dimulai sewaktu kita berselancar dan dapat dibagi atas dua bagian besar, yaitu *Remote Controlled PC* dan *Infeksi Digital :Virus dan Trojan*. Pada awalnya situs web hanya berisi teks dan gambar dan ini merupakan kemajuan pesat sejak adanya Internet. Namun hal ini tidak berlangsung lama, sebab web menjadi lebih dinamis dengan menyertakan komponen-komponen aktif kedalamnya. Komponen-komponen ini selain membuat web lebih menarik, juga menyimpan potensi bahaya dari penyalahgunaannya.

Bahaya terbesar terhadap komputer kita tetaplah virus dan *trojan horse* (atau singkatnya disebut trojan). Dari sifatnya, program-program kecil ini berkembang biak dan menyebar luas pada jaringan komputer dan media-media penyimpanan seperti hard disk, disket, dan CD ROM. Dengan adanya Internet, bahaya yang dibawa oleh program-program ini meningkat ke skala global, mengingat virus dan trojan dapat menyebar ke seluruh dunia hanya dalam waktu beberapa jam saja. Suatu PC yang digunakan untuk *sharing* data, apakah hanya melalui data transfer, jaringan, ataupun Internet, perlu diberikan perlindungan yang memadai terhadap virus dan trojan.

c. Hacker attack

Bahaya lain yang muncul adalah *hacker attack* (serangan hacker). *Hacker* adalah sekumpulan atau beberapa kelompok yang bertujuan untuk mengembangkan ilmu pengetahuan dan *sharing* informasi bebas tanpa batas. *Hacker* adalah seseorang yang tertarik untuk mengetahui secara mendalam mengenai kerja suatu system, komputer, atau jaringan komputer. Mereka terdiri dari para programmer yang ahli jaringan. Mereka jugalah yang berjasa membangun Internet lewat pengembangan sistem operasi *UNIX*. Karakter hacker yang bersifat merusak, yaitu *Dark-side hacker* dan *Malicious hacker*.

3. Sebutkan beberapa kasus kejahatan dunia maya yang pernah terjadi dan menjadi berita di mass media.

Jawab :

Beberapa kasus kejahatan dunia maya di Indonesia yang menjadi berita di mass media :

- a. Kasus Cybercrime yang terungkap di Bandung ada 7 pelaku carding, pembobolan kartu kredit melalui internet. Dengan adanya kejahatan tersebut dapat menurunkan citra dan nama baik bangsa Indonesia, karena pemesanan barang melalui internet E-Bussiness dari berbagai negara dilakukan dengan kartu kredit palsu.
 - b. Jaringan Pemilu di Hack. Jaringan internet di Pusat Tabulasi Nasional Komisi Pemilihan Umum sempat down (terganggu) beberapa kali. Untuk menangani kasus kriminal di dunia maya yang biasa disebut cybercrime, Komisi Pemilihan Umum sudah menggandeng kepolisian. "Cybercrime polisi juga sudah membantu. Domain kerjasamanya antara KPU dengan kepolisian," kata Ketua Tim Teknologi Informasi KPU, Husni Fahmi, di Kantor KPU, Jalan Imam Bonjol, Menteng, Jakarta Pusat, Rabu, 15 April 2009.
 - c. Beli Ipod Rp 12 Miliar, Dikirim Batu. Pelaku kejahatan warga negara Singapura. Korbannya warga Austria. Selasa, 24 Februari 2009 Unit Cyber Crime Markas Besar Polisi Republik Indonesia (Mabes Polri) mengungkap sindikat penipuan penjualan alat pemutar musik buatan Apple, Ipod, senilai US\$ 1 juta atau sekitar Rp 12 miliar. Pelakunya bernama Krisan, 32 tahun, warga Singapura. Sekarang dia sudah ditahan di Mabes Polri.
 - d. Membobol Bank. MEDAN (Berita): Petugas Reserse Ekonomi Sat Reskrim Poltabes MS dibawah pimpinan Kasat Reskrim Kompokol Gidion Arif Setyawan SiK berhasil membongkar kasus kejahatan dengan menggunakan fasilitas dunia maya (Cyber Crime), via media internet, di Bank Mandiri Jalan Cirebon Medan, Rabu, (19/11). Dalam pengungkapan tersebut, selain berhasil menyita barang bukti 1 lembar KTP a/n David William, 2 unit HP jenis Nokia, 1 lembar rekening Koran nomor 106-0005648319 pada Bank Mandiri a/n David William, 1 buah jam tangan, serta 1 unit computer yang digunakan tersangka, petugas Serse Ekonomi Sat Reskrim Poltabes MS juga berhasil meringkus dua tersangka di rumah makan Joko Solo Jalan Stadion Teladan Medan, Senin 17 November 2008.
4. Apa yang dimaksud dengan :
- a. Komputer
 - b. Internet
 - c. Cyber
 - d. Cyberspace
 - e. Multimedia
 - f. Teknologi Informasi
 - g. Informasi Elektronik
 - h. Transaksi Elektronik

Jawab :

- a. **Komputer** adalah alat yang dipakai untuk mengolah data menurut prosedur yang telah dirumuskan. Kata *computer* semula dipergunakan untuk menggambarkan orang yang perkerjaannya melakukan perhitungan aritmatika, dengan atau tanpa alat bantu, tetapi arti kata ini kemudian dipindahkan kepada mesin itu sendiri. Asal mulanya, pengolahan informasi hampir eksklusif berhubungan dengan masalah aritmatika, tetapi komputer modern dipakai untuk banyak tugas yang tidak berhubungan dengan matematika.
- b. **Internet** (kependekan dari *interconnected-networking*) ialah rangkaian komputer yang terhubung di dalam beberapa rangkaian. Manakala Internet (huruf 'I' besar) ialah sistem komputer umum, yang terhubung secara global dan menggunakan TCP/IP sebagai protokol pertukaran paket (*packet switching communication protocol*). Rangkaian internet yang terbesar dinamakan **Internet**. Cara menghubungkan rangkaian dengan kaedah ini dinamakan internetworking.
- c. **Cyber** adalah istilah yang digunakan orang untuk menyatakan sesuatu yang berhubungan dengan Internet atau dunia maya. Wiener sebagai pencetus Cybernetics theory mengakui bahwa istilah Cyber sebenarnya pernah digagas oleh Ampere yang namanya digunakan sebagai satuan kuat arus. Oleh karena itu jika ditilik dari asal-usulnya, istilah cyber sebenarnya erat hubungannya dengan kawat listrik. Sehingga tidak mengherankan, jika istilah tersebut juga digunakan untuk organ buatan listrik CYBORG yang merupakan singkatan dari Cybernetics Organics.
- d. **Cyberspace** adalah Dunia maya, dunia internet, virtual space. Kata ini dipopulerkan oleh William Gibson dalam novel fantasinya yang berjudul Neuromancer (1984) untuk menerangkan dunia komputer dan masyarakat yang berkumpul di sekitarnya. Menurutnya, **cyberspace adalah {consensual hallucination experienced daily by billions of legitimate operators ... a graphical representation of data abstracted from the banks of every computer in the human system}**. Substansi cyberspace sebenarnya adalah keberadaan informasi dan komunikasi yang dalam konteks ini dilakukan secara elektronik dalam bentuk visualisasi tatap muka interaktif. Komunikasi virtual (virtual communication) tersebut - yang dipahami sebagai virtual reality - sering disalahpahami sebagai {alam maya}, padahal keberadaan sistem elektronik itu sendiri adalah konkrit di mana komunikasi virtual sebenarnya dilakukan dengan cara representasi informasi digital yang bersifat diskrit.
- e. **Multimedia** adalah penggunaan komputer untuk menyajikan dan menggabungkan teks, suara, gambar, animasi dan video dengan alat bantu (tool) dan koneksi (link) sehingga pengguna dapat ber-(navigasi), berinteraksi, berkarya dan berkomunikasi. Multimedia sering digunakan dalam dunia hiburan. Selain dari dunia hiburan, Multimedia juga diadopsi oleh dunia Game.
- f. **Teknologi Informasi** adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
- g. **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.
- h. **Transaksi Elektronik** adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.

5. Apa yang dimaksud dengan :
- a. Typo site
 - b. Keylogger
 - c. Sniffing
 - d. Brute Force Attacking
 - e. Web Deface
 - f. Email Spamming
 - g. Denial of Service
 - h. Virus

Jawab :

- a. **Typo site** adalah sebuah kejahatan yang unik dan umumnya korban tidak menyadari. Salah satu cara yang digunakan adalah pelaku membuat sebuah situs yang namanya mirip dengan situs asli. Sebagai contoh adalah <http://banka.com> dibuat dengan nama <http://bankaa.com>. Typo site sangat mudah dibuat bagi domain .com ; .net dan .org serta beberapa domain lainnya. Kemudian situs tersebut dibuat mirip dengan aslinya. Tujuannya adalah untuk menangkap user ID, password dan data-data pribadi.
- b. **Keylogger** adalah software yang dipasang di komputer dan mempunyai kerja mencatat semua aktivitas yang dilakukan oleh keyboard. Apapun yang kita ketikkan di keyboard, maka akan dicatat oleh keylogger.
- c. **Sniffing** (mengendus) adalah teknik mencium paket data yang sedang lewat. Cara ini banyak digunakan oleh para admin agar jaringan lokal di dalamnya aman. Tapi harus berhati-hati juga, kadang teknik sniffing ini di gunakan oleh tangan-tangan yang tidak bertanggung jawab, untuk hal-hal yang di katakan privasi, yaitu mencium username, password dan apa yang sedang anda akses akan tercium oleh para cracker yang ada di jaringan lokal anda.
- d. **Brute Force Attacking** adalah teknik menyerang yang paling banyak digunakan untuk memecahkan password, kunci, kode atau kombinasi. Cara kerja metode ini sangat sederhana yaitu mencoba semua kombinasi yang mungkin. Seperti ciri khas sebuah brute force, metode ini dijamin akan menemukan solusi. Tetapi yang menjadi pertanyaan adalah kapan solusi itu akan ditemukan dan berapa besar memori yang dibutuhkan sampai solusi itu ditemukan.
- e. **Web Deface** adalah suatu teknik ilegal yang digunakan untuk mengganti atau mengubah seluruh atau sebagian halaman dari suatu website tanpa se-ijin pengelolanya. dan yang sedang marak akhir-akhir ini adalah defacing Profile Friendster secara massal.
- f. **Email spamming** adalah unsolicited email (email yang tidak diminta) yang dikirim ke banyak orang. Contoh kiriman email yang berisi spam: iklan, advertensi, tawaran untuk bergabung ke MLM, undian, informasi palsu, phishing, penipuan. Ya, NimHost selalu berusaha memerangi siapapun yang melakukan spam. *Spam* ini biasanya datang bertubi-tubi tanpa diminta dan sering kali tidak dikehendaki oleh penerimanya.
- g. **Denial of Service** atau **Serangan DoS** adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang

dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

- h. **Virus (virus komputer)** merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus komputer dapat dianalogikan dengan virus biologis yang menyebar dengan cara menyisipkan dirinya sendiri ke sel makhluk hidup. Virus komputer dapat merusak (misalnya dengan merusak data pada dokumen), membuat pengguna komputer merasa terganggu, maupun tidak menimbulkan efek sama sekali.
6. Setujukah Saudara dengan pernyataan bahwa: pemrosesan kejahatan dunia maya saat ini belum efektif karena kurangnya kemampuan dan ketrampilan aparat dalam bidang dunia maya? Jelaskan!

Jawab :

Ya setuju, karena kejahatan dunia maya atau cyber crime di Indonesia saat ini tergolong cukup memprihatinkan. Di sisi lain, penegakan hukum terhadap pelaku kejahatan dunia maya masih terkendala ketiadaan undang-undang yang mengatur secara khusus atau *lex specialis* mengenai kejahatan dunia maya. Sementara kita sering kali melihat dan mendengar adanya kejahatan dan pelanggaran dunia maya tapi belum nampak proses pengadilan terhadap pelaku-pelakunya, dan ini salah satu faktornya kekurangsiapan baik keterampilan maupun kemampuan aparat-aparat kita, baik taktis, teknis penyidikan, penuntutan dan pemeriksaan di pengadilan tidak dikuasai karena menyangkut sistem yang ada di dalam komputer. Oleh karena itu perlu melatih aparat yang terkait untuk meningkatkan kemampuan dan keterampilannya, sehingga penegakan hukum Cyber dapat dilakukan dan pelaku kejahatan cyber dapat segera diadili dan menjadi jera. Juga degan merekrut ahli-ahli komputer serta dengan mengoptimalkan infrastruktur yang ada.

7. Instansi pemerintah mana yang menurut Saudara bertanggungjawab untuk mengatur (membuat regulasi) pemanfaatan dunia maya, khususnya informasi dan transaksi elektronik?

Jawab :

Menurut saya instansi pemerintah yang turut bertanggung jawab untuk penegakkan regulasi tentang pemanfaatan dunia maya, khususnya informasi dan transaksi elektronik adalah :

- a. Depkominfo (Departemen Komunikasi dan Informasi)
 - b. KADIN (Kantor Dagang dan Industri)
 - c. Depkumham (Departemen Hukum dan Hak Asasi Manusia)
8. Beberapa waktu yang lalu pemerintah melakukan pemblokiran terhadap situs-situs yang dianggap berbahaya terutama situs-situs porno. Berhasilkah tindakan ini, dan apakah situs-situs terlarang tersebut sekarang ini benar benar sudah tidak bisa lagi diakses?

Jawab :

Blokir situs porno yang digagas dan dilakukan pemerintah jelas merupakan langkah yang baik dan mulia di tengah banjir situs-situs porno yang luar biasa itu. Ada 4 juta limaratus ribu situs porno di internet dan tiap pekannya bertambah sebanyak 250 situs merangsang syawat, seperti yang tulis media Indonesia beberapa waktu lalu. Lalu kita bertanya akan berjumlah berapa jika

situs haram itu tidak diblokier ? bukan tidak mungkin situs birahi itu akan mencapai triliunan, bahkan mungkin tidak dapat dihitung lagi. Dampaknya, tidak usaha dibahas lagi kecuali jelas-jelas merusak mental penikmatnya. Tidak pandang usia, anak-anak hingga yang sepuh sekalipun akan terkikis kira moralitas dan spiritualitasnya.

Kemudian pertanyaannya lagi, ***berhasilkah internet kita bebas dari situs porno ? jawabannya adalah mengurangi meminimal mungkin.*** Sebab tidak mungkin pemerintah dan lembaga jaringan walaupun sekompak bagaimanapun menghapus sampai titik nol. Sebab itu terkait dengan server yang dipakai. Kalau server yang digunakan itu produk dalam negeri itu masih mungkin. Tapi kalau server luar negeri yang dipakai, maka situs dosa itu tidak mungkin dihilangkan. Selain soal server, meng-update situs porno yang tiap hari bertaburan membutuhkan waktu, yang tidak mungkin di update tiap hari. Ini artinya, walaupun server dalam negeri yang dipakai, masih bisa pecinta situs porno menikmatinya dengan puas sambil menunggu situs yang baru datang itu di update. Setelah cukup waktu pemerintah meng-update situs yang baru datang” itu, si pencinta situs porno tersebut dapat mengakses situs yang lebih baru lagi yang masih nunggu giliran waktu di update, yang lalu kemudian di blokir. Jadi tiap hari situs porno dapat hadir di internet.

Oleh sebab itu, kita tidak boleh menggantungkan sepenuhnya kepada blokir pemerintah, melainkan public yang mendukung dengan kesadarannya sendiri. Mereka produsen situs tidak akan diam dengan upaya pemblokiran. Mereka pasti meniasati untuk selalu lolos sebab keuntungan yang didapat sangat melimpah. Per bulan pa ling sedikit mereka meraih keuntungan 30 juta ke 50 juta. “Tikus” boleh saja loncat sana loncat sini, tapi si tikus kadang lupa bahwa makanan yang ada di sampingnya terduduk racun yang mematikan atau walaupun tidak mata ia akan akan sekarat mengerang sakit. Para provider “silahkan” mengalirkan situs-situs porno, toh nanti ia akan kejeput dengan sanksi yang mesti menjeratnya sesuai dengan UU informasi dan transaksi elektronik (UU ITB) pasal 27 : “Denda Rp. 1 milyar dan enam tahun penjara bagi orang yang membuat, mendistribusikan, mentranmi sikan yang melanggar kesusilaan, judi, menghina dan mencemari nama baik, memeras dan mengancam”.

-- ooOoo --