DEPARTEMEN PENDIDIKAN NASIONAL

UNIVERSITAS GADJAH MADA

FAKULTAS HUKUM

PENULISAN HUKUM

PENGGUNAAN BUKTI ELEKTRONIK DALAM PEMBUKTIAN PERKARA KEJAHATAN DUNIA MAYA

Penulisan Hukum ini disusun untuk melengkapi persyaratan dalam memperoleh gelar Sarjana Hukum

DISUSUN OLEH :

Nama : Nuurlaila. F. Aziizah

NIM : 03 / 169388 / HK / 16476

Bagian : Hukum Pidana

YOGYAKARTA

2008

HALAMAN PERSETUJUAN

PENGGUNAAN BUKTI ELEKTRONIK DALAM PEMBUKTIAN PERKARA KEJAHATAN DUNIA MAYA

Disusun Oleh

N. F. Aziizah

NIM : 03 / 169388 / HK / 16476

Menyetujui

Dosen Pembimbing

Edward O.S Hiariej, S.H., M.Hum

NIP : 132232463

HALAMAN PENGESAHAN

Penulisan Hukum ini telah dipertahankan dihadapan Dewan penguji Fakultas Hukum Universitas Gadjah Mada, Pada Hari Selasa, Tanggal 26 Februari 2008

Dewan Penguji

Ketua

Sigid Riyanto, S.H., Msi
NIP : 131692729

Anggota I

Edward O.S Hiariej, S.H., M.Hum
NIP : 132232463

Anggota II

Dra. Dani Krisnawati, S.H., M.Hum
NIP : 132049433

Mengetahui
Ketua Bagian Hukum Pidana

Sigid Riyanto, S.H., Msi
NIP : 131692729

Mengesahkan :
Dekan Fakultas Hukum
Universitas Gadjah Mada

Dr. Marsudi Triatmodjo, S.H.,L.L.M
NIP : 131.598.151

HALAMAN PERNYATAAN

Dengan ini saya menyatakan bahwa Penulisan Hukum ini tidak pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi lain, dan sepanjang pengetahuan saya didalamnya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 28 Januari 2008

N. F. Aziizah

HALAMAN PERSEMBAHAN

Skripsi ini Penulis persembahkan sebagai kenangan kepada Alm. Soerjadi S.H Ketua Mahkamah Agung RI dan Ketua Mahkamah Tentara Agung ke-III yang memberikan kehidupannya dengan Sederhana, Jujur, Berani, Profesional, dan Loyal kepada Negara DEMI TEGAKNYA KEBENARAN DAN KEADILAN HUKUM BERDASARKAN KETUHANAN YANG MAHA ESA. Selama 27 tahun sejak Beliau pensiun sebagai Ketua MA, tiada waktu dan perhatian yang Beliau sia-siakan untuk mengabdi kepada tegaknya hukum dengan mengajar memberi nasehat hukum dan membuat pertimbangan hukum kepada siapapun yang meminta hal itu kepada Beliau.

KATA PENGANTAR

Segala puji dan syukur Penulis panjatkan kehadirat ALLAH S.W.T yang telah memberikan berkah, rahmat, dan hidayah-Nya kepada Penulis agar dapat menyelesaikan penulisan skripsi ini yang berjudul "Penggunaan Bukti Elektronik dalam Pembuktian Perkara Kejahatan Dunia Maya".

Penulis menyadari bahwa penulisan hukum ini masih jauh dari sempurna dan masih terdapat banyak kekurangan karena segala keterbatasan yang dimiliki Penulis. Oleh karena itu, dengan segala kerendahan hati, saran dan kritik yang membangun sangat Penulis harapkan demi kesempurnaan penulisan hukum ini.

Penulisan hukum ini tidak akan terwujud tanpa bantuan dari berbagai pihak, baik bantuan yang diberikan secara langsung maupun tidak langsung. Atas segala bantuan yang telah diberikan, Penulis menghaturkan penghargaan dan terima kasih yang sebenar-benarnya kepada para pihak yang telah banyak membantu dan menolong Penulis selama pembuatan skripsi ini :

1. Dr. Marsudi Triatmodjo, S.H., L.L.M, selaku Dekan Fakultas Hukum Universitas Gadjah Mada.
2. Bapak Sigid Riyanto, S.H., M.Si, selaku Ketua Jurusan Hukum Pidana.
3. Bapak Edward O.S Hiariej, S.H., M.Hum, selaku Dosen Pembimbing yang dengan sabar dan penuh pengertian telah membantu Penulis dalam penulisan skripsi ini.

4. Bapak Sigid Riyanto, S.H., M.Si, Ibu Dra. Hj. Dani Krisnawati, S.H., M.Hum, dan Bapak Eddy O.S Hiariej, S.H., M.Hum selaku Dosen Penguji.
5. Ibu Hj. Sri Suyatie, S.H, selaku Dosen Pembimbing Akademik.
6. Ketua Pengadilan Negeri Jakarta Barat, yang telah memberikan izin kepada Penulis untuk melakukan penelitian dalam mencari bahan dan data penulisan hukum.
7. Ibu Suwasti SH, CN, selaku Jaksa Madya dan Jaksa Penuntut Umum Kejaksaan Tinggi DKI JAYA yang telah membantu Penulis dalam mencari data penulisan skripsi.
8. Bapak Edmon Makarim S.Kom, SH, LLM, selaku Ketua Pusat Hak Kekayaan Intelektual Lembaga Kajian Hukum dan Teknologi Fakultas Hukum Universitas Indonesia yang telah membimbing Penulis dalam melakukan penelitian serta mendapatkan bahan dan data penulisan skripsi.
9. Bapak Eddy Hartono, S.Ik, selaku Penyidik Madya Unit V IT & Cyber Crime Direktorat Ekonomi dan Khusus BARESKRIM MABES POLRI yang telah membantu Penulis dalam melakukan penelitian skripsi ini.
10. Ibu Dra. Hj. Dani Krisnawati , S.H., M.Hum, selaku Sekretaris Bagian Hukum Pidana Fakultas Hukum Universitas Gadjah Mada yang telah banyak membantu selama penulisan skripsi ini.

My sPeCial tHankS GoEs to …….. :

1. Mama

Terima kasih yang tak terucap untuk Mama yang tak henti-hentinya beribadah dan berdo'a kepada ALLAH S.W.T agar anak-anaknya (Aziizah dan Karim) dapat menyelesaikan studinya dan menjadi seorang Sarjana. Love U Sooo Bloody MucH, Mom!

2. Ayah

Orang Tua adalah cermin seorang anak untuk melihat masa depannya. Ayah adalah sosok yang sangat Aziizah kagumi. Terima kasih Ayah yang selama ini membiayai sekolahku, dan mendidik ku agar kelak menjadi seorang Profesional yang tangguh di Bidang Hukum. Insya ALLAH dengan gelar kesarjanaan yang telah Aziizah raih ini dapat menjadi modal untuk menjadi seorang profesionalisme seperti Alm. Soerjadi., S.H, kakek Aziizah yang selalu menjadi panutan. Menjadi Sarjana adalah awal dari perjuanganku yah. Insya ALLAH Aziizah bisa membuat Ayah bangga.. Love U So much, Dad !

3. My Dearest One and Only Brother (Yusuf Ismail Abdul Karim)

Terima kasih ya Dikoo untuk supportnya, thank's bgt udah ngajarin aku tentang TI hehehe. Ayo raih nilai setinggi-tingginya, dan cepet lulus ya! Make Mom and Dad to be Proud of U !!!!

4. Rio Fajar Aviantara

Makasiiiy banget ya Bie untuk support, do'a, dan perhatian kamu selama ini ke aku.. Aku seneng bgt selama 4 tahun ini aku punya someone 2 share about almost everything, and 2 me U'r always be somebody who cares, for me passionately with every thought and with every breath, someone who will help me see things, in a different light.. And mksiy yaa buat printer n komputernya di Tanjung Mas Raya B8 No.5 hehe

5. Sahabat-sahabatku

Lenggi (Miss u so Much, Sis!), Handa, Ekha (C u @ Bali), Andy (Thx bgt ya Ndy supportnya,curhatnya+masa2 di jgj hehehe), Kobel, Ernest, Dana, Asenk, Qdut (mksi yaa udh nemenin aku waktu kalian di Jgj), Bomzy, Gege, Linda

6. Teman-teman UGM ku

{Vikaaa, Kusuma S.H (maaf ya sering ngrepotin n mksiii bgt2 ya Kus), Army S.H (thx bgt ya My, cpt kerja ya!), Oswald (smg Sukses ya! Makasi bgt yaa pinjeman2 bukunya, diskusi2nya), Rafles S.H (Makasi ya Rafles udah ngajarin aku hehe), Made S.H (huaa tenkyu bgt pinjeman2nya..), Togu S.H, Ncek S.H, Arya S.H, Rifky S.H, Vardy SH, and thank u all yang tak bisa kusebutkan satu per satu.

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Dalam era informasi (*information age*), keberadaan suatu informasi mempunyai arti dan peranan yang sangat penting didalam aspek kehidupan sehingga ketergantungan akan tersedianya informasi semakin meningkat. Perubahan bentuk masyarakat menjadi suatu masyarakat informasi (*information society*) memicu perkembangan teknologi informasi (*information technology revolution*) yang menciptakan perangkat teknologi yang kian canggih dan informasi yang berkualitas.

”Kita telah berada dalam teknologi elektronik yang berbasiskan lingkungan digital, contohnya komputer pribadi, mesin fax, penggunaan kartu kredit, dan hal-hal lainnya”.[1]

> Hal yang membuat internet memiliki peran yang sangat penting adalah potensi yang dimilikinya sebagai media teknologi informasi, antara lain :
> 1. keberadaannya sebagai jaringan elektronik publik yang sangat besar;
> 2. mampu memenuhi berbagai kebutuhan berinformasi dan berkomunikasi secara murah, cepat, dan mudah diakses, dan;
> 3. menggunakan data elektronik sebagai media penyampaian pesan/data sehingga dapat dilakukan pengiriman, penerimaan, dan penyebarluasan informasi secara mudah dan ringkas.[2]

Di Indonesia, perkembangan teknologi informasi semakin pesat dan pengggunanya pun semakin banyak tetapi perkembangan ini tidak diimbangi

---

[1] Edmon Makarim, 2005, *Pengantar Hukum Telematika*, Rajagrafindo Perkasa, Jakarta, Hlm. 31

[2] Jurnal Hukum dan Teknologi No. 1, 2001, “*Pokok - pokok pikiran rancangan Undang-undang informasi dan transaksi elektronik* (RUU-IETE)”, LKHT Fakultas Hukum UI ‘M.Arsyad sanusi, 2005, *Hukum dan Teknologi Informasi*, Tim KemasBuku, Jakarta, Hlm. 120’

dengan perkembangan produk hukumnya. Data atau informasi elektronik akan diolah dan diproses dalam suatu sistem elektronik dalam bentuk gelombang digital (*digital information*). Dengan kemajuan teknologi informasi yang pesat, diiringi dengan terjadinya perikatan antar pihak yang dilakukan dengan cara pertukaran informasi untuk melakukan transaksi perdagangan secara elektronik di ruang lingkup maya (*cyber*).

> Transaksi elektronik yang sering disebut sebagai "*online contract*" sebenarnya ialah transaksi yang dilakukan secara elektronik dengan memadukan jaringan (*networking*) dari sistem informasi berbasiskan komputer (*computer-based information system*) dengan sistem komunikasi yang berdasarkan atas jaringan dan jasa telekomunikasi (*telecommunication-based*), yang selanjutnya difasilitasi oleh keberadaan jaringan komputer global internet.[3]

Akan tetapi kerap timbul dampak negatif dari perkembangan teknologi informasi tersebut salah satu contohnya seperti pembobolan rekening nasabah secara online melalui dunia maya (*cyber*). Secara teknis, informasi dan/atau sistem informasi itu sendiri sangat rentan untuk tidak berjalan sebagaimana seharusnya (*malfunction*), dapat diubah-ubah ataupun diterobos oleh pihak lain. Untuk melindungi kerahasiaan informasi pribadi dari ancaman pelanggaran kerahasiannya, dibutuhkan keamanan data (*data security*), keamanan komputer serta jaringannya. Dalam Asosiasi Teknologi Informasi Kanada pada Kongres Industri Informasi Internasional 2000 di Quebec, pernah menyatakan bahwa :

"*Information technology touches every aspect of human life and so can electronically enabled crime*".[4]

---

[3] Edmon Makarim, 2003, *Kompilasi Hukum Telematika*, Rajagrafindo Persada, Jakarta, Hlm. 223

[4] Information Technology Association of Canada (ITAC), *IIIC Common Views Paper On : Cyber Crime*, IIIC 2000 Millenium Congress, September 19 th.,2000,p.2 'Barda Nawawi, 2005,

"Demikian pula dengan perkembangan zaman, banyak kejahatan konvensional dilakukan dengan modus operandi yang canggih sehingga dalam proses beracara diperlukan teknik atau prosedur khusus untuk mengungkap suatu kejahatan".[5] Kegiatan perbankan yang memiliki potensi kejahatan dunia maya antara lain adalah layanan *online shopping* (berbelanja secara online) yang memberikan fasilitas pembayaran melalui kartu kredit (*credit card fraud*). Jenis kejahatan ini muncul akibat kemudahan sistem pembayaran menggunakan kartu kredit yang diberikan *online shop*. "Modusnya ialah pelaku menggunakan nomor kartu kredit korban untuk berbelanja di *online shop* ".[6] Pelaku dapat saja memperoleh nomor kartu kredit korban dengan model kejahatan kartu kredit yang konvensional atau melalui dunia maya.

Karena itulah, sistem hukum yang efektif telah menjadi tembok akhir bagi pencari keadilan sebagai penunjang dari penegakan hukum (*law enforcement*) untuk meminimumkan berbagai kejahatan di internet. Sebagai salah satu contoh kasus, tersangka perusakan situs Golkar, www.golkar.or.id, yakni Iqra Syafaat (27), diringkus polisi dari unit *Cyber Crime* Mabes Polri di warung elektronik Balerang di Jalan Raden Patah Nomor 81 Batam pada 2 Agustus 2006. Selain di warnet, Iqra juga melancarkan penyerangannya (*hacking/cracking*) di rumahnya kawasan Tanjung Uma, Batam. Tersangka hanya lulusan SMU, yang kerap berjualan buku elektronik (*e-book*). Penyerangan situs Golkar itu dilakukan pada

---

Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan, Citra Aditya Bakti, Bandung, Hlm. 136'

[5] Krisnawati, "*et all*", *Bunga Rampai Hukum Pidana Khusus*, 2006, Pena Pundi Aksara, Jakarta, Hlm. 3

[6] Eddy O.S Hiariej, 28 November 2005, *Materi Kuliah Hukum dan Teknologi*, FH UGM Jogjakarta

tanggal 9-13 Juli 2006. Kemudian, pada tanggal 17 Juli 2006, Partai Golkar melalui pengacaranya Zulhendri Hasan melaporkan hal tersebut ke Mabes Polri. Situs Golkar selama kurun waktu tersebut telah diserang 1.257 kali dari 31 lokasi yang tercatat di *Internet Protocol Address* (*IP Address*) dari sejumlah kota seperti Jakarta, Bekasi, Bandung, Surabaya, Lampung, Palembang, Medan, dan Batam. Selain itu, berdasarkan *IP Address* yang tercatat, penyerangan juga terhubung dengan *hacker* asing dari luar negeri seperti Malaysia, Amerika Serikat, Brazil, Turky, dan Rumania. Namun, yang disidik polisi terkait perusakan dengan pola yang dilakukan Iqra. Menurut Kepala Unit Information Technology and Cyber Crime Direktorat Ekonomi dan Khusus Badan Reserse Kriminal Mabes Polri Komisaris Besar Petrus Reinhard Golose, serangan (*deface*) pertama kali terjadi pada 9 Juli 2006. Iqra mengganti foto beberapa tokoh Golkar menjadi foto gorila putih tersenyum. Serangan berikutnya pada 10 Juli 2006, halaman muka situs Golkar diisi dengan foto mesum aktris *Hollywood* dengan tulisan "bersatu untuk malu". Kerugian materiil yang ditimbulkan dari perusakan situs Golkar itu sekitar Rp 150 juta. Berdasarkan pemeriksaan dan analisa laboratorium komputer forensik, penyidik menemukan pola serangan dari Batam menggunakan tiga *IP Address* yaitu 222.124.136.52, 222.124.136.81, 222.124.136.101. Ketiganya diketahui milik PT Inforsys Indonesia. Petrus menambahkan, berdasarkan pemeriksaan teknisi IT PT. Inforsys Indonesia, *IP Address* 222.124.136.81 digunakan oleh Warnet Barelang. "Kami juga melakukan *virtual undercover*, yaitu *chat* dengan program MirC dengan *server* Dalnet di *hacker community*. Ketahuan *nick name* Iqra yaitu Nogra. Kami juga *chat* dengan *Yahoo Messenger*,

dia memakai identitas singapore *bm@yahoo.com*" papar Petrus. Petrus mengungkapkan, Iqra selama ini kerap kali melakukan kejahatan *cyber* dengan modus menembus dan merusak sejumlah situs untuk mencari kelemahan situs. Setelah itu, dia menjual informasi yang diperolehnya. Pembayaran yang diperoleh secara tunai melalui *Western Union*. Iqra saban hari "bekerja" di depan komputer di warnet antara 10-12 jam. "Rekor tertinggi pendapatannya 600.000 dollar Amerika," imbuh Petrus. Polisi masih menyidik kemungkinan motivasi politik dibalik kejahatan cyber itu.[7]

Selain itu terdapat kejahatan dunia maya yang berhubungan dengan nama domain. Nama domain (*domain name*) digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang yang mencoba menarik keuntungan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis. Istilah yang sering digunakan adalah *cybersquatting*. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain (kasus: mustika-ratu.com). Kejahatan lain yang berhubungan dengan nama domain adalah membuat “domain plesetan”, yaitu domain yang mirip dengan nama domain orang lain.

“(Seperti kasus klikbca.com), istilah yang digunakan saat ini adalah *typosquatting*”.[8] Dengan adanya penyalahgunaan didalam transaksi elektronik tersebut karena terbentuk dari suatu proses elektronik, sehingga objeknya pun

[7] www.polri.go.id/berita, 10 Agustus 2006, *Perusak Situs Golkar Tertangkap*, diakses pada tanggal 28 Februari 2007

[8] www.lkhtnet.com, 31 Juli 2004, *Kasus Klik BCA.com*, Edmon Makarim, diakses pada tanggal 28 Februari 2007

berubah, barang menjadi data elektronik dan alat buktinya pun bersifat elektronik. Mengacu pada ketentuan hukum positif di Indonesia, ada beberapa peraturan perundang-undangan yang telah mengatur mengenai alat bukti elektronik (*digital evidence*) sebagai alat bukti yang sah di muka pengadilan. Salah satu contohnya, yaitu pada Undang - Undang No. 25 Tahun 2003 tentang Pencucian Uang. Terhadap tindak pidana yang telah memiliki aturan hukum yang mengatur mengenai *digital evidence* (alat bukti elektronik) bukanlah suatu masalah. Namun, bagi perbuatan melanggar hukum yang belum memiliki aturan hukum khusus mengenai bukti elektronik sebagai alat bukti yang sah di muka pengadilan, maka diperlukan kecakapan aparat penegak hukum untuk melihat dan menterjemahkan bukti elektronik yang ada menjadi alat-alat bukti sebagaimana diatur dalam Pasal 184 Undang - Undang No. 8 Tahun 1981 tentang Hukum Acara Pidana sebagai alat bukti yang sah di muka pengadilan. Mengingat bahwa pada asasnya, hakim tidak dapat menolak setiap perkara yang diajukan ke persidangan dengan dalil tidak ada dasar hukumnya. Sesuai dengan adagium *ius curia novit*, yaitu hakim dianggap tahu akan hukumnya. Berdasarkan uraian diatas, penulis memilih judul penelitian skripsi yaitu : "Penggunaan Bukti Elektronik Dalam Pembuktian Perkara Kejahatan Dunia Maya".

B. Perumusan Masalah

Bertolak dari latar belakang masalah diatas, untuk mendukung efektivitas komunikasi dengan memanfaatkan secara optimal Teknologi Informasi demi tercapainya keadilan, kemanfaatan dan kepastian hukum, dan menjadi langkah

preventif serta represif terhadap perkara kejahatan dunia maya, dengan demikian dapat dirumuskan masalahnya sebagai berikut :

Bagaimana penggunaan bukti elektronik dalam pemeriksaan perkara kejahatan dunia maya ?

C. Tujuan Penelitian

Penelitian penulisan hukum ini bertujuan untuk :

1. Tujuan Subjektif

   Untuk memperoleh gelar Sarjana Hukum dari Universitas Gadjah Mada.

2. Tujuan Objektif

   Untuk menjelaskan bagaimana penggunaan bukti elektronik dalam pembuktian perkara kejahatan dunia maya di pengadilan

D. Keaslian Penelitian

Untuk melihat keaslian penelitian telah dilakukan penelusuran penelitian pada berbagai referensi dan hasil penelitian serta dalam media cetak maupun elektronik. Penelitian yang berkaitan dengan data atau dokumen elektronik khususnya ”Penggunaan Bukti Elektronik dalam Pembuktian Perkara Kejahatan Dunia Maya” belum pernah dilakukan dan dalam kesempatan ini peneliti akan meneliti masalah tersebut, dengan demikian penelitian ini adalah asli.

E. Manfaat Penelitian

Dari hasil penelitian ini diharapkan dapat bermanfaat baik untuk kepentingan akademis maupun kepentingan praktis.

1. Manfaat Akademis

   a. Dari hasil penelitian penulisan hukum ini diharapkan dapat

memberikan kontribusi pengembangan ilmu pengetahuan pada umumnya, dan pengembangan ilmu hukum pada khususnya.

b. Dapat digunakan sebagai salah satu kelengkapan dalam persyaratan untuk memperoleh gelar Sarjana Hukum dari Universitas Gadjah Mada.

2. Manfaat Praktis

Dari hasil penelitian ini diharapkan dapat memberikan manfaat kepada masyarakat pada umumnya untuk mendukung agar Bukti Elektronik menjadi Alat Bukti yang Sah di Muka Pengadilan.

F. Tinjauan Pustaka

Hukum Pidana seyogyanya berkembang sesuai dengan perkembangan zaman yang memicu kemajuan teknologi. Untuk mengikuti kemajuan teknologi yang pesat, hukum pidana semakin nyata dibutuhkan di dalam suatu masyarakat.

> Menurut Moelyatno, Hukum Pidana adalah bagian daripada keseluruhan hukum yang berlaku di suatu negara, yang mengadakan dasar-dasar dan aturan-aturan untuk :
> 1) Menentukan perbuatan-perbuatan mana yang tidak boleh, yang dilarang, dengan disertai ancaman atau sangsi yang berupa pidana tertentu bagi barangsiapa melanggar larangan tersebut.
> 2) Menentukan kapan dan dalam hal-hal apa kepada mereka yang telah melanggar larangan-larangan itu dapat dikenai atau dijatuhi pidana sebagaimana yang telah diancamkan.
> 3) Menentukan dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang disangka telah melanggar larangan tersebut.[9]

Tentang penentuan perbuatan mana yang dipandang sebagai perbuatan pidana, kita menganut azas yang dinamakan azas legalitas (*principle of legality*), yakni suatu perbuatan hanya merupakan tindak pidana, jika ditentukan terlebih

[9] Moeljatno, 1993, *Asas - asas Hukum Pidana*, Rineka Cipta, Jakarta, Hlm. 1

dahulu dalam suatu ketentuan perundang-undangan (pasal 1 ayat 1 KUHP). Dalam bahasa latin, ada pepatah yang maknanya sama dan berbunyi : *Nullum delictum nulla poena sine preavia legi poenali* (tiada kejahatan, tiada hukuman pidana tanpa undang-undang hukum pidana terlebih dahulu).[10] Barangsiapa yang melakukan perbuatan pidana diancam dengan pidana tertentu yang telah ditentukan dalam ketentuan perundang-undangan. Akan tetapi, dalam memidana seseorang yang telah disangka melakukan perbuatan pidana tersebut, dikenal asas yang berbunyi : "*Tidak dipidana tanpa kesalahan*". Dalam bahasa Belanda : "*Geen straf zonder schuld*". Penentuan mengenai dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang disangka melakukan perbuatan pidana diatur didalam hukum pidana formal atau Hukum Acara Pidana. "Van Bemmelen mengatakan : Ilmu Hukum Acara Pidana mempelajari peraturan-peraturan yang diciptakan oleh negara, karena adanya dugaan terjadi pelanggaran undang-undang pidana".[11]

Sebelum kita masuk ke dalam pengertian informasi, kita harus mengetahui terlebih dahulu akar dari informasi tersebut, yaitu Data. Menurut Turban, Rainer, dan Potter, "***Data*** *are raw facts or elementary description of things, events, activities, and transactions that are captured, recorded, stored, and classified, but not organized to convey any specific meaning. Example of data would include bank ballances"*. Data ialah gambaran dasar, fakta-fakta awal yang belum terperinci dari perihal, peristiwa, kegiatan, dan transaksi yang ditangkap, direkam,

---

[10] Wirjono Prodjodikoro, 2003, *Asas-asas Hukum Pidana di Indonesia*, Refika Aditama, Bandung, Hlm. 42

[11] Andi Hamzah, 1985 : 17-18, 'Mohammad Taufik Makarao, Suhasril, 2004, *Hukum Acara Pidana dalam Teori dan Praktek*, Penerbit Ghalia Indonesia, Jakarta, Hlm. 2'

disimpan, dan terklasifikasi tetapi tidak terorganisir untuk dapat menyatakan arti khusus apapun.

Contoh data ialah catatan saldo rekening bank.[12]

Sedangkan pengertian informasi menurut Turban, Rainer, dan Potter, "***Information*** *is a collection of facts organized in some manner so that they are meaningful to a recipient. For example, if we include costumer names with bank ballances, we would have useful information*". "Contoh informasi ialah saldo rekening bank yang disertai dengan identitas pemegang rekening".[13] Dengan kata lain, informasi bersumber dari data yang telah diproses. Sedangkan yang dimaksud dengan informasi elektronik dapat berupa catatan elektronik, data atau dokumen elektronik, surat elektronik, ataupun tanda tangan elektronik.

Suatu data/informasi yang telah diolah oleh sistem informasi secara elektronik tersebut, akan tersimpan didalam suatu media tertentu, yang dinamakan dokumen elektronik. Sistem penyimpanan data dan/atau informasi elektronik yang berbasiskan komputer dinamakan *Databases* dan data yang dikomunikasikan melalui media telekomunikasi dinamakan *Data Messages*. Apabila kita merujuk pada Keppres No.8 Tahun 1997 tentang Dokumen Perusahaan ("UUDP"), dapat kita cermati pengertian Dokumen Perusahaan adalah data, catatan, dan atau keterangan yang dibuat dan/atau diterima oleh perusahaan dalam rangka pelaksanaan kegiatannya baik tertulis diatas kertas atau sarana lain maupun terekam dalam bentuk corak apapun yang dapat dilihat, dibaca, atau didengar. Adapun yang menarik dari keberadaan UU Pokok Kearsipan dan Dokumen

[12]Turban,Rainer, dan Potter.,*Introduction to Information Technology* 'Edmon Makarim, *Kompilasi Hukum Telematika*, Rajagrafindo Persada, Jakarta, Hlm. 31 (terjemahan bebas penulis)'

[13] *Ibid*, Hlm. 31

Perusahaan diatas ialah terbukanya pemahaman mengenai keberadaan suatu informasi yang tersimpan secara elektronik (arsip elektronik).

Definisi mengenai kejahatan komputer atau penyalahgunaan komputer menurut departemen kehakiman Amerika antara lain, bahwa penyalahgunaan komputer dibagi dua bidang utama. Pertama, penggunaan komputer sebagai alat untuk melakukan kejahatan, seperti pencurian. Kedua, komputer tersebut merupakan objek atau sasaran dari tindak kejahatan tersebut, seperti sabotase yang menyebabkan komputer tidak dapat berfungsi sebagaimana mestinya, atau pencurian data. Laporan Kongres PBB X/2000 menyatakan *Computer-Related Crime* (CRC) mencakup :

> "Keseluruhan bentuk-bentuk baru dari kejahatan yang ditujukan pada komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer"[14]

G. Metode penelitian

1. Jenis Penelitian

   Penelitian ini merupakan kombinasi antara penelitian hukum empiris dan penelitian hukum normatif. Penelitian hukum empiris dilakukan melalui observasi dan wawancara yang mendalam dengan responden dan

[14]Dokumen Kongres PBB X, A/CONF.187/L.10, 16-4-2000, hlm. 1-2 dan dokumen A/CONF.187/15, 19-7-2000, hlm. 26 : "*the entirely new forms of crime that were directed at computers, networks and their users, and the more traditional form of crime that were now being committed with the use of computer equipment*", 'Barda Nawawi Arief, 2005, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*, Citra Aditya Bakti, Bandung, Hlm. 136'

narasumber yang berkompeten dan terkait dengan masalah yang diteliti (objek yang diteliti) untuk mendapatkan data primer.

Penelitian hukum normatif dilakukan dengan mengumpulkan bahan hukum, baik primer, sekunder maupun tersier.

2. Jenis Data

Adapun data-data yang diperlukan dalam Penulisan Hukum ini adalah sebagai berikut :

a. Pada penelitian hukum normatif, data yang dicari berupa data sekunder dan data tersier. Data sekunder yaitu berupa data - data dan keterangan yang diperoleh melalui penelitian kepustakaan (*library research*) dengan mempelajari dokumen - dokumen atau tulisan para ahli, buku - buku literatur, Yurisprudensi serta berbagai macam peraturan perundang-undangan yang berhubungan dengan materi atau isi dari permasalahan. Data tersier yaitu berupa data-data yang diperoleh dari berbagai situs di Internet,

b. Pada penelitian hukum empiris, data yang dicari berupa data primer, yaitu berupa data-data yang diperoleh dari hasil pengamatan serta penelitian secara langsung di lapangan (*field research*).

3. Cara Pengumpulan Data

Data yang dikumpulkan penulis bersumber pada :

a. Studi Kepustakaan (*library research*)

Asal data ini bersifat data sekunder, yaitu data-data dan keterangan yang diperoleh melalui penelitian kepustakaan (*library research*) dengan

mempelajari dokumen - dokumen atau tulisan para ahli, buku - buku literatur, Yurisprudensi serta berbagai macam peraturan perundang-undangan yang berhubungan dengan materi atau isi dari permasalahan.

1) Kitab Undang - undang Hukum Pidana (KUHP)
2) Undang - Undang RI No. 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP)
3) Undang - Undang No. 36 Tahun 1999 tentang Telekomunikasi
4) Undang - Undang No. 20 Tahun 2001 tentang Perubahan Atas Undang - Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi
5) Undang - Undang Nomor 19 Tahun 2002 tentang Hak Cipta
6) Undang - Undang No. 25 Tahun 2003 tentang Pencucian Uang
7) Undang - Undang No. 21 Tahun 2007 tentang Perdagangan Orang
8) Keppres Nomor 8 Tahun 1997 tentang Dokumen Perusahaan
9) Rancangan Peraturan PerUndang-undangan KUHP Buku II Tindak Pidana
10) Rancangan Peraturan PerUndang-undangan KUHAP Tahun 2007
11) Rancangan Peraturan PerUndang-undangan Informasi dan Transaksi Elektronik

Serta data tersier, yaitu data–data yang diperoleh dari berbagai situs di internet.

b. Studi Lapangan (*field research*)

Asal data ini bersifat data primer, yaitu data–data yang diperoleh dari hasil pengamatan serta penelitian secara langsung di lapangan (*field research*).

Adapun metode pengumpulan data dapat berupa :

1) Dengan pedoman wawancara dari Narasumber dan Responden dengan menggunakan alat penelitian seperti *block note* (notes) dan/atau *tape recorder*.
2) Responden dan Narasumber

   Narasumber :

   a) Pakar di bidang Hukum Pidana UGM
   b) Ketua Pusat Hak Kekayaan Intelektual Lembaga Kajian Hukum dan Teknologi Fakultas Hukum UI (LKHT FHUI)

   Responden :

   c) Penyidik Madya Unit V IT dan Cyber Crime Direktorat Ekonomi dan Khusus Badan Reserse Kriminal Markas Besar POLRI
   d) Jaksa Madya dan Jaksa Penuntut Umum Kejaksaan Tinggi DKI JAYA
   e) Hakim Pengadilan Negeri Jakarta Barat
3) Lokasi Penelitian
   a) Lembaga Kajian Hukum dan Teknologi Fakultas Hukum Universitas Indonesia (LKHT FHUI)

b) Unit V Direktorat Ekonomi dan Khusus Badan Reserse Kriminal Markas Besar POLRI

c) Kejaksaan Tinggi DKI JAYA

d) Pengadilan Negeri Jakarta Barat

4. Analisis Data

Keseluruhan penelitian ini diperoleh dengan mengkombinasikan antara penelitian hukum normatif dengan penelitian hukum empiris yang dikaji dan dianalisis secara kualitatif dengan melakukan pendekatan hukum. Data dan informasi yang ditemukan akan diukur dengan ketentuan hukum yang berlaku berkaitan dengan isi dari permasalahan. Data yang telah diukur tersebut akan dianalisis dan dilakukan evaluasi penerapan hukumnya untuk mengetahui bagaimana penggunaan bukti elektronik dalam membuktikan perkara kejahatan dunia maya.

H. Sistematika Penulisan

Penulisan laporan penelitian ini akan disusun dalam 5 (lima) bab yaitu Bab I, Bab II, Bab III, Bab IV, dan Bab V. Dari Bab-bab tersebut kemudian diuraikan lagi menjadi sub bab-sub bab yang diperlukan. Sistematika penulisan selengkapnya dapat diuraikan sebagai berikut :

Bab I **Pendahuluan**, memuat latar belakang masalah, perumusan masalah, tujuan penelitian, keaslian penelitian, manfaat penelitian, tinjauan pustaka, metode penelitian dan sistematika penulisan mengenai ‘Penggunaan Bukti Elektronik Dalam Pembuktian Perkara Kejahatan Dunia Maya’.

Bab II **Tinjauan umum mengenai kejahatan dunia maya (*cybercrime*),** memuat pengertian umum tentang *cybercrime* menurut peraturan perundang-undangan di Indonesia, menurut rancangan peraturan perundang-undangan di Indonesia, menurut peraturan perundang-undangan di negara lain, modus operandi *cybercrime* meliputi *hacking*, *cracking*, j*oycomputing*, dan *carding* serta memuat pengertian dan klasifikasi dari bukti elektronik, dan peraturan mengenai bukti elektronik menurut peraturan perundang-undangan di Indonesia.

Bab III **Tinjauan aspek pembuktian dalam perkara pidana di Indonesia**, memuat tentang teori atau sistem pembuktian, jenis-jenis alat bukti menurut KUHAP, pengertian barang bukti, dan unsur pembuktian yang menimbulkan keyakinan hakim dalam memutus suatu perkara pidana.

Bab IV. **Hasil Penelitian dan Pembahasan**, memuat dan menjabarkan hasil penelitian dan pembahasan terhadap penggunaan bukti elektronik dalam pemeriksaan perkara kejahatan dunia maya di pengadilan.

Bab V. **Penutup**, bab ini berisi kesimpulan dari bab-bab terdahulu dan uraian singkat mengenai pokok-pokok analisis dan permasalahan yang ada, dan saran yang dianggap perlu.

BAB II

TINJAUAN UMUM MENGENAI KEJAHATAN DUNIA MAYA (*CYBERCRIME*)

A. Pengertian kejahatan dunia maya (*cybercrime*)

”Menurut M.v.T (*Memorie van Toelichting*) dikatakan bahwa kejahatan (*misdrijven*) adalah “*rechtsdelicten*”, yaitu perbuatan-perbuatan yang meskipun tidak ditentukan dalam undang-undang, sebagai perbuatan pidana, telah dirasakan sebagai *onrecht*, sebagai perbuatan yang bertentangan dengan tata-hukum”.[15] Dunia maya dapat disamakan dengan (internet : *inter-network*) yaitu sebutan untuk sekumpulan jaringan komputer yang menghubungkan situs akademik (*electronic learning*) seperti di UGM (*www.ugm.ac.id*), situs pemerintahan (e*lectronic government*), pelayanan transaksi elektronik melalui ATM (*electronic banking*), komersial (periklanan), organisasi, maupun perorangan. ”Dunia maya (*cyberspace*) dapat dideskripsikan sebagai suatu “ruang/dunia” non fisik yang didalamnya terjadi komunikasi-komunikasi elektronik dan tersimpan data-data digital didalam sebuah sistem komputer atau jaringannya”.[16] Melalui ruang dunia maya ini, kesepakatan-kesepakatan bisnis dapat dilakukan secara instan dari seluruh penjuru dunia, tanpa perlu lagi pena, kertas, dan bahkan tidak perlu lagi bertatap muka langsung. ”Bahkan, kini terjadi transaksi perdagangan secara elektronik yang sering disebut *e-commerce* (*electronic commerce*) yang menggunakan kartu kredit dan kartu debit untuk menggantikan mata uang

[15] Moeljatno, 2000, *Asas-asas Hukum Pidana*, Rineka Cipta, Jakarta, Hlm. 71
[16] M.Arsyad Sanusi, 2005, Hukum dan Teknologi Informasi, Tim KemasBuku, Hlm. 102

konvensional didalam transaksi yang mereka lakukan".[17] "Istilah dunia maya (*cyberspace*) pertama kali diperkenalkan oleh William Gibson pada tahun 1984, yaitu "*a futuristic computer network that people use by pludgging their minds into it*" atau dapat diartikan sebagai suatu jaringan komputer masa depan yang digunakan manusia dengan menghubungkan pikirannya ke dalam jaringan tersebut".[18] Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi adalah kejahatan yang berkaitan dengan aplikasi internet. Kejahatan ini dalam istilah asing sering disebut dengan *cybercrime* yang dilakukan didalam dunia maya (*cyberspace*). Dunia maya (*cyberspace*) tersebut bersifat global, artinya tidak terikat pada yuridiksi nasional suatu negara. "Tempat terjadinya kejahatan (*locus delicti*) dari kejahatan dunia maya (*cybercrime)* ini berada dalam ruang maya (*cyberspace*), yaitu suatu ruang yang berbasiskan pada jaringan komputer global internet".[19] "Menurut Achmad Ali, dunia maya ini sifatnya melampaui teritorial negara".[20] Berkaitan dengan kejahatan dunia maya ini, Eddy O.S Hiariej, staf pengajar pada FH UGM, mengatakan :

> "Ada kontradiksi yang sangat mencolok untuk menindak kejahatan seperti ini. Dalam hukum diperlukan adanya kepastian termasuk alat bukti kejahatan, tempat kejahatan, dan korban dari tindak kejahatan tersebut, sedangkan dalam *Crime by Computer* (*cybercrime* / kejahatan dunia maya) ini semuanya serba maya, lintas negara, dan lintas waktu"[21]

---

[17] M.Arsyad Sanusi, *op.cit*, Hlm. 103
[18] Petrus Reinhard Golose, 12 April 2007, *Penegakan Hukum Cyber Crime dalam Sistem Hukum Indonesia* dalam Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia, FHUI Jakarta, Hlm. 7
[19] Drs.Abdul Wahid,S.H.,MA dan Mohammad Labib,S.H, 2005, *Kejahatan Mayantara (cyber crime)*, Refika Aditama, Bandung, Hlm. 76
[20] *Ibid*, Hal. 69
[21] Eddy.O.S Hiariej, 13 April 2001, Bernas, '*Ibid*, Hlm. 76'

Sedangkan American Herritage Dictionary mendefinisikan *cyberspace* sebagai "*the electronic medium of computer networks, in which online communication takes place*" atau media elektronik jaringan komputer dimana komunikasi *online* terjadi. "Disimpulkan dari pengertian tersebut, Petrus Reinhard Golose mengemukakan bahwa dengan adanya internet, komunikasi antar manusia dapat terjadi secara *online* dan tanpa eksistensi fisik yang rawan akan penyalahgunaan dan dapat melahirkan berbagai bentuk perbuatan hukum baru ataupun kejahatan dengan metode baru yang sebelumnya belum pernah ada".[22]

Donn B. Parker memberikan definisi mengenai penyalahgunaan komputer : "*Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffered loss and a perpetrator by intention made or could have gain*", dan diterjemahkan oleh Andi Hamzah sebagai "penyalahgunaan komputer didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan".[23]

Kejahatan dalam bidang teknologi informasi secara umum terdiri dari dua kelompok, yaitu :

1) Kejahatan konvensional yang menggunakan bidang teknologi informasi sebagai alat bantunya

   Contohnya pembelian barang dengan menggunakan nomor kartu kredit

---

[22] Petrus Reinhard Golose, 12 April 2007, *Penegakan Hukum Cyber Crime dalam Sistem Hukum Indonesia* dalam Handout Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia, FHUI, Jakarta, Hlm. 8

[23] Donn B.Parker, 1976, Crime by Computer, Hlm.12, 'Andi Hamzah, 1993, *Hukum Pidana yang berkaitan dengan komputer*, Sinar Grafika Offset, Hlm. 18

curian melalui media internet;

2) Kejahatan timbul setelah adanya internet, dengan menggunakan sistem komputer sebagai korbannya

   Contoh kejahatan ini ialah perusak situs internet (*cracking*), pengiriman virus atau program-program komputer yang bertujuan untuk merusak sistem kerja komputer.

"LPKIA (Lembaga Pendidikan Komputer Indonesia Amerika) mendefinisikan kejahatan dunia maya sebagai penggunaan komputer secara ilegal".[24] Dalam hal kejahatan dunia maya, Polri sebagai aparat penegak hukum telah menyiapkan unit khusus untuk menangani kejahatan dunia maya ini, yaitu Unit V IT/*Cyber Crime* Direktorat II Ekonomi Khusus Bareskrim Polri. Polri dalam hal ini unit *cyber crime* menggunakan parameter berdasarkan dua dokumen Konferensi PBB mengenai *The Prevention of Crime and The Treatment of Offenders* di Havana, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal, yaitu "*cybercrime*" dan "*computer related crime*". Dalam *background paper* untuk lokakarya Konferensi PBB X/2000 di Wina, Austria istilah "*cybercrime*" dibagi dalam dua kategori. Pertama, *cybercrime* dalam arti sempit disebut "*computer crime*". Kedua, *cybercrime* dalam arti luas disebut "*computer related crime*". Secara gamblang dalam dokumen tersebut dinyatakan :

[24] www.lkhtnet.com, 31 Januari 2004, *Kejahatan dalam Dunia Cyber*, LKHT FH UI, diakses pada tanggal 28 Februari 2007

a. *Cybercrime in a narrow sense (computer crime) : any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed by them.*

b. *Cybercrime in a broader sense (computer related crime) : any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possesion, offering or distributing information by means of a computer system or network.*

Dengan demikian *cybercrime* meliputi kejahatan, yaitu yang dilakukan :

1. dengan menggunakan sarana-sarana dari sistem atau jaringan komputer (*by means of a computer system or network*);
2. di dalam sistem atau jaringan komputer (*in a computer system or network*); dan
3. terhadap sistem atau jaringan komputer (*against a computer system or network*).

Disimpulkan dari definisi tersebut, maka dalam arti sempit *cybercrime* adalah *computer crime* yang ditujukan terhadap sistem atau jaringan komputer, sedangkan dalam arti luas, *cybercrime* mencakup seluruh bentuk baru kejahatan yang ditujukan pada komputer, jaringan komputer dan penggunanya serta bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer (*computer-related crime*). Hal ini dimuat dalam laporan Konferensi PBB X/2000 : *"The term "Computer-related crime" had been developed to encompass both the entirely new forms of crime that were directed at computers, networks and their users, and the more traditional form of*

crime that were now being committed with use or assistance of computer equipment".[25] Council of Europe memberikan klasifikasi yang lebih rinci mengenai modus operandi *cybercrime* yang digolongkan sebagai berikut : *illegal access, illegal interception, Data interference, Misuse of Devices, Computer related forgery, Computer related fraud, Child-pornography, dan infrigements of copy rights and related rights*. Andi Hamzah memberikan definisi mengenai kejahatan komputer, yaitu : "Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".[26]

> Menurut Petrus Reinhard Golose, dalam kasus kejahatan dunia maya, baik korban maupun pelaku tidak berhadapan langsung dalam 1(satu) tempat kejadian perkara. Dalam beberapa kasus, baik korban maupun pelaku dapat berada pada negara yang berbeda. Hal tersebut menggambarkan bahwa kejahatan dunia maya merupakan salah satu bentuk kejahatan lintas negara (*transnational crime*), dan tak berbatas (*borderless*), tanpa kekerasan (*non violence*), tidak ada kontak fisik (*no phisically contact*) dan tanpa nama (*anonimity*).[27]

Untuk menangani kejahatan dunia maya (*cybercrime*) di Indonesia, Polri telah melakukan tindakan-tindakan penegakan hukum, pendekatan, dan telah menyusun strategi penanggulangan dan penanganan kejahatan dunia maya tersebut, yakni melaksanakan penyelidikan dan penyidikan tindak pidana mayantara (*cybercrime*) terutama kegiatan yang berhubungan dengan teknologi informasi : teknologi komputer, teknologi komunikasi, teknologi elektronika, dan teknologi penyiaran dan menyelenggarakan fungsi laboratorium komputer forensik dalam rangka memberikan dukungan teknis proses penyidikan kejahatan dunia maya.

---

[25] Barda Nawawi Arief, 2001, *Masalah Penegakan Hukum dan Penanggulangan Kejahatan*, Citra Aditya Bakti, Bandung, Hlm. 249-250

[26] Andi Hamzah, 1989, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, Hlm.26

[27] Petrus Reinhard Golose, 12 April 2007, *Penegakan Hukum Cyber Crime dalam Sistem Hukum Indonesia* dalam Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia, FHUI, Jakarta, Hlm. 19

Kejahatan dunia maya (c*ybercrime*) yang berhasil dilidik dan/atau disidik oleh Unit V IT dan *CyberCrime* Bareskrim Polri pada tahun 2006 dapat dilihat pada tabel di bawah ini[28] :

TABEL 1

REKAPITULASI KEJAHATAN MEMPERGUNAKAN INTERNET YANG DILIDIK/DISIDIK UNIT V IT & CYBERCRIME TAHUN 2006

No.	Jenis	Jumlah	Sumber		Keterangan
			Komplain Luar Negeri via Deplu/NCB	Laporan polisi	
1.	Penipuan	51	50	1	
2.	Pemalsuan	2	2		Phising
3.	Pengancaman	3	3		Melalui email (PM Australia & peledakan bom)
4.	Perjudian	5		5	
5.	Terorisme	1		1	www.anshar.net
6.	Perusakan	1		1	Deface website Partai Golkar www.golkar.or.id
7.	Lain-lain	2	2		Hacking, instrusion

[28] Denpasar, 26 Februari 2007, Petrus Reinhard Golose, *Rekapitulasi Kejahatan mempergunakan Internet yang dilidik/sidik Unit V IT & CyberCrime tahun 2006*, search engine google "Keamanan Internet di Indonesia", diakses pada tanggal 26 April 2007

"Adapun hukum positif saat ini yang dipergunakan oleh Unit V Direktorat II Ekonomi dan Khusus IT & Cyber Crime Badan Reserse Kriminal Mabes Polri dalam melaksanakan tugas penyidikan kejahatan dunia maya (*cybercrime*), adalah sebagai berikut"[29] :

1. Kitab Undang-undang Hukum Pidana (KUHP)

   Dalam upaya menangani kasus kejahatan dunia maya, para penyidik melakukan interpretasi ekstensif (perumpamaan dan persamaan) terhadap pasal-pasal yang terdapat dalam KUHP. Adapun pasal-pasal yang dapat dikenakan dalam KUHP terhadap kejahatan dunia maya, antara lain :

   a. Pasal 362 KUHP yang dikenakan untuk kasus *Carding* dimana pelaku mencuri kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan *software card generator* di internet untuk melakukan transaksi di *E-Commerce*.
   b. Pasal 378 KUHP yang dikenakan untuk penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan.
   c. Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *email*.
   d. Pasal 331 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media internet. Modusnya adalah pelaku menyebarkan *email* kepada teman-teman korban tentang suatu cerita yang

[29] Petrus Reinhard Golose, *op.cit*, Hlm. 30-31

tidak benar atau mengirimkan *email* secara berantai melalui *mailling list* (*millis*) tentang berita yang tidak benar.

e. Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *on-line* di internet dengan penyelenggara dari Indonesia.

f. Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun *website* porno yang banyak beredar dan mudah diakses di internet.

g. Pasal 282 dan 311 KUHP dapat dikenakan untuk penyebaran foto atau film pribadi seseorang yang vulgar di internet.

h. Pasal 378 dan 262 KUHP dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kredit yang nomor kartu kreditnya merupakan hasil curian.

i. Pasal 406 KUHP dapat dikenakan pada kasus *deface* suatu *website*, karena pelaku setelah berhasil memasuki *website* korban, selanjutnya melakukan pengrusakan dengan cara mengganti tampilan asli dari *website* tersebut.

1. <u>Menurut Peraturan Perndang-undangan di Indonesia</u>

Dalam perkembangannya, telah ada regulasi yang berkaitan dengan kejahatan di bidang teknologi informasi atau telekomunikasi, diantaranya :

a. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi, yang mengancam pidana bagi perbuatan :

   1) tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi (Pasal 22 jo. Pasal 50)

2) menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi (Pasal 38 jo. Pasal 55)
3) menyadap informasi melalui jaringan telekomunikasi (Pasal 40 jo. Pasal 56)

Menurut definisi yang termuat dalam undang-undang telekomunikasi ini, yang dimaksud dengan telekomunikasi ialah setiap pemancaran, pengiriman, dan/atau penerimaan dari setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Perangkat telekomunikasi ialah setiap alat-alat perlengkapan yang digunakan dalam bertelekomunikasi. Dan yang dimaksud dengan jaringan telekomunikasi ialah rangkaian perangkat telekomunikasi dan kelengkapannya yang digunakan dalam bertelekomunikasi. Penyalahgunaan internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan undang-undang ini, terutama bagi para *hacker* yang masuk ke sistem jaringan milik orang lain sebagaimana diatur dalam Pasal 22 Undang-undang Telekomunikasi ini.

b. Undang-undang No.19 Tahun 2002 Tentang Hak Cipta

Menurut Pasal 1 (8) Undang-undang tentang Hak Cipta, program komputer adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut. Dalam Pasal 30 mengatur

mengenai jangka waktu hak cipta untuk program komputer berlaku selama 50 tahun.

2. <u>Menurut Rancangan Peraturan Perundang-undangan di Indonesia</u>

a. Menurut Rancangan Undang-Undang KUHP Buku II Tahun 2005[30]

1) Bagian Kelima Tindak Pidana terhadap Informatika dan Telematika, Paragraf 1 tentang Penggunaan dan Perusakan Informasi Elektronik dan Domain

a) Dipidana dengan pidana penjara paling lama 4 (empat) tahun dan pidana denda paling banyak Kategori IV, setiap orang yang menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan/atau sistem elektronik. (Pasal 373)

b) Dipidana dengan pidana penjara paling lama 1 (satu) dan pidana denda paling banyak Kategori II penyelenggara agen elektronik yang tidak menyediakan fitur pada agen elektronik yang dioperasikannya yang memungkinkan penggunanya melakukan perubahan informasi yang masih dalam proses transaksi. (Pasal 374)

c) Dipidana dengan pidana penjara paling lama 6 (enam) tahun dan pidana denda paling banyak Kategori IV setiap orang yang memiliki dan menggunakan nama domain berdasarkan itikad tidak

[30] www.legalitas.org/database/rancangan/2005/BUKU%20KEDUA%20KUHP, 2005, RUU KUHP Buku II Tindak Pidana, diakses pada tanggal 27 Februari 2008

baik melanggar persaingan usaha tidak sehat dan melanggar hak orang lain. (Pasal 375)

Tindak pidana sebagaimana dimaksud pada Pasal 375 ayat (1) diatas hanya dapat dituntut atas pengaduan dari orang yang terkena tindak pidana.

2) Paragraf 2 tentang Tanpa Hak Mengakses Komputer dan Sistem Elektronik

a) Dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan pidana denda paling banyak Kategori IV setiap orang yang :

(1) menggunakan, mengakses komputer, dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi pertahanan nasional atau hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap negara dan/atau hubungan dengan subjek hukum internasional;

(2) melakukan tindakan yang secara tanpa hak yang menyebabkan transmisi dari program, informasi, kode atau perintah komputer dan/atau sistem elektronik yang dilindungi Negara menjadi rusak;

(3) menggunakan dan/atau mengakses komputer dan/atau sistem elektronik secara tanpa hak atau melampaui wewenangnya, baik dari dalam maupun luar negeri untuk memperoleh informasi dari komputer dan/atau sistem elektronik yang dilindungi oleh negara;

(4) menggunakan dan/atau mengakses komputer dan/atau sistem elektronik milik pemerintah yang dilindungi secara tanpa hak;

(5) menggunakan dan/atau mengakses tanpa hak atau melampaui wewenangnya, komputer dan/atau sistem elektronik yang dilindungi oleh negara, yang mengakibatkan komputer dan/atau sistem elektronik tersebut menjadi rusak;

(6) menggunakan dan/atau mengakses tanpa hak atau melampaui wewenangnya, komputer dan/atau sistem elektronik yang dilindungi oleh masyarakat, yang mengakibatkan komputer dan/atau sistem elektronik tersebut menjadi rusak;

(7) mempengaruhi atau mengakibatkan terganggunya komputer dan/atau sistem elektronik yang digunakan oleh pemerintah;

(8) menyebarkan, memperdagangkan, dan/atau memanfaatkan kode akses (*password*) atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos komputer dan/atau sistem elektronik dengan tujuan menyalahgunakan komputer dan/atau sistem elektronik yang digunakan atau dilindungi oleh pemerintah;

(9) melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun; atau

(10) melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak komputer atau sistem elektronik lainnya

yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun. (Pasal 376)

b) Dipidana dengan pidana penjara paling singkat 3 (tiga) tahun dan paling lama 15 (lima belas) tahun dan pidana denda paling sedikit Kategori IV dan paling banyak Kategori VI, setiap orang yang menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi. (Pasal 377)

c) Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan pidana denda paling banyak Kategori VI, setiap orang yang :

(1) menggunakan dan/atau mengakses komputer dan/atau sistem elektronik secara tanpa hak atau melampaui wewenangnya dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari Bank Sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya;

(2) menggunakan data atau mengakses dengan cara apapun kartu kredit atau kartu pembayaran milik orang lain secara tanpa hak dalam transaksi elektronik untuk memperoleh keuntungan;

(3) menggunakan dan/atau mengakses komputer dan/atau sistem elektronik Bank Sentral, lembaga perbankan dan/atau lembaga

keuangan yang dilindungi secara tanpa hak atau melampaui wewenangnya, dengan maksud menyalahgunakan, dan/atau untuk mendapatkan keuntungan daripadanya; atau

(4) menyebarkan, memperdagangkan, dan/atau memanfaatkan kode akses atau informasi yang serupa dengan hal tersebut yang dapat digunakan menerobos komputer dan/atau sistem elektronik dengan tujuan menyalahgunakan yang akibatnya dapat mempengaruhi sistem elektronik Bank Sentral, lembaga perbankan dan/atau lembaga keuangan, serta perniagaan di dalam dan luar negeri.

3) Paragraf 3 tentang Pornografi Anak melalui Komputer

a) Dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan pidana denda Kategori IV setiap orang yang tanpa hak melakukan tindak pidana yang berkaitan dengan pornografi anak berupa :

(1) memproduksi pornografi anak dengan tujuan untuk didistribusikan melalui sistem komputer;

(2) menyediakan pornografi anak melalui suatu sistem komputer;

(3) mendistribusikan atau mengirimkan pornografi anak melalui sistem komputer;

(4) membeli pornografi anak melalui suatu sistem komputer untuk diri sendiri atau orang lain; atau

(5) memiliki pornografi anak di dalam suatu sistem komputer atau dalam suatu media penyimpanan data komputer. (Pasal 379)

b. Menurut Rancangan Undang - Undang Informasi dan Transaksi Elektronik (RUU ITE)[31]

”RUU ITE merupakan peleburan konsepsi beberapa RUU yang berkaitan dengan Teknologi Informasi, yaitu RUU IETE (RUU Informasi Elektronik dan Transaksi Elektronik), RUU PTI (RUU Pemanfaatan Teknologi Informasi), dan RUU TiPiTI (RUU Tindak Pidana Teknologi Informasi), lalu kemudian menjadi RUU ITE”.[32]

1) BAB VII tentang Perbuatan yang Dilarang

a) Setiap orang dilarang menyebarkan informasi elektronik yang memiliki muatan pornografi dan atau pornoaksi melalui komputer atau sistem elektronik. Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 26, dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan pidana denda paling banyak Rp.1.000.000.000,-. (satu milyar rupiah). (Pasal 26 jo. Pasal 42)

b) Setiap orang dilarang:

(1) menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan atau sistem elektronik. Setiap orang yang melanggar

[31] www.legalitas.org/database/rancangan/2005/RUU_ITE, 14 Juni 2005, Diakses pada tanggal 27 Februari 2008

[32] Edmon Makarim, 12 April 2007, “Tindak Pidana terkait dengan Komputer dan Internet : Suatu Kajian Pidana Materiil dan Formil”, Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia, FHUI, Jakarta

ketentuan sebagaimana dimaksud dalam Pasal 27 ayat (1), dipidana dengan pidana penjara paling lama 4 (empat) tahun dan atau denda paling banyak Rp. 1.000.000.000.,- (satu milyar rupiah). (Pasal 27 jo. Pasal 42)

(2) menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, untuk memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi. Setiap orang yang melanggar Pasal 27 ayat (2), dipidana dengan pidana penjara paling lama 20 (dua puluh) tahun dan atau denda paling banyak Rp.10.000.000.000,- (sepuluh milyar rupiah). (Pasal 27 jo. Pasal 46)

(3) menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, untuk memperoleh, mengubah, merusak, atau menghilangkan informasi pertahanan nasional atau hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap Negara dan atau hubungan dengan subyek Hukum Internasional. Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 27 ayat (3), dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah) (Pasal 27 jo. Pasal 45)

c) Setiap orang dilarang melakukan tindakan yang secara tanpa hak yang menyebabkan transmisi dari program, informasi, kode atau perintah, komputer dan atau sistem elektronik yang dilindungi Negara menjadi rusak. Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 28, dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah).

(Pasal 28 jo. Pasal 45)

d) Setiap orang dilarang menggunakan dan atau mengakses komputer dan atau sistem elektronik secara tanpa hak atau melampaui wewenangnya, baik dari dalam maupun luar negeri untuk memperoleh informasi dari komputer dan atau sistem elektronik yang dilindungi oleh negara. Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 29, dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah).

(Pasal 29 jo. Pasal 45)

e) Setiap orang dilarang:

(1) menggunakan dan atau mengakses komputer dan atau sistem elektronik milik pemerintah yang dilindungi secara tanpa hak;

(2) menggunakan dan atau mengakses tanpa hak atau melampaui wewenangnya, komputer dan atau sistem elektronik yang

dilindungi oleh negara, yang mengakibatkan komputer dan atau sistem elektronik tersebut menjadi rusak;

(3) menggunakan dan atau mengakses tanpa hak atau melampaui wewenangnya, komputer dan atau sistem elektronik yang dilindungi oleh masyarakat, yang mengakibatkan komputer dan atau sistem elektronik tersebut menjadi rusak;

(4) mempengaruhi atau mengakibatkan terganggunya komputer dan atau sistem elektronik yang digunakan oleh pemerintah;

Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 30 ayat (1), Pasal 30 ayat (2), Pasal 30 ayat (3), Pasal 30 ayat (4), dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah). (Pasal 30 jo. Pasal 45)

f) Setiap orang dilarang :

(1) menggunakan dan atau mengakses komputer dan atau sistem elektronik secara tanpa hak atau melampaui wewenangnya untuk memperoleh keuntungan atau memperoleh informasi keuangan dari Bank Sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya. Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 31 ayat (1), dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah).

(Pasal 31 jo. Pasal 47)

(2) Menggunakan dan atau mengakses dengan cara apapun kartu kredit atau kartu pembayaran milik orang lain secara tanpa hak dalam transaksi elektronik untuk memperoleh keuntungan. Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 31 ayat (2), dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah). (Pasal 31 jo. Pasal 47)

g) Setiap orang dilarang menggunakan dan atau mengakses komputer dan atau sistem elektronik Bank Sentral, lembaga perbankan dan atau lembaga keuangan yang dilindungi secara tanpa hak atau melampaui wewenangnya, untuk disalah gunakan, dan atau untuk mendapatkan keuntungan daripadanya. Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 32, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah). (Pasal 32 jo. Pasal 47)

h) Setiap orang dilarang:

(1) menyebarkan, memperdagangkan, dan atau memanfaatkan kode akses *(password)* atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos komputer dan atau sistem elektronik dengan tujuan menyalahgunakan yang akibatnya dapat mempengaruhi sistem elektronik Bank Sentral, lembaga perbankan

dan atau lembaga keuangan, serta perniagaan di dalam dan luar negeri. Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 33 ayat (1), dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah). (Pasal 33 jo Pasal 47)

(2) Menyebarkan, memperdagangkan, dan atau memanfaatkan kode akses *(password)* atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos komputer dan atau sistem elektronik dengan tujuan menyalahgunakan komputer dan atau sistem elektronik yang digunakan atau dilindungi oleh pemerintah.

Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 33 ayat (2), dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah). (Pasal 33 jo. Pasal 45)

i) Setiap orang dilarang melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak komputer atau sistem elektronik lainnya yang dilindungi negara dan berada di wilayah yurisdiksi Indonesia. Setiap orang yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 34 dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan atau denda paling banyak Rp.2.000.000.000.,- (dua milyar rupiah).

(Pasal 34 jo. Pasal 45)

3. <u>Menurut Peraturan Perundang-undangan di Negara Lain</u>

> Secara regional, *cybercrime* mulai diterima sebagai suatu kejahatan transnasional sebagaimana disepakati SOMTC (*Senior Official Meeting On Transnational Crime*) yang diadakan di Singapura pada tanggal 9 sampai 10 Oktober 2001, yang menambahkan dua jenis kejahatan bersifat transnational dari sebelumnya berjumlah 6 (enam) jenis kejahatan sebagaimana disepakati dalam *Meeting of Asean Minister Interior in Manila* (pertemuan menteri dalam negeri ASEAN di Manila) pada tanggal 20 Desember 1997 menjadi 8 (delapan) jenis kejahatan transnasional yaitu : (i) *Illicit drug trafficking* (perdagangan ilegal narkotika dan psikotropika), (ii) *Money laundering* (pencucian uang), (iii) *Terrorism* (terorisme), (iv) *Arms smuggling* (penyelundupan senjata api), (v) *Trafficking in person* (perdagangan manusia), (vi) *Sea piracy* (pembajakan di laut), (vii) *Cybercrime* (kejahatan dunia maya), dan (viii) *International economic crime* (kejahatan ekonomi internasional).[33]

Dalam beberapa literatur, kejahatan dunia maya (*cybercrime*) sering diidentikkan sebagai *computer crime*. *Organization of European Community Development* (OECD), memberikan pengertian kejahatan komputer (*computer crime*) sebagai : "*any illegal, unethical or unauthorized behaviour relating to the automatic processing and/or the transmission of data*".[34] Departemen Kehakiman Amerika memberikan definisi mengenai kejahatan komputer atau penyalahgunaan komputer, antara lain :

> "*…any illegal act requiring knowledge of computer technology for it's perpretation, investigation, or prosecution. It has two main categories. First, computer as a tool of crime, such as found, an theaf property…. Second, computer is the object of crime such sabotage, theaf or alteration data,…….*"[35]

---

[33] Petrus Reinhard Golose, 12 April 2007, *Penegakan Hukum Cyber Crime dalam Sistem Hukum Indonesia* dalam Handout Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia, FHUI, Jakarta, Hlm. 10

[34] Agustus 2006, *Perkembangan Cyber Crime dan Upaya Penanganannya di Indonesia oleh POLRI* dalam Buletin Hukum Perbankan dan Kebanksentaralan Volume 4 Nomor 2, Hlm.34

[35] U.S. Departement of Justice, H.Kadish Sanford ed., Encyclopedia of crime and justice : Volume 1 (New York: The Free Press Division of Macmillan Inc, 1983, Hlm.218, 'Edmon Makarim, 2005, *Pengantar Hukum Telematika*, Rajagrafindo Perkasa, Jakarta, Hlm 426

Dilihat dari definisi yang diberikan oleh Departemen Kehakiman Amerika, penyalahgunaan komputer dibagi atas 2 kategori utama. "Yang pertama, komputer sebagai alat untuk melakukan kejahatan, contoh kasus yang ditemukan adalah pencurian. Dan yang kedua, komputer sebagai objek atau sasaran dari kejahatan, seperti sabotase komputer sehingga tidak berjalan sebagaimana mestinya (*malfunction*), pengubahan atau pencurian data".[36] Sedangkan Eoghan Casey memberikan definisi mengenai kejahatan dunia maya "*Cyber crime is used troughout this text to refer to any crime that involves computer and networks, including crimes that do not rely heavily on computer*".[37] Kemudian, National Police Agency (NPA) juga mengeluarkan pengertian mengenai kejahatan komputer yaitu sebagai berikut : "*Computer crime is crime toward to computer*".[38] NPA memberikan pengertian yang lebih luas dan tidak memberikan batasan, yaitu kejahatan komputer yang berkaitan dengan komputer, dapat berupa kejahatan dengan menggunakan komputer, atau kejahatan terhadap komputer.

a. Belanda

Di Belanda, dibentuk suatu komisi yang disebut komisi Franken yang bertugas memberi masukan mengenai pengaturan kejahatan mayantara. Adapun usulan komisi Franken adalah kejahatan mayantara dimasukkan dalam KUHP Belanda melalui amandemen KUHP Belanda dengan memasukkannya pada ketentuan pidana tertentu. Selanjutnya komisi

[36] terjemahan bebas penulis
[37] Eoughan Casey, Digital Evidence and Computer Crime, 2001, London : A Harcourt Science and Technology Company, page 16, '*Op.Cit*, Hlm. 35'
[38] Edmon Makarim, 2005, *Pengantar Hukum Telematika*, Rajagrafindo Perkasa, Jakarta, Hlm. 427

Franken mengajukan 18 usulan dalam perumusan KUHP Belanda diantaranya yaitu (Eddy Djunaedi Karnasudirja, 1993) :

1) Usulan 1, merupakan peraturan baru sebagai perluasan Pasal 161 bis Sr yang mengatur menghancurkan, merusak, atau menjadikan tidak dapat dipakai lagi, menyebabkan terganggunya jalannya atau bekerjanya pekerjaan atau menghalangi tindakan pengamanan suatu alat yang diotomatisasikan untuk menyimpan atau penggolongan data atau untuk telekomunikasi.
2) Usulan 2, peraturan baru untuk melindungi alat yang dikomputerisasikan untuk penyimpanan data/atau untuk telekomunikasi.
3) Usulan 3, penyempurnaan Pasal 351 Sr menghancurkan, merusak, atau membuat tidak dapat berfungsi lagi peralatan yang diotomatisasikan untuk meyimpan atau mengolah data/atau untuk telekomunikasi.
4) Usulan 4, berkaitan dengan perubahan data dari peralatan yang diotomatisasi.
5) Usulan 6, Amandemen Pasal 139e Sr dimaksudkan untuk dapat menghukum mereka yang berusaha menyadap data dengan alat khusus.

b. Australia

Didalam ***Criminal Code Act* 1995** yang diamandemen oleh *Federal Legislation THE CYBER-CRIME ACT* 2001, pengaturan *computer crime* sebagai *unauthorized access to computer system*.[39]

[39] Stein Schjolberg, Chief Judge Moss District Court, Norway, ***THE LEGAL FRAMEWORK-***

478.1 Criminal Code Act 1995 ayat (1) *A person is guilty of an offence if : the person causes any unauthorized access to, or modification of, restricted data; and the persons intends to cause the access or modification; and the person knows that the access or modification is unauthorized*. Yaitu, setiap orang dinyatakan bersalah apabila dengan sengaja dan melawan hukum mengakses tanpa hak dan/atau memodifikasi data yang terdapat dalam sistem komputer, dan orang tersebut mengetahui bahwa tindakan mengakses atau memodifikasi itu tidak sah dan melawan hukum. *Restricted data* (data yang terlarang) ialah data yang berada didalam komputer.[40]

c. Jerman

Dalam ***Penal Code Section 202.a. Data Espionage*** :

1) *Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access shall be liable to imprisonment for a term not exceeding three years or to a fine.*

Penal Code Section 303b Computer Sabotage *:*

1) *Imprisonment not exceeding five years or a fine shall be imposed on any person who interferes with data processing which is of essential importance to another business, another's enterprise or an*

UNAUTHORIZED ACCESS TO COMPUTER SYSTEMS PENAL LEGISLATION IN 44 COUNTRIES (update April,7,2003) dalam 'Barda Nawawi Arief, 2005, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*, Citra Aditya Bakti, Bandung, Hlm. 147

[40] Terjemahan bebas penulis

*administrative authority by destroying, damaging, rendering useless, removing, or altering a computer system or a data carrie*r.[41]

B. Modus operandi kejahatan dunia maya (*cyber crime*)

1. *Hacking (unauthorized access to computer system and service)*

"*Hacking* didefinisikan sebagai suatu kejahatan yang dilakukan dengan cara memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya".[42] *Hacking* dapat dijelaskan sebagai suatu perilaku obsesif dan/atau tanpa otorisasi yang sah (*unauthorized access*) dalam menggunakan komputer atau sistem jaringan komputer dan pelakunya disebut dengan istilah *hacker*. Pada awalnya beberapa orang mahasiswa yang berasal dari *Massachusets Institute of Technology* (MIT) Amerika melakukan eksperimen dengan menggunakan komputer institutnya. Mereka melakukan penyusupan-penyusupan dalam menggunakan komputer dengan maksud agar penggunaan komputer tersebut dapat dilakukan kapan dan dimana saja. Para mahasiswa tersebut membuat program yang bertujuan mengoptimalkan fungsi dan kerja komputer. Selain membuat program, mereka juga bekerja dalam pembuatan proyek MAC (*Multiple Access Computer*). Pada saat inilah pertama kali istilah "*hacker*" digunakan. Istilah ini berawal dari kata "*hack*" yang saat itu artinya "teknik pemrograman kreatif yang mampu memecahkan

[41] Barda Nawawi, *op.cit*, Hlm. 152
[42] Hinca IP Panjaitan, 2005, *Membangun Cyber Law Indonesia yang Demokratis*, IMLPC, Jakarta, 'Buletin Hukum Perbankan dan Kesentralan, Hlm. 35'

masalah secara jauh dan lebih efisien dari teknik biasa". Saat itu, sebuah tindakan "*computer hacking*" sangat bermanfaat karena dapat meningkatkan kemampuan program dan lebih hemat. Kemudian, sejalan dengan perkembangan teknologi komputer dan pesatnya pertumbuhan jaringan internet, mendorong meningkatnya pertumbuhan para hacker. Khususnya di tahun 90-an, dimana internet telah berkembang dengan pesat. "Beberapa tahap *hacking* yang dapat dikonstruksikan sebagai kejahatan meliputi :"[43]

a. mengumpulkan dan mempelajari informasi yang ada mengenai sistem operasi komputer atau jaringan komputer yang dipakai pada target sasaran
b. menyusup atau mengakses jaringan komputer target sasaran
c. menjelajahi sistem komputer dan mencari akses yang lebih tinggi
d. membuat *backdoor* dan menghilangkan jejak

"Seorang *hacker* meyakini bahwa komputer dan jaringan komputer merupakan wahana untuk melakukan tindakan atau perbuatan kreatif sekaligus dapat mengubah kehidupan ini menjadi lebih baik".[44]

2. *Cracking*

Cracking adalah sisi gelap dari *hacker* dan memiliki ketertarikan untuk mencuri informasi, melakukan berbagai macam kerusakan dan sesekali waktu juga melumpuhkan keseluruhan sistem komputer. "*Hacker* ilegal, yang kerap mencuri dan/atau merusak data atau program, disebut dengan istilah *cracker*".[45]

---

[43]Agus Raharjo, 2002, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung, Hlm. 175

[44]*Ibid*, Hlm. 175

[45]James O'Brian, 1999, *Management Information System*, McGraw-Hill, Hlm. 21, 'Donny Budi Utoyo, *Kajian Sosial Komunitas Maya Hacker/Cracker dalam "Jurnal Hukum Teknologi*", volume 2 nomor 1 tahun 2005, LKHT FH UI, Depok, Hlm. 48

Para *hacker* jahat (*cracker*) membentuk komunitasnya sendiri (*cyber community*), dimana mereka sering menunjukkan keahlian mereka, bahkan sering juga disertai dengan tindakan-tindakan yang merugikan. "Seperti kerusakan sistem komputer, hilangnya seluruh data didalam komputer, tidak berfungsinya *search engine*; seperti yahoo, CNN yang sempat terhenti beberapa hari, dan tentunya kerugian dari segi ekonomi".[46] Salah satu aktifitas *cracking* yang paling dikenal adalah pembajakan situs *web* dan kemudian mengganti tampilan halaman mukanya. Tindakan ini biasa dikenal dengan istilah *deface*. Sebagai salah satu contoh kasus *deface*, tersangka perusakan situs Golkar, *www.golkar.or.id*, yakni Tersangka Iqra Syafaat (27) hanya lulusan SMU yang kerap berjualan buku elektronik (*e-book*), diringkus polisi dari unit *Cyber Crime* Mabes Polri di warung elektronik Balerang di Jalan Raden Patah Nomor 81 Batam pada 2 Agustus 2006. Penyerangan situs Golkar itu dilakukan pada tanggal 9-13 Juli 2006. Situs Golkar selama kurun waktu tersebut telah diserang 1.257 kali dari 31 lokasi yang tercatat di *Internet Protocol Address* (*IP Address*) dari sejumlah kota seperti Jakarta, Bekasi, Bandung, Surabaya, Lampung, Palembang, Medan, dan Batam. Selain itu, berdasarkan *IP Address* yang tercatat, penyerangan juga terhubung dengan *hacker* asing dari luar negeri seperti Malaysia, Amerika Serikat, Brazil, Turki, dan Rumania. Namun, yang disidik polisi terkait perusakan dengan pola yang dilakukan Iqra. Menurut Kepala Unit *Information Technology and Cyber Crime* Direktorat Ekonomi dan Khusus Badan Reserse Kriminal Mabes Polri Komisaris Besar Petrus Reinhard

[46] www.lkhtnet.com, 31 Juli 2004, *Kejahatan dan Komputer*, LKHT FH UI, Depok, diakses pada tanggal 28 Februari 2007

Golose, serangan (*deface*) pertama kali terjadi pada 9 Juli 2006. Iqra mengganti foto beberapa tokoh Golkar menjadi foto gorila putih tersenyum. Serangan berikutnya pada 10 Juli 2006, halaman muka situs Golkar diisi dengan foto mesum aktris *Hollywood* dengan tulisan "bersatu untuk malu". Kerugian materiil yang ditimbulkan dari perusakan situs Golkar itu sekitar Rp 150 juta. Ketua DPP Golkar Muladi mencium adanya motivasi politik dibalik kejahatan dunia maya tersebut, "Sebab ada upaya mendelegitimasi dan menjelekkan Golkar. Apalagi dilakukan dari berbagai kota," ujar Muladi, usai jumpa pers di Mabes Polri, Senin (7/8). Dan Polisi masih menyidik kemungkinan motivasi tersebut.

3. *Joycomputing*

Joycomputing merupakan salah satu modus operandi kejahatan dunia maya dimana pelaku secara tidak sah mencuri *service* atau mencuri waktu dalam penggunaan komputer/internet untuk kepentingan tertentu, seperti iseng, main-main, atau merusak sistem. *Joycomputing* terilhami dari kasus yang terjadi di negara Belanda, yang memidana pelaku yang mengambil mobil milik orang lain untuk bersenang-senang, tanpa niat untuk memiliki mobil tersebut (*joyriding*). *Joycomputing* dianalogikan seperti *joyriding*, namun objeknya merupakan sistem/jaringan dari suatu komputer yang diakses secara tidak sah atau tanpa izin di dalam dunia maya (*cyberspace*). Muladi, guru besar Fakultas Hukum UNDIP Semarang menyatakan bahwa pelaku tindak pidana komputer dalam melakukan perbuatannya semata-mata bukan hanya profit, melainkan bagaimana dapat mengakali (*outsmart*) suatu sistem komputer dan

melakukannya untuk kesenangan semata. ”Profil ini merupakan profil pelaku kejahatan dunia maya *joycomputing* yang bertujuan untuk kesenangan semata”.[47]

4. *Carding*

”Menurut Setiadi, secara definitif *carding* dapat didefinisikan sebagai tindakan penggunaan kartu kredit yang dilakukan oleh orang yang tidak seharusnya menggunakan kartu kredit tersebut untuk melakukan transaksi melalui internet”.[48] Secara terminologi, *carding* berasal dari Bahasa Inggris, yaitu *card* (kartu). Para pakar teknologi informasi memberikan label kepada para pelaku penyalahgunaan kartu kredit dengan sebutan *carder* yang sampai sekarang istilah itu masih digunakan kepada mereka. ”Sekarang yang menurut Bahasa Inggris, yang lazim digunakan adalah *credit card fraud* atau dalam istilah Bahasa Indonesia adalah penipuan kartu kredit, yang diartikan sebagai penggunaan kartu kredit yang dilakukan oleh orang yang tidak seharusnya menggunakan kartu kredit tersebut untuk melakukan transaksi melalui internet”.[49] Menurut Thom Mrozek (*United States Attorny Central District Of California*), “*Carding is a term used by hackers to describe the use of stolen credit card information to purchase items or services*”.[50]

---

[47]Widyopramono Hadiwidjojo, *Cybercrime dan pencegahannya* dalam Jurnal Hukum Teknologi, volume 2 nomor 1 tahun 2005, LKHT FH UI, Depok, Hlm. 10
[48]Setiadi, *Penegakan Hukum Terhadap Pelaku Tindak Pidana Internet Banking* dalam Jurnal Hukum Teknologi, volume 2 nomor 1 tahun 2005, LKHT FH UI, Depok, Hlm. 19
[49]*Ibid*, Hlm. 20
[50]Ade Ary Syam Indradi, 2006, *Carding Modus Operandi, Penyidikan, dan Penindakan*, Pensil-324, Jakarta, Hlm. 35

Dalam beberapa kasus yang diungkap Polri, perkembangan modus operandi *carding* atau melakukan penipuan/penyalahgunaan kartu kredit melalui internet, adalah sebagai berikut[51] :

a. Modus I (1996-1998), para *carder* mengirimkan barang hasil *carding* mereka langsung ke suatu alamat di Indonesia.
b. Modus II (1998-2000), para *carder* tidak lagi secara langsung menuliskan "Indonesia" pada alamat pengiriman, tetapi menuliskan nama negara lain. Kantor pos negara lain tersebut akan meneruskan kiriman yang 'salah tujuan' tersebut ke Indonesia. Hal ini dilakukan para *carder* karena semakin banyak *merchant* atau perusahaan penyedia *e-commerce* di internet yang menolak mengirim produknya ke Indonesia.
c. Modus III (2000-2002), para *carder* mengirimkan paket pesanan mereka ke rekan mereka yang berada di luar negeri. Kemudian rekan mereka tersebut akan mengirimkan kembali paket pesanan tersebut ke Indonesia secara normal dan legal. Hal ini dilakukan oleh *carder* selain karena modus operandi mereka mulai tercium oleh aparat penegak hukum, juga disebabkan semakin sulitnya mencari *merchant* yang bisa mengirim produknya ke Indonesia.
d. Modus IV (2002-sekarang), para *carder* lebih mengutamakan mendapatkan uang tunai. Caranya adalah dengan mentransfer sejumlah dana dari kartu kredit bajakan ke sebuah rekening di *www.PayPal.com*, kemudian dari PayPal, dana yang telah terkumpul tersebut mereka kirimkan ke rekening bank yang mereka tunjuk. "Cara lainnya adalah dengan melakukan penipuan, seolah-olah mereka menjual barang hasil *carding*, dan menjebak korban dengan meminta mengirimkan uang muka dalam jumlah tertentu kepada mereka". Namun, masih terdapat juga para *carder* yang kerap menggunakan modus operandi I sampai dengan III, terutama bagi *carder* pemula.

Jenis kejahatan ini (*carding*), bila ditinjau dari segi sasarannya termasuk bentuk *cyber crime against property* atau jenis *cybercrime* yang sasarannya properti milik seseorang. Sedangkan dari modus operandinya, tergolong dalam *computer facilitated crime*, yaitu pola kejahatan umum yang menggunakan komputer dalam aksinya. "Motif *carding* adalah pemenuhan keuntungan material berupa barang atau uang".[52]

---

[51] Setiadi , *OpCit*, Hlm. 22
[52] Ade Ary Syam Indradi, 2006, *Carding Modus Operandi, Penyidikan, dan Penindakan*, Pensil-324, Jakarta, Hlm. 36

Kejahatan teknologi informasi di dunia maya mencakup segala aspek dari kehidupan manusia termasuk kejahatan tradisional yang terdapat dalam KUHP namun dilakukan secara elektronik, "*Information technology touches every aspect of human life an so can electronically enabled crime*".[53] Dilihat dari keterangan diatas diketahui adanya modus operandi yang dilakukan pelaku kejahatan dunia maya melalui suatu proses elektronik dimana objek dari kejahatan dunia maya tersebut berubah, barang menjadi data elektronik. Sehingga bukti yang diperoleh pun bersifat elektronik. Pengertian data elektronik akan ditinjau secara umum di bawah ini.

C. Tinjauan umum data elektronik

1. Pengertian data elektronik

Menurut Turban, Rainer, dan Potter, "***Data*** *are raw facts or elementary description of things, events, activities, and transactions that are captured, recorded, stored, and classified, but not organized to convey any specific meaning. Example of data would include bank ballances"*. [54] "Data ialah gambaran dasar, fakta-fakta awal yang belum terperinci dari perihal, peristiwa, kegiatan, dan transaksi yang ditangkap, direkam, disimpan, dan terklasifikasi

[53] Information Technology Association of Canada (ITAC), IIIC Common Views Paper On : Cyber Crime, IIIC 2000 Millenium Congress, September 19th.,2002,p.2 'Barda Nawawi, 2005, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*, Citra Aditya Bakti, Bandung, Hlm. 136'

[54] Turban,Rainer, dan Potter.,*Introduction to Information Technology* 'Edmon Makarim, *Kompilasi Hukum Telematika* Hlm. 31, Jakarta

tetapi tidak terorganisir untuk dapat menyatakan arti khusus apapun. Contoh data ialah catatan saldo rekening bank".[55]

Sedangkan pengertian informasi menurut Turban, Rainer, dan Potter, "***Information*** *is a collection of facts organized in some manner so that they are meaningful to a recipient. For example, if we include costumer names with bank ballances, we would have useful information*". [56] "Informasi ialah kumpulan dari fakta (data) yang terorganisir dalam suatu bentuk atau cara sehingga dapat berarti bagi penerimanya. Contoh informasi ialah saldo rekening bank yang disertai dengan identitas pemegang rekening".[57] Dengan kata lain, informasi bersumber dari data yang telah diproses. Informasi elektronik dapat berupa catatan elektronik, data atau dokumen elektronik, surat elektronik, ataupun tanda tangan elektronik. Suatu data/informasi yang telah diolah oleh sistem informasi secara elektronik tersebut, akan tersimpan didalam suatu media tertentu secara elektronik, yang dinamakan dokumen elektronik. Sistem penyimpanan data/atau informasi elektronik yang berbasiskan komputer dinamakan *Databases* dan data yang dikomunikasikan melalui media telekomunikasi dinamakan *Data Messages*. *"Data messages* inilah yang menjadi landasan utama terbentuknya suatu kontrak elektronik, baik dalam hubungannya dengan kesepakatan mengenai persyaratan-persyaratan dan ketentuan-ketentuan kontrak (*terms and conditions*) ataupun

[55] terjemahan bebas penulis
[56] *Ibid,* Hlm. 31
[57] terjemahan bebas penulis

yang berkaitan dengan substansi kontrak itu sendiri."[58] Sejauh ini telah ada beberapa teknik yang ditawarkan dan dianggap cukup mampu untuk memberikan jaminan keautentikan dan integritas dari suatu *data messages*. Teknik yang dimaksud ialah teknik kriptografi (*cryptography*) yaitu suatu teknik pengamanan serta penjaminan keautentikan data yang terdiri dari dua proses, yaitu yang pertama enkripsi (*encryption* : proses yang dilakukan untuk membuat suatu data menjadi tidak terbaca oleh pihak yang tidak berhak karena data-data tersebut telah dikonversikan kedalam bahasa sansi atau kode-kode tertentu) dan yang kedua dekripsi (*decryption*) yang merupakan kebalikan dari enkripsi, yaitu proses menjadikan informasi atau data yang telah di-enkripsi tersebut menjadi dapat terbaca oleh pihak yang berhak. "Dalam metode kriptografi konvensional, enkripsi dan dekripsi biasanya dilakukan dengan menggunakan pasangan kunci tertentu yang disebut dengan kunci pribadi yang bersifat personal dan rahasia (*private key*) dan kunci umum (*public key*)[59] Dalam praktek bisnis, keberadaan dokumen elektronik ini menjadi satu konsekuensi dengan perkembangan teknologi.[60]

> *Standard Working Group on Digital Evidence* (SWGDE) mendefinisikan bukti elektronik sebagai semua informasi yang memiliki nilai pembuktian yang kuat yang disimpan dan ditransmisikan dalam bentuk sinyal-sinyal listrik digital. Maka dari itu, data yang sesuai dengan definisi ini biasanya adalah berupa kumpulan logika-logika digital yang membentuk sebuah informasi, termasuk teks-teks dokumen, video, audio, *file* gambar, alamat-alamat komunikasi digital.[61]

---

[58] M.Arsyad Sanusi, 2005, *Hukum dan Teknologi Informasi*, Tim KemasBuku, Jakarta, Hlm. 204-205

[59] M.Arsyad Sanusi, *op.cit*, Hlm. 205

[60] Rapin Mudiardjo, *Data Elektronik sebagai Alat Bukti Masih Dipertanyakan*, www.hukumonline.com, 8 Juli 2002, diakses pada tanggal 28 Februari 2007

[61] Search Engine : *Digital Evidence*, diakses pada tanggal 18 April 2007

2. Klasifikasi Bukti Elektronik

"Hakim Mohammed Chawki dari *Computer Crime Research Center* mengklasifikasikan bukti elektronik menjadi tiga kategori, sebagai berikut" : [62]

a. *Real Evidence*

Real Evidence atau *Physical Evidence* ialah bukti yang terdiri dari objek-objek nyata/berwujud yang dapat dilihat dan disentuh. "*Real evidence* juga merupakan bukti langsung berupa rekaman otomatis yang dihasilkan oleh komputer itu sendiri dengan menjalankan *software* dan *receipt* dari informasi yang diperoleh dari alat (*device*) yang lain, contohnya *computer log files*".[63]

> Edmon Makarim mengemukakan bukti elektronik sebagai suatu alat bukti yang sah dan yang berdiri sendiri (*real evidence*), tentunya harus dapat diberikan jaminan bahwa suatu rekaman/salinan data (*data recording*) berjalan sesuai dengan prosedur yang berlaku (telah dikalibrasi dan diprogram) sedemikian rupa sehingga hasil *print out* suatu data dapat diterima dalam pembuktian suatu kasus."[64]

b. *Testamentary Evidence*

Testamentary Evidence juga dikenal dengan istilah *Hearsay Evidence* dimana keterangan dari saksi maupun *expert witness* yaitu keterangan dari seorang ahli dapat diberikan selama persidangan, berdasarkan pengalaman dan pengamatan individu. "Peranan dari keterangan ahli sesuai dengan peraturan perundang-undangan kita yaitu UU No.8 Tahun 1981 KUHAP, bahwa keterangan ahli dinilai sebagai alat bukti yang mempunyai kekuatan pembuktian jika keterangan yang diberikan tentang sesuatu hal berdasarkan

---

[62] *Judge* Mohammed Chawki, 10 Maret 2004, Source : *Computer Crime Research Center*, "*The Digital Evidence in The Information Era*", diakses pada tanggal 2 April 2007

[63] Edmon Makarim, 12 April 2007, "Tindak Pidana terkait dengan Komputer dan Internet : Suatu Kajian Pidana Materiil dan Formil", *Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia*, FHUI, Jakarta

[64] Hasil wawancara dengan Edmon Makarim pada tanggal 15 Maret 2007 di FHUI Jakarta

keahlian khusus dalam bidang yang dimilikinya dan yang berupa keterangan "menurut pengetahuannya" secara murni".[65] "Perkembangan ilmu dan teknologi sedikit banyak membawa dampak terhadap kualitas metode kejahatan, memaksa kita untuk mengimbanginya dengan kualitas dan metode pembuktian yang memerlukan pengetahuan dan keahlian (*skill and knowledge*)".[66] Kedudukan seorang ahli dalam memperjelas tindak pidana yang terjadi serta menerangkan atau menjelaskan bukti elektronik sangat penting dalam memberikan keyakinan hakim dalam memutus perkara kejahatan dunia maya.

c. *Circumstantial Evidence*

"Pengertian dari *Circumstantial Evidence* ini adalah merupakan Bukti terperinci yang diperoleh berdasarkan ucapan atau pengamatan dari kejadian yang sebenarnya yang mendorong untuk mendukung suatu kesimpulan, tetapi bukan untuk membuktikannya. *Circumstantial evidence* atau *derived evidence* ini merupakan kombinasi dari *real evidence* dan *hearsay evidence*".[67]

D. Pengaturan mengenai data elektronik

1. Pengaturan data elektronik dalam peraturan perundang-undangan di Indonesia

---

[65] M.Yahya Harahap, 2006, *Pembahasan Pernasalahan dan Penerapan Hukum Edisi Kedua*, Sinar Grafika, Jakarta, Hlm. 301

[66] M.Yahya Harahap, *op.cit*, Hlm. 297

[67] Edmon Makarim, 12 April 2007, "Tindak Pidana terkait dengan Komputer dan Internet : Suatu Kajian Pidana Materiil dan Formil*", Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia*, FHUI, Jakarta

a. Undang - Undang No. 8 tahun 1997 tentang Dokumen Perusahaan

Dengan dikeluarkannya Undang-undang No.8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan, Pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan). ”Misalnya *Compact Disk – Read Only Memory* (CD-ROM), dan *Write-Once–Read–Many* (WORM), yang diatur dalam Pasal 12 UU tentang Dokumen Perusahaan tersebut sebagai alat bukti yang sah”.[68]

b. Undang-Undang No. 20 Tahun 2001 tentang Perubahan Atas Undang-Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi

Berdasarkan Undang-Undang No. 20 Tahun 2001 tentang Perubahan Atas Undang-Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi, adanya perluasan mengenai sumber perolehan alat bukti yang sah berupa petunjuk. Berdasarkan KUHAP, alat bukti petunjuk hanya dapat diperoleh dari keterangan saksi, surat, dan keterangan terdakwa. Tetapi, menurut Undang-Undang No. 20 Tahun 2001, bukti petunjuk juga dapat diperoleh dari alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan

[68] Petrus Reinhard Golose, 12 April 2007, “Penegakan Hukum Cyber Crime dalam Sistem Hukum Indonesia”, *Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia*, FHUI, Jakarta, Hlm. 23

alat optik atau yang serupa dengan itu tetapi tidak terbatas pada data penghubung elektronik (*electronic data interchange*), surat elektronik (*e-mail*), telegram, teleks, faksimili, dan dari dokumen, yakni setiap rekaman data atau informasi yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna.

c. Undang-Undang No. 25 Tahun 2003 tentang Pencucian Uang

Menurut *Report on Money Laundering and Terrorist Financing Typologies* 2003-2004 yang dikeluarkan oleh *Financial Acton Task Force on Money Laundering* (FATF), salah satu tipologi *money laundering* adalah melalui sistem *wire transfer*. *Wire Transfer* disini merujuk pada setiap transaksi keuangan yang dilakukan oleh seseorang melalui sebuah institusi keuangan dengan menggunakan perangkat elektronik yang menyediakan sejumlah uang untuk seseorang di institusi keuangan lain. *Wire Transfer* meliputi pula transaksi keuangan yang terjadi melewati batas nasional, antara satu negara dengan negara lainnya. Undang-undang *money laundering* ini merupakan undang-undang yang paling ampuh bagi seseorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab

penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam Pasal 2 angka (1q) Undang-undang pencucian uang. [69] Undang-undang ini mengatur juga mengenai alat bukti elektronik atau *digital evidence* sesuai dengan Pasal 38 huruf (b), yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

d. Undang - Undang No. 21 tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang

"Dalam Pasal 29 Undang-Undang No. 21 tahun 2007 tentang Perdagangan Orang ini mengatur mengenai alat bukti selain sebagaimana ditentukan dalam Undang-Undang Hukum Acara Pidana, dapat pula berupa" :[70]

1) informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu;dan
2) data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tidak terbatas pada :
   a) tulisan, suara atau gambar;
   b) peta, rancangan, foto atau sejenisnya;

[69] Petrus Reinhard Golose, *op.cit*, Hlm. 23
[70] www.legalitas.org/incl-php/buka.php?d=2000+7&f=uu21-2007, UU Perdagangan Orang, diakses pada tanggal 27 Februari 2008

c) huruf, tanda, angka, simbol atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.

BAB III

TINJAUAN ASPEK PEMBUKTIAN DALAM PERKARA PIDANA DI INDONESIA

A. Teori Pembuktian

"Menurut Pitlo, pembuktian adalah suatu cara yang dilakukan oleh suatu pihak atas fakta dan hak yang berhubungan dengan kepentingannya".[71] "Menurut Subekti, yang dimaksudkan dengan "membuktikan" adalah meyakinkan hakim tentang kebenaran dalil ataupun dalil-dalil yang dikemukakan oleh para pihak dalam suatu persengketaan".[72] "Pembuktian tentang benar tidaknya terdakwa melakukan perbuatan yang didakwakan, merupakan bagian yang terpenting dalam hukum acara pidana".[73] Membuktikan berarti memberi kepastian kepada hakim tentang adanya peristiwa-peristiwa tertentu.

> Adapun enam butir pokok yang menjadi alat ukur dalam teori pembuktian, dapat diuraikan sebagai berikut[74] :
>
> 1. Dasar pembuktian yang tersimpul dalam pertimbangan keputusan pengadilan untuk memperoleh fakta-fakta yang benar (*bewijsgronden*)
> 2. Alat-alat bukti yang dapat digunakan oleh hakim untuk mendapatkan gambaran mengenai terjadinya perbuatan pidana yang sudah lampau (*bewijsmiddelen*)
> 3. Penguraian bagaimana cara menyampaikan alat-alat bukti kepada hakim di sidang pengadilan (*bewijsvoering*)
> 4. Kekuatan pembuktian dalam masing-masing alat-alat bukti dalam rangkaian penilaian terbuktinya suatu dakwaan (*bewijskracht*)
> 5. Beban pembuktian yang diwajibkan oleh undang-undang untuk membuktikan tentang dakwaan di muka sidang pengadilan (*bewijslast*)

---

[71] Edmon Makarim, 2003, *Kompilasi Hukum Telematika*, Rajagrafindo Persada, Jakarta, Hlm. 417
[72] Subekti, 1995, *Hukum Pembuktian*, Pradnya Paramita, Jakarta, Hlm. 1
[73] Andi Hamzah, 2005, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, Hlm. 245
[74] Bambang Poernomo, *Pokok-pokok Tata Cara Peradilan Indonesia*, Liberty, Jogjakarta, Hlm.39

6. Bukti minimum yang diperlukan dalam pembuktian untuk mengikat kebebasan hakim (*bewijsminimum*)

"Dalam hukum pembuktian dikenal istilah *notoire feiten notorious* (*generally known*) yang berarti setiap hal yang "sudah umum diketahui" tidak lagi perlu dibuktikan dalam pemeriksaan sidang pengadilan".[75] Hal ini tercantum dalam Pasal 184 ayat (2) yang berbunyi, "hal yang secara umum diketahui tidak perlu dibuktikan". "Menurut Yahya Harahap, mengenai pengertian "hal yang secara umum sudah diketahui" ditinjau dari segi hukum, tiada lain daripada "perihal" atau "keadaan tertentu" atau *omstandigheiden* atau *circumstances*, yang sudah sedemikian mestinya atau kesimpulan atau resultan yang menimbulkan akibat yang pasti demikian".[76]

B. Sistem Pembuktian

Pada hakekatnya, pembuktian dimulai sejak adanya suatu peristiwa hukum. Apabila ada unsur-unsur pidana (bukti awal telah terjadinya tindak pidana) maka barulah dari proses tersebut dilakukan penyelidikan (serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyelidikan menurut cara yang diatur dalam undang-undang ini), dan dalam Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian dalam pasal 1 angka 13, penyidikan ialah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang

[75] M.Yahya Harahap, Yahya Harahap, 2006, *Pembahasan Permasalahan dan Penerapan KUHAP,* Sinar Grafika, Jakarta, Hlm. 276
[76] *Ibid*, Hlm. 276

dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya. "Menurut M.Yahya Harahap, pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang membuktikan kesalahan yang didakwakan kepada terdakwa".[77]

Ilmu pengetahuan hukum, mengenal empat sistem pembuktian, yang akan diuraikan sebagai berikut :

1. **Pembuktian Berdasarkan Keyakinan Hakim Belaka (*Conviction in Time*)**

   Suatu sistem pembuktian yang bersifat subjektif, yakni untuk menentukan bersalah atau tidaknya terdakwa hanya berdasarkan keyakinan hakim semata. Putusan hakim tidak didasarkan kepada alat-alat bukti yang diatur oleh undang-undang, hakim hanya mengikuti hati nuraninya saja. Keyakinan hakim dapat diperoleh dan disimpulkan hakim dari alat-alat bukti yang diperiksanya dalam sidang pengadilan. Hakim dapat juga mengabaikan hasil pemeriksaan alat-alat bukti itu, dan langsung menarik keyakinan dari keterangan atau pengakuan terdakwa. Sistem ini seolah-olah menyerahkan sepenuhnya nasib terdakwa kepada keyakinan hakim sepenuhnya. "Menurut Yahya Harahap, keyakinan hakimlah yang menentukan wujud kebenaran sejati dalam sistem pembuktian ini".[78] Menurut Andi Hamzah, sistem pembuktian ini dianut oleh peradilan *jury* di Perancis. "Praktek peradilan *jury* di Perancis membuat pertimbangan

[77] M. Yahya Harahap, o*p.cit*, Hlm. 273
[78] Yahya Harahap, 1988 dan 1993, *Pembahasan Permasalahan dan Penerapan KUHAP Jilid I dan II*, *Pustaka Kartini*, Jakarta, Hlm. 797-798

berdasarkan metode ini dan mengakibatkan banyaknya putusan yang aneh".[79] "Wirjono Prodjodikoro mengatakan bahwa sistem pembuktian ini pernah dianut di Indonesia, yaitu pada pengadilan distrik dan pengadilan kabupaten. Sistem ini memungkinkan hakim menyebut apa saja yang menjadi dasar keyakinannya, misalnya keterangan dukun".[80]

2. Sistem Pembuktian Berdasarkan Undang-Undang Secara Positif (*Positief Wettelijk Bewijstheorie*)

"Suatu sistem pembuktian yang berkembang pada zaman pertengahan yang ditujukan untuk menentukan bersalah atau tidaknya terdakwa harus berpedoman pada prinsip pembuktian dengan alat-alat bukti yang ditentukan undang-undang". [81] Sistem ini berbanding terbalik dengan *Conviction in Time*, dimana keyakinan hakim disampingkan dalam sistem ini. Menurut sistem ini, undang-undang menetapkan secara limitatif alat-alat bukti yang mana yang boleh dipakai hakim. Jika alat-alat bukti tersebut telah dipakai secara sah seperti yang ditetapkan oleh undang-undang, maka hakim harus menetapkan keadaan sah terbukti, meskipun hakim ternyata berkeyakinan bahwa yang harus dianggap terbukti itu tidak benar. Menurut D. Simmon, sistem ini berusaha untuk menyingkirkan semua pertimbangan subjektif hakim dan mengikat hakim dengan peraturan pembuktian yang keras. "Sistem ini disebut juga dengan teori pembuktian formal (*formele bewijstheorie*)".[82] "Teori ini ditolak oleh Wirjono Prodjodikoro untuk dianut di Indonesia, karena katanya bagaimana hakim dapat

[79] Andi Hamzah, 1985, *Pengantar Hukum Acara Pidana Indonesia*, Ghalia, Jakarta, Hlm. 230-231
[80] Muhammad Taufik Makarao dan Suhasril, 2004, *Hukum Acara Pidana dalam teori dan praktek*, Ghalia Indonesia, Jakarta, Hlm. 104
[81] Edmon Makarim, 2003, *Kompilasi Hukum Telematika*, Rajagrafindo Persada, Jakarta, Hlm. 421
[82] Andi Hamzah, 2005, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta Hlm. 247

menetapkan kebenaran selain dengan cara menyatakan kepada keyakinannya tentang hal kebenaran itu, lagipula keyakinan seorang hakim yang jujur dan berpengalaman mungkin sekali adalah sesuai dengan keyakinan masyarakat".[83]

3. Sistem Pembuktian Berdasarkan Keyakinan Hakim atas Alasan yang Logis (*La Conviction Raisonee*)

Menurut sistem pembuktian ini, hakim memegang peranan yang penting disini. Hakim baru dapat menghukum seorang terdakwa apabila ia telah meyakini bahwa perbuatan yang bersangkutan terbukti kebenarannya. Keyakinan tersebut harus disertai dengan alasan-alasan yang berdasarkan atas suatu rangkaian pemikiran (logika). "Hakim wajib menguraikan dan menjelaskan alasan-alasan yang menjadi dasar keyakinannya atas kesalahan terdakwa".[84] Sistem pembuktian ini mengakui adanya alat bukti tertentu tetapi tidak ditetapkan secara limitatif oleh undang-undang.

4. Sistem Pembuktian Menurut Undang-Undang Secara Negatif (*Negatief Wettelijk Bewijstheorie*)

Sistem ini merupakan penggabungan antara sistem pembuktian menurut undang-undang secara positif dengan sistem pembuktian berdasarkan keyakinan hakim semata. Hasil penggabungan ini dapat dirumuskan : "salah tidaknya seorang terdakwa ditentukan oleh hakim yang didasarkan kepada cara dan dengan alat-alat bukti yang sah menurut undang-undang". "Sistem

[83] Andi Hamzah, *op.cit*, Hlm. 247
[84] Edmon Makarim, 2003, *Kompilasi Hukum Telematika*, Rajagrafindo Persada, Jakarta, Hlm. 422

pembuktian menurut undang-undang secara negatif ini merupakan suatu keseimbangan antara sistem yang saling bertolak belakang secara ekstrim".[85]

> Dalam sistem atau teori pembuktian yang berdasarkan undang-undang secara negatif (*negatief wettelijk bewijstheorie*) ini, pemidanaan didasarkan kepada pembuktian yang berganda (*dubbel en grondslag*, menurut D. Simmons), yaitu pada peraturan perundang-undangan dan pada keyakinan hakim, dan menurut undang-undang, dasar keyakinan hakim itu bersumber pada peraturan undang-undang.[86]

C. Alat-alat Bukti

1. Jenis-jenis Alat Bukti menurut KUHAP

Setiap macam alat-alat bukti disebutkan secara limitatif didalam KUHAP dan diuraikan menurut urutan dalam Pasal 184 KUHAP, antara lain :

a. Keterangan Saksi

Pada umumnya, setiap orang dapat menjadi saksi di muka persidangan. Kekecualian menjadi saksi tercantum dalam Pasal 186 KUHAP, adalah sebagai berikut :

1) keluarga sedarah atau semenda dalam garis lurus ke atas atau ke bawah sampai derajat ketiga dari terdakwa atau yang bersama-sama sebagai terdakwa;
2) saudara dari terdakwa atau yang bersama-sama sebagai terdakwa, saudara ibu atau saudara bapak, juga mereka yang mempunyai hubungan karena perkawinan, dan anak-anak saudara terdakwa sampai derajat ketiga;

---

[85] Yahya Harahap, 1988 dan 1993, *Pembahasan Permasalahan dan Penerapan KUHAP Jilid I dan II*, *Pustaka Kartini*, Jakarta, Hlm. 799

[86] Andi Hamzah, 2005, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta Hlm. 250

3) suami atau istri terdakwa meskipun telah bercerai atau yang bersama-sama sebagai terdakwa.

Disamping karena hubungan keluarga atau semenda, juga ditentukan oleh Pasal 170 KUHAP bahwa mereka yang karena pekerjaan, harkat martabat atau jabatannya diwajibkan menyimpan rahasia, dapat minta dibebaskan dari kewajiban untuk memberi keterangan sebagai saksi. Contoh orang yang harus menyimpan rahasia jabatannya misalnya seorang dokter yang harus merahasiakan penyakit yang diderita pasiennya. Sedangkan yang dimaksud karena martabatnya dapat mengundurkan diri adalah mengenai hal yang dipercayakan kepada mereka, misalnya pastor agama Katolik Roma yang berhubungan dengan kerahasiaan orang-orang yang melakukan pengakuan dosa kepada pastor tersebut. Menurut Pasal 170 KUHAP di atas mengatakan "dapat minta dibebaskan dari kewajiban untuk memberi keterangan sebagai saksi…" maka berarti apabila mereka bersedia menjadi saksi, dapat diperiksa oleh hakim. "Oleh karena itu, kekecualian menjadi saksi karena harus menyimpan rahasia jabatan atau karena martabatnya merupakan kekecualian relatif".[87] Kekecualian menjadi saksi dibawah sumpah juga ditambahkan dalam Pasal 171 KUHAP, yaitu :

1) anak yang umurnya belum cukup lima belas tahun dan belum pernah kawin;

[87] Andi Hamzah, 2005, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta Hlm. 258

2) orang sakit ingatan atau sakit jiwa meskipun kadang-kadang ingatannya baik kembali.

Dalam hal kewajiban saksi mengucapkan sumpah atau janji, dalam Pasal 160 ayat (3) dikatakan bahwa sebelum saksi memberikan keterangan, saksi wajib mengucapkan sumpah atau janji menurut cara agamanya masing-masing, bahwa ia akan menberikan keterangan yang sebenarnya dan tidak lain daripada yang sebenarnya. Pengucapan sumpah atau janji didalam Pasal 161 KUHAP merupakan syarat mutlak. Dalam hal saksi atau ahli yang menolak untuk bersumpah atau berjanji sebagaimana dimaksud dalam Pasal 160 ayat (3) dan ayat (4), maka pemeriksaan terhadapnya tetap dilakukan, sedang ia dengan surat penetapan hakim ketua sidang dapat dikenakan sandera di tempat rumah tahanan negara paling lama empat belas hari. Apabila dalam tenggang waktu penyanderaan tersebut telah lampau dan saksi atau ahli tetap tidak mau mengucapkan sumpah atau janji, maka keterangan yang telah diberikan merupakan keterangan yang dapat menguatkan keyakinan hakim. Dalam Pasal 161 ayat (2) menunjukkan bahwa keterangan saksi atau ahli yang tidak disumpah atau mengucapkan janji, tidak akan dianggap menjadi alat bukti yang sah, melainkan hanyalah merupakan keterangan yang dapat menguatkan keyakinan hakim, bukan merupakan dasar atau sumber keyakinan hakim.

Mengenai isi dan keterangan seorang saksi, dalam keterangan saksi tidak termasuk keterangan yang diperoleh dari orang lain atau dalam ilmu

hukum acara pidana disebut *testimonium de auditu* atau *hearsay evidence*. *Testimonium de auditu* tidak diperkenankan sebagai alat bukti dalam "Hukum Acara Pidana Indonesia menurut Andi Hamzah selaras dengan tujuan Hukum Acara Pidana yaitu mencari kebenaran materiil. Namun demikian, *testimonium de auditu* perlu juga didengar oleh hakim, walaupun tidak mempunyai nilai sebagai bukti kesaksian, tetapi dapat memperkuat keyakinan hakim yang bersumber kepada dua alat bukti yang lain".[88] Selanjutnya dapat dikemukakan adanya batas nilai suatu kesaksian yang berdiri sendiri dari seorang saksi yang disebut *unus testis nullus testis* (satu saksi bukan saksi). Hal ini dapat dilihat pada Pasal 185 ayat (2) yang menyebutkan bahwa keterangan seorang saksi saja tidak cukup untuk membuktikan bahwa terdakwa bersalah terhadap perbuatan yang didakwakan kepadanya. Namun, ketentuan sebagaimana tercantum dalam ayat (2) di atas tidak berlaku menurut Pasal 185 ayat (3) apabila disertai dengan suatu alat bukti yang sah lainnya. Menurut KUHAP, keterangan *unus testis nullus testis* , hanya berlaku bagi pemeriksaan biasa dan pemeriksaan singkat, tidak berlaku bagi pemeriksaan cepat. Hal ini disimpulkan dari penjelasan Pasal 184 yang mengemukakan dalam acara pemeriksaan cepat, keyakinan hakim cukup didukung satu alat bukti yang sah. Namun, tidak semua keterangan saksi yang mempunyai nilai sebagai alat bukti. Berdasarkan Pasal 1 angka 27 KUHAP, keterangan saksi yang

[88] Andi Hamzah, o*p.cit*, Hlm. 260

mempunyai nilai pembuktian ialah keterangan dari saksi mengenai suatu peristiwa pidana :

1) yang saksi lihat sendiri,
2) saksi dengar sendiri,
3) dan saksi alami sendiri,
4) dengan menyebut alasan dari pengetahuannya itu.

Pasal 185 ayat (1) menegaskan kembali bahwa keterangan saksi yang tersebut diatas dapat dinilai sebagai alat bukti, maka keterangan saksi itu harus "dinyatakan" di sidang pengadilan. Menurut M. Yahya Harahap, Alat bukti kesaksian sebagai alat bukti yang sah adalah bersifat bebas dan "tidak sempurna" dan tidak "menentukan" atau "tidak mengikat".

b. Keterangan Ahli

Keterangan seorang ahli disebut sebagai alat bukti pada urutan yang kedua setelah keterangan saksi oleh Pasal 183 KUHAP. Didalam Pasal 186 KUHAP menyatakan bahwa keterangan seorang ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan. Tidak diberikan penjelasan yang khusus mengenai apa yang dimaksud dengan keterangan ahli menurut KUHAP, dan menurut Andi Hamzah dapat merupakan kesenjangan pula. Sebagai suatu perbandingan, *California Evidence Code* mendefinisikan "seorang ahli", sebagai berikut :

> "*A person is qualified to testify as an expert if he has special knowledge, skill, experience, training, or education sufficient to qualify him as an expert on the subject to which his testimony relates*".

"Dalam terjemahan yang dikemukakan oleh Andi Hamzah, seseorang dapat memberikan keterangan sebagai ahli jika ia mempunyai pengetahuan, keahlian, pengalaman, latihan, atau pendidikan khusus yang memadai untuk memenuhi syarat sebagai seorang ahli tentang hal yang berkaitan dengan keterangannya".[89] KUHAP membedakan keterangan ahli di persidangan sebagai alat bukti "keterangan ahli" (Pasal 186 KUHAP) dan keterangan seorang ahli secara tertulis di luar sidang pengadilan sebagai alat bukti "surat" (Pasal 187 butir c KUHAP). Contohnya ialah *visum et repertum* yang dibuat oleh seorang dokter. Seorang Ahli dapat memberikan keterangan mengenai tandatangan dan tulisan sebagai alat bukti dalam hal terjadi pemalsuan tandatangan dan tulisan tangan. Hal ini termuat dalam Surat Edaran Jaksa Agung RI kepada jajaran kejaksaan di seluruh Indonesia No.SE-003/J.A/2/1984 yang merupakan aturan pelaksanaan dari Pasal 184 ayat (1) huruf c jo. Pasal 187 KUHAP. Tetapi menurut Yahya Harahap hanya sebatas mengenai keterangan ahli tentang tanda tangan dan tulisan. Jika tanda tangan atau tulisan hendak dijadikan alat bukti, untuk menentukan autentikasi tanda tangan dan tulisan tersebut, ahli yang dimintai keterangannya untuk itu menurut SE Jaksa Agung untuk tindak pidana umum dan tindak pidana khusus, keterangan ahli autentikasi diberikan oleh LABKRIM MABAK.[90] Pada pemeriksaan penyidikan demi untuk kepentingan peradilan, peyidik berwenang mengajukan permintaan keterangan dari seorang ahli.

[89]Andi Hamzah, 2005, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, Hlm. 268
[90] M.Yahya Harahap, Yahya Harahap, 2006, *Pembahasan Permasalahan dan Penerapan KUHAP*, Sinar Grafika, Jakarta, Hlm. 301

"Menurut Yahya Harahap, apabila keterangan ahli bersifat "diminta', ahli tersebut membuat "laporan" sesuai dengan yang dikehendaki penyidik".[91] Laporan tersebut menurut penjelasan Pasal 186 KUHAP dibuat dengan mengingat sumpah di waktu ia menerima jabatan atau pekerjaan. Oleh penjelasan Pasal 186, laporan seperti itu "bernilai sebagai alat bukti" keterangan ahli yang diberi nama alat bukti keterangan ahli "berbentuk laporan". Apabila hal itu tidak diberikan pada waktu pemeriksaan oleh penyidik atau penuntut umum, maka pada pemeriksaan di sidang, seorang ahli diminta untuk memberikan keterangan dan dicatat dalam berita acara pemeriksaan. "Keterangan tersebut diberikan setelah ia mengucapkan sumpah atau janji di hadapan hakim".[92] "Menurut Yahya Harahap, pada sisi lain, alat bukti keterangan ahli yang berbentuk laporan juga menyentuh alat bukti surat".[93] Hal ini diatur dalam Pasal 187 huruf (c) KUHAP yang menentukan salah satu yang termasuk alat bukti surat ialah "surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai sesuatu hal atau sesuatu keadaan yang diminta secara resmi daripadanya". Hal ini tergantung pada kebijakan hakim dapat menilainya sebagai alat bukti keterangan ahli "berbentuk laporan" atau menyebutnya sebagai alat bukti surat. "Kedua alat bukti tersebut sama-sama bersifat "kekuatan pembuktian yang bebas" dan tidak mengikat".[94] "Keterangan yang sekalipun diberikan oleh beberapa ahli namun dalam

[91] M.Yahya Harahap, *op.cit*, Hlm. 296
[92] Titik Terang, *Kitab Undang-undang Hukum Acara Pidana*, 1995, Titik Terang, Hlm. 170
[93] M.Yahya Harahap, *loc.cit*, Hlm. 304
[94] *Ibid*, Hlm. 304

bidang dan keahlian yang sama atau hanya mengungkap suatu keadaan atau suatu hal yang sama, maka hanya dianggap sebagai satu alat bukti saja".[95]

c. Surat

Selain Pasal 184 KUHAP yang menyebutkan alat-alat bukti secara limitatif, didalam Pasal 187 diuraikan tentang alat bukti surat yang terdiri dari empat butir. Asser-Anema memberikan pengertian mengenai surat ialah segala sesuatu yang mengandung tanda-tanda baca yang dapat dimengerti, dimaksud untuk mengeluarkan isi pikiran. "Sedangkan surat menurut Prof. A. Pitlo adalah pembawa tanda tangan bacaan yang berarti, yang menerjemahkan suatu isi pikiran. Tidak termasuk kata surat, adalah foto dan peta, sebab benda ini tidak memuat tanda bacaan".[96] Surat sebagaimana tersebut dalam Pasal 184 ayat (1) huruf c, dibuat atas sumpah jabatan atau dikuatkan dengan sumpah, adalah :

1) berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat dihadapannya, yang memuat keterangan tentang kejadian atau keadaan yang didengar, dilihat, atau yang dialaminya sendiri, disertai dengan alasan yang jelas dan tegas tentang keterangannya itu;
2) surat yang dibuat menurut ketentuan peraturan perundang-undangan atau surat yang dibuat oleh pejabat mengenai hal yang termasuk

[95] *Ibid*, Hlm. 305
[96] Muhammad Taufik Makarao dan Suhasril, 2004, *Hukum Acara Pidana dalam teori dan praktek*, Ghalia Indonesia, Jakarta, Hlm. 127

dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukkan bagi pembuktian sesuatu hal atau sesuatu keadaan;

3) surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai sesuatu hal atau sesuatu keadaan yang diminta secara resmi daripadanya;

4) surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.

Jenis-jenis surat ini tercantum dalam Pasal 187 KUHAP sebagai alat bukti yang sah di persidangan.

> Pasal 187 butir (a) dan (b) diatas disebut juga akta otentik, berupa berita acara atau surat resmi yang dibuat oleh pejabat umum, seperti notaris, paspor, surat izin mengendarai (SIM), kartu tanda penduduk (KTP), akta lahir, dan sebagainya. Pasal 187 butir (c), misalnya keterangan ahli yang berupa laporan atau *visum et repertum*, kematian seseorang karena diracun, dan sebagainya. Pasal 187 butir (d) disebut juga surat atau akte dibawah tangan.[97]

"Menurut Martiman Prodjohamodjojo, Pasal 187 butir (d), adalah surat yang tidak sengaja dibuat untuk menjadi alat bukti, tetapi karena isinya surat ada hubungannya dengan alat bukti yang lain, maka dapat dijadikan sebagai alat bukti tambahan yang memperkuat alat bukti yang lain".[98] Menurut Andi Hamzah, selaras dengan bunyi Pasal 187 butir (d), maka surat di bawah tangan ini masih mempunyai nilai jika ada hubungannya dengan isi dari alat pembuktian yang lain. Contoh surat ini adalah keterangan saksi yang menerangkan bahwa ia (saksi) telah menyerahkan uang kepada terdakwa. "Keterangan ini merupakan satu-satunya alat bukti

[97] M.Yahya Harahap, Yahya Harahap, 2006, *Pembahasan Permasalahan dan Penerapan KUHAP,* Sinar Grafika, Jakarta, Hlm. 307

[98] Muhammad Taufik Makarao, S.H.,M.H dan Drs. Suhasril, *op.cit*, Hlm. 128

di samping sehelai surat tanda terima (kuitansi) yang ada hubungannya dengan keterangan saksi tentang pemberian uang kepada terdakwa cukup sebagai bukti minimum sesuai dengan Pasal 183 KUHAP dan Pasal 187 butir (d) KUHAP".[99] Secara formal, alat bukti surat sebagaimana disebut dalam pasal 187 huruf (a), (b), dan (c) adalah alat bukti sempurna, sebab dibuat secara resmi menurut formalitas yang ditentukan oleh peraturan perundang-undangan, sedangkan surat yang disebut dalam butir (d) bukan merupakan alat bukti yang sempurna. Dari segi materiil, semua bentuk alat bukti surat yang disebut dalam Pasal 187 bukanlah alat bukti yang mempunyai kekuatan mengikat. Sama seperti keterangan saksi atau keterangan ahli, surat juga mempunyai kekuatan pembuktian yang bersifat bebas (*vrij bewijskracht*). Adapun alasan ketidakterikatan hakim atas alat bukti surat didasarkan pada beberapa asas antara lain, asas proses pemeriksaan perkara pidana ialah untuk mencari kebenaran materiil atau setidak-tidaknya mendekati kebenaran sejati (*materiel waarheid*), bukan mencari keterangan formil. Selain itu, asas batas minimum pembuktian (*bewijs minimum*) yang diperlukan dalam pembuktian untuk mengikat kebebasan hakim sebagaimana tercantum dalam Pasal 183, bahwa hakim baru boleh menjatuhkan pidana kepada seorang terdakwa telah terbukti dengan sekurang-kurangnya dua alat bukti yang sah dan keyakinan hakim bahwa terdakwalah yang melakukannya. Dengan demikian, bagaimanapun sempurnanya alat bukti surat, namun alat bukti surat ini

[99]Andi Hamzah, 2005, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, Hlm. 270

tidaklah dapat berdiri sendiri, melainkan sekurang-kurangnya harus dibantu dengan satu alat bukti yang sah lainnya guna memenuhi batas minimum pembuktian yang telah ditentukan dalam Pasal 183 KUHAP.

d. Petunjuk

Petunjuk merupakan alat bukti keempat yang disebutkan dalam Pasal 184 KUHAP. Dalam Pasal 188 ayat (1) disebutkan pengertian petunjuk, yaitu perbuatan, kejadian atau keadaaan, yang karena persesuaiannya, baik antara yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya.

> Yahya Harahap mendefinisikan petunjuk dengan menambah beberapa kata, yakni petunjuk adalah suatu "isyarat" yang dapat "ditarik dari suatu perbuatan, kejadian, atau keadaan" dimana isyarat tadi mempunyai "persesuaian" antara yang satu dengan yang lain maupun isyarat tadi mempunyai persesuaian dengan tindak pidana itu sendiri, dan dari isyarat yang bersesuaian tersebut "melahirkan" atau "mewujudkan" suatu petunjuk yang "membentuk kenyataan" terjadinya suatu tindak pidana dan terdakwalah pelakunya.[100]

Menurut Pasal 188 ayat (2) KUHAP dalam hal cara memperoleh alat bukti petunjuk, hanya dapat diperoleh dari : 1) keterangan saksi; 2) surat; dan 3) keterangan terdakwa.

Apabila alat bukti yang menjadi sumber dari petunjuk tidak ada dalam persidangan pengadilan, maka dengan sendirinya tidak akan ada alat bukti petunjuk. Nilai kekuatan pembuktian (*bewijskracht*) dari alat bukti petunjuk sama dengan alat bukti yang lain yaitu bebas. Hakim tidak

[100] Muhammad Taufik Makarao dan Suhasril, 2004, *Hukum Acara Pidana dalam teori dan praktek*,
Ghalia Indonesia, Jakarta, Hlm. 129

terikat atas kebenaran persesuaian yang diwujudkan oleh petunjuk. Namun demikian, sebagaimana dikatakan Pasal 188 ayat (3), penilaian atas kekuatan pembuktian dari suatu petunjuk dalam setiap keadaan tertentu dilakukan oleh hakim dengan arif dan bijaksana, setelah ia mengadakan pemeriksaan dengan penuh kecermatan dan kesaksamaan berdasarkan hati nuraninya.

e. Keterangan Terdakwa

Pengertian keterangan terdakwa tercantum dalam Pasal 189 ayat (1) KUHAP yang berbunyi, keterangan terdakwa ialah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri atau alami sendiri. Keterangan terdakwa yang diberikan di luar sidang dapat digunakan untuk membantu menemukan bukti di sidang, asalkan keterangan itu didukung oleh suatu alat bukti yang sah sepanjang mengenai hal yang didakwakan kepadanya. Keterangan terdakwa hanya dapat digunakan terhadap dirinya sendiri. Keterangan terdakwa saja tidak cukup untuk membuktikan bahwa ia bersalah melakukan perbuatan yang didakwakan kepadanya, melainkan harus disertai dengan alat bukti yang lain.

> Terhadap bunyi Pasal 189 ayat (2), Yahya Harahap mengatakan, bentuk keterangan yang dapat diklasifikasikan sebagai keterangan terdakwa yang diberikan di luar sidang adalah :
> 1) keterangan yang diberikannya dalam pemeriksaan penyidikan;
> 2) dan keterangan itu dicatat dalam berita acara penyidikan;

3) serta berita acara penyidikan itu ditandatangani oleh pejabat penyidik dan terdakwa. [101]

Pengakuan tersangka dalam tingkat penyidikan dapat dicabut kembali dalam pemeriksaan pengadilan. "Alasan klise dicabutnya pengakuan tersebut adalah karena tersangka disiksa oleh petugas penyidik".[102]

D. Pengertian Barang Bukti

Barang bukti adalah barang atau benda yang berhubungan dengan kejahatan.

> Barang atau benda tersebut dapat dikategorikan sebagai *corpus delicti* yang berarti barang-barang atau benda-benda yang menjadi objek delik dan barang dengan mana delik dilakukan yaitu alat yang dipakai untuk melakukan kejahatan. Ada pula yang termasuk barang bukti ialah barang-barang yang dikategorikan sebagai *instrumenta delicti* yang berarti barang-barang atau benda-benda hasil kejahatan, barang atau benda yang berhubungan langsung dengan tindak pidana.[103]

Barang bukti dengan alat bukti mempunyai hubungan yang erat dan merupakan rangkaian yang tidak terpisahkan. Dalam persidangan setelah semua alat bukti diperiksa, selanjutnya dilanjutkan dengan pemeriksaan barang bukti. Barang bukti dalam proses pembuktian biasanya diperoleh melalui penyitaan. "Dengan penyitaan maka penyidik akan mencari keterhubungan antara barang yang

---

[101] Yahya Harahap, 1988 dan 1993, *Pembahasan Permasalahan dan Penerapan KUHAP Jilid I dan II*, *Pustaka Kartini*, Jakarta, Hlm. 858-859

[102] Muhammad Taufik Makarao dan Suhasril, 2004, *Hukum Acara Pidana dalam teori dan praktek*, Ghalia Indonesia, Jakarta, Hlm. 131

[103] Andi Hamzah, 1986, *Kamus Hukum*, Ghalia, Jakarta, Hal.100 dalam 'Edmon Makarim, 2003 ,*Kompilasi Hukum Telematika*, Rajagrafindo Persada, Jakarta, Hlm. 446

diketemukan dengan tindak pidana yang dilakukan".[104] Barang bukti mempunyai nilai/fungsi dan bermanfaat dalam upaya pembuktian, walaupun barang bukti yang disita oleh petugas penyidik tersebut secara yuridis formal bukan sebagai alat bukti yang sah menurut KUHAP. Akan tetapi, dalam praktik peradilan, barang bukti tersebut ternyata dapat memberikan keterangan yang berfungsi sebagai tambahan dari alat bukti yang sah dalam bentuk keterangan saksi, keterangan ahli (*visum et repertum*), maupun keterangan terdakwa. Misalnya sebuah benda berupa senjata api atau senjata tajam setelah disita menjadi barang bukti kemudian ditunjukkan dan ditanyakan kepada saksi dan saksi tersebut memberikan keterangan bahwa barang bukti tersebut oleh tersangka telah digunakan untuk melakukan pembunuhan atau penganiayaan. Demikian pula mayat korban pembunuhan setelah dilakukan pemeriksaan ilmiah oleh Ahli Kedokteran Kehakiman (Laboratorium Forensik) kemudian hasil pemeriksaannya dituangkan dalam *visum et repertum* yang isinya bersesuaian dengan keterangan saksi yang diperkuat oleh keterangan tersangka/terdakwa. Disamping itu, dengan diajukannya barang bukti di muka persidangan, maka hakim melalui putusannya dapat secara sekaligus menetapkan status hukum dari barang bukti yang bersangkutan, "yaitu apakah diserahkan kepada pihak yang paling berhak menerimanya atau dirampas untuk kepentingan negara atau untuk dimusnahkan atau dirusak sehingga tidak dapat dipergunakan kembali {Pasal 194 jo 197 ayat (1) huruf (i) KUHAP}".[105]

---

[104] *Ibid*, Hlm. 447

[105] HMA. Kuffal, 2005, *Tata Cara Penggeledahan dan Penyitaan*, UMM Press, Malang, Hlm. 25-29

E. Unsur Pembuktian yang Menimbulkan Keyakinan Hakim dalam Memutus Suatu Perkara Pidana di Indonesia

Kitab Undang-undang Hukum Acara Pidana (KUHAP) menganut sistem pembuktian berdasarkan undang-undang secara negatif (*negatief wettelijk bewijstheorie*). Hal ini disebutkan dalam Pasal 183 KUHAP yang berbunyi : "Hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya". "Disimpulkan dari kalimat tersebut nyata bahwa pembuktian harus didasarkan kepada KUHAP, yaitu alat bukti yang sah tersebut dalam Pasal 184 KUHAP, disertai dengan keyakinan hakim yang diperoleh dari alat-alat bukti tersebut".[106]

> Wirjono Prodjodikoro berpendapat bahwa sistem pembuktian berdasarkan undang-undang secara negatif (*negetief wettelijk bewijstheorie*) sebaiknya dipertahankan berdasarkan dua alasan, pertama memang sudah selayaknya harus ada keyakinan hakim mengenai kesalahan terdakwa untuk dapat menjatuhkan suatu hukuman pidana, janganlah hakim terpaksa memidana seseorang sedangkan hakim tidak yakin atas kesalahan terdakwa. Kedua ialah berfaedah jika ada aturan yang mengikat hakim dalam menyusun keyakinannya, agar ada patokan-patokan tertentu yang harus dituruti oleh hakim dalam melakukan peradilan.[107]

"Menurut Subekti, ketidakpastian hukum (*rechtsonzekerheid*) dan kesewenang-wenangan (*willekeur*) akan timbul apabila hakim, dalam melaksanakan tugasnya tersebut, diperbolehkan menyandarkan putusan hanya atas keyakinannya, biarpun itu sangat kuat dan sangat murni. Keyakinan hakim itu

---

[106] Andi Hamzah, 2005, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, Hlm. 250

[107] Wirjono Prodjodikoro dalam Andi Hamzah, 2005, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, Hlm. 252

harus didasarkan pada sesuatu, yang oleh Undang-Undang dinamakan alat bukti".[108]

[108] Subekti, 1995, *Hukum Pembuktian*, Pradnya Paramita, Jakarta, Hlm. 2

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

"Berdasarkan data Polri, kasus kejahatan dunia maya yang terjadi selama kurun waktu 5 (lima) tahun dari tahun 2002 sampai dengan tahun 2006 tercatat 71 (tujuh puluh satu) kasus. Dari 71 (tujuh puluh satu) kasus yang dilaporkan tersebut, 35 (tiga puluh lima) kasus telah dinyatakan P-21 oleh Jaksa Penuntut Umum dan beberapa kasus telah mendapatkan vonis".[109] Agar suatu perkara pidana dapat sampai pada tingkat penuntutan dan pemeriksaan di sidang pengadilan, maka sebelumnya harus melewati beberapa tindakan-tindakan pada tingkat penyidik. Apabila ada unsur-unsur pidana (bukti awal telah terjadinya tindak pidana) maka barulah dari proses tersebut dilakukan penyelidikan (serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyelidikan menurut cara yang diatur dalam undang-undang ini), dan dalam Undang-undang Nomor 2 Tahun 2002 tentang Kepolisian dalam pasal 1 angka 13, penyidikan ialah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya. Penyelidik yang dimaksud menurut Pasal 1 KUHAP adalah pejabat polisi negara Republik Indonesia yang diberi wewenang oleh undang-undang ini untuk melakukan penyelidikan. Sedangkan penyidik

---

[109] Petrus Reinhard Golose, 12 April 2007, *Penegakan Hukum Cyber Crime dalam Sistem Hukum Indonesia* dalam Handout Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia, FHUI, Jakarta, Hlm. 6

yang dimaksud dalam Pasal 1 butir 1 ialah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi kewenangan khusus oleh undang-undang untuk melakukan penyidikan. Penyidik pembantu yang diatur oleh Pasal 1 butir 3 KUHAP ialah pejabat kepolisian negara Republik Indonesia yang karena diberi wewenang tertentu dapat melakukan tugas penyidikan yang diatur dalam undang-undang tentang hukum acara pidana.

"Dari hasil wawancara penulis dengan penyidik madya unit V IT dan *cybercrime* Direktorat Ekonomi dan Khusus Bareskrim Mabes Polri, selaku penyidik kasus penyerangan situs golkar (*deface*) Bapak Eddy Hartono, S.Ik mengemukakan langkah-langkah yang dilakukan oleh Polri dalam menangani kasus *hacking* atau kasus-kasus perusakan terhadap komputer melalui jaringan, adalah sebagai berikut"[110] :

1) Pembuatan Laporan Polisi, yang diikuti dengan pemanggilan Saksi dari pemilik ISP (*Internet Service Provider*) yang telah diketahui bahwa ISP tersebut digunakan oleh si pelaku (*hacker*);
2) Pemeriksaan di Tempat Kejadian Perkara (TKP) dan warnet atau café net yang digunakan pelaku, sekaligus untuk mengumpulkan, melacak dan/atau melakukan penyitaan terhadap bukti elektronik (*digital evidence*) yang ada di TKP, seperti *hard disk*;
3) Melakukan pemeriksaan terhadap para saksi dan ahli yang memiliki keahlian dibidang teknologi informasi, baik dari Universitas Indonesia (UI), Universitas Padjajaran (UNPAD) atau lembaga-lembaga lainnya;

[110] Hasil wawancara dengan Eddy Hartono pada tanggal 24 April 2007

4) Pemeriksaan terhadap tersangka, setelah didahului dengan upaya paksa penangkapan dan/atau penahanan, berdasarkan bukti permulaan dan/atau alat bukti yang cukup;
5) Pemberkasan dan penerapan pasal-pasal pidana yang dapat disangkakan terhadap tersangka.

"Dalam melakukan penyidikan suatu kasus kejahatan dunia maya, seorang penyidik dapat menggunakan alat-alat investigasi standar (*standart investigative tools*), antara lain"[111] :

1) Informasi sebagai dasar bagi suatu kasus

Informasi dapat diperoleh dari observasi, pengujian bukti elektronik yang tersimpan dalam *hard disk* atau bahkan masih dalam memori. Bagi penyidik, sangat penting untuk memperoleh informasi melalui *crime scene search* (penyidikan di tempat kejadian perkara) yang bertumpu pada komputer.

2) *Interview* dan Interogasi

Alat ini dipergunakan untuk memperoleh informasi dari pihak-pihak yang terlibat dalam kejahatan dunia maya. Wawancara ini meliputi perolehan informasi dengan memberikan pertanyaan kepada saksi-saksi, korban, dan pihak lain yang mungkin memiliki informasi relevan untuk memecahkan kasus tersebut. Sedangkan interogasi meliputi perolehan informasi dengan memberikan pertanyaan kepada tersangka dan saksi. Adapun tekniknya dilakukan dengan pendekatan simpatik yang meliputi :

[111] Petrus Reinhard Golose, *op.cit,* Hlm. 16

a) Pendekatan logis

Menggunakan alasan-alasan untuk meyakinkan tersangka untuk mengakui perbuatannya;

b) *Indifference*

Dengan berpura-pura tidak memerlukan pengakuan karena penyidik telah memiliki cukup bukti walaupun tanpa pengakuan. Hal tersebut efektif untuk kasus dengan banyak tersangka, dimana keterangan yang bersangkutan saling dikonfrontir;

c) *Facing-saving approach*

Dengan membiarkan tersangka memberikan alasan-alasan atas tindakannya dan menunjukkan pengertian mengapa yang bersangkutan melakukan tindakan tersebut.

3) Instrumen

Kegunaan teknologi dalam memperoleh bukti-bukti. Dalam kasus kejahatan dunia maya, penggunaan data teknik *recovery* untuk menemukan informasi yang "*deleted*" dan "*erased*" dalam *disk* merupakan salah satu tipe instrumennya. Selain itu, contoh-contoh tradisional lainnya meliputi teknik forensik untuk mengumpulkan dan menganalisis bukti-bukti dan analisis DNA.

4) Menyusun laporan kasus

Setelah semua bukti fisik telah dikumpulkan dan didokumentasikan serta interogasi telah dilaksanakan, langkah yang harus dilakukan ialah penyusunan laporan kasus yang memuat :

a) Laporan penyelidikan;

b) Laporan penyidikan kasus pidana yang ditindaklanjuti dari laporan penyelidikan;

c) Dokumentasi bukti-bukti elektronik

d) Laporan laboratorium dari ahli forensik komputer;

e) Pernyataan-pernyataan tertulis dari saksi-saksi, tersangka, dan ahli;

f) Laporan TKP, foto-foto dan rekaman video;

g) *Print out* dari bukti-bukti digital yang berkaitan.

5) Pemeriksaan berkas perkara oleh Jaksa Penuntut Umum

Penuntut umum memberikan arahan kepada penyidik atas kelemahan-kelemahan berkas perkara dan tambahan informasi atau bukti tambahan yang perlu diperoleh atau klarifikasi fakta-fakta dalam rangka memperkuat tuntutan serta menyiapkan saksi-saksi untuk proses persidangan jika kasus tersebut dilimpahkan ke pengadilan.

6) Membuat keputusan untuk menuntut

Jika berkas perkara dinyatakan lengkap, penuntut umum melakukan penuntutan hukum kepada tersangka dalam suatu persidangan yang sangat tergantung dari yuridiksi dan prosedur yang ditentukan oleh undang-undang. Dalam tahap ini pilihan jenis tuntutan ditetapkan berdasarkan hukum pembuktian yang diatur dalam KUHAP.

A. Kasus Posisi I

Dani Firmansyah merupakan tersangka pelaku *hacking* situs *http://tnp.kpu.go.id* milik Komisi Pemilihan Umum pada tanggal 17 April 2004. Dani menyatakan bahwa keinginannya untuk melakukan *hacking* ini didasarkan atas dasar perkataan dari Tim Ahli Komisi Pemilihan Umum dan anggota KPU yang menyatakan bahwa situs yang dikelolanya tersebut aman dengan sistem pengamanan tujuh lapis (*seven layers*). Tersangka ingin membuktikan bahwa situs tersebut tidak aman seperti yang dikatakan mereka. Menurut dakwaan Jaksa Penuntut Umum (JPU), perkara ini bermulai dari hari Sabtu tanggal 17 April 2004 sekitar pukul 11:24:16 WIB atau setidak-tidaknya dalam bulan April 2004, bertempat di PT. Danareksa, Jalan Medan Merdeka Selatan No. 14 Jakarta Pusat. Pada hari itu, terdakwa secara tanpa hak melakukan akses ke jaringan telekomunikasi milik Komisi Pemilihan Umum (KPU) dan melakukan penyerangan (*attacking*) ke *server* tnp.kpu.go.id dengan cara *SQL* (*Structure Query Language*) *Injection*, dan berhasil menembus Kunci Pengaman *Internet Protocol* (*IP*) tnp.kpu.go.id 230.130.201.134. Terdakwa melakukannya dengan menggunakan teknik *spoofing* (penyesatan) yaitu melakukan *hacking* (mengakses ke jaringan telekomunikasi) dari *Internet Protocol* (*IP*) 202.158.10.117 PT. DANAREKSA dengan menggunakan *Internet Protocol* (*IP*) *Proxy* Thailand yaitu 208.147.1.1 Terdakwa mendapatkan *IP* Thailand tersebut dari situs *http://www.samair.ru/proxy*. Kemudian dengan menggunakan

IP Proxy Thailand tersebut terdakwa dengan menggunakan akses internet dari kantor terdakwa mencoba menganalisa kembali variabel-variabel yang ada di situs *http://tnp.kpu.go.id* dengan metode *SQL Injection* yaitu dengan menambahkan perintah *SQL* dari *URL* (*Uniform Resource Locator*) yang disebutkan diatas yaitu : *http://tnp.kpu.go.id/DPRDII/dpr_dapil.asp?type=view&kodeprop=1&kokodekab=7*. Dari hasil analisa didapat nama kolom di tabel partai milik *web http://tnp.kpu.go.id*. Kemudian dari hasil uji coba diperoleh kesimpulan bahwa situs milik KPU di *http://tnp.kpu.go.id* terkena *Bug SQL Injection*. Hal ini bisa dilihat dari *message error* yang nampak di *browser Internet Explorer* yang terdakwa gunakan pada saat menggunakan metode *SQL Injection*. Dengan menggunakan modifikasi di *URL* yang disebut diatas lalu, terdakwa tambahkan *command-command SQL* seperti contoh dibawah ini : *http://tnp.kpu.go.id/DPRDII/dpr_dapil.asp?type=view&kodeprop=1&kokodekab=7;UPDATE partai set nama = partai dibenerin dulu webnya' where pkid=13'*.

Dengan mengakses *URL* diatas maka salah satu nama partai di *website http://tnp.kpu.go.id* berubah menjadi : "partai dibenerin dulu webnya". Terdakwa berhasil melakukan *UPDATE* tabel (merubah tabel) nama partai jam 11:24:16 sampai dengan 11:34:27.

Adapun nama-nama Partai Peserta Pemilu yang berhasil diubah secara tanpa hak, tidak sah adalah :

No.	Nama Partai Asli	No.	Nama Partai Yang Telah Diubah
1.	Partai Nasional Indonesia Marhaenis	1.	Partai Jambu
2.	Partai Buruh Sosial Demokrat	2.	Partai Kelereng
3.	Partai Bulan Bintang	3.	Partai Cucok Rowo
4.	Partai Merdeka	4.	Partai Si Yoyo
5.	Partai Persatuan Pembangunan	5.	Partai Mbah Jambon
6.	Partai Demokrat Kebangsaan	6.	Partai Kolor Ijo
7.	Partai Perhimpunan Indonesia Baru	7.	Partai Dukun Beranak
8.	Partai Nasional Benteng Kemerdekaan	8.	Partai Wiro Sablenk
9.	Partai Demokrat	9.	Partai Air Minum Kemasan Botol
10.	Partai Keadilan dan Persatuan Indonesia	10.	Partai Dibenerin Dulu Webnya
11.	Partai Demokrasi Indonesia	11.	Partai Jangan Marah Ya…

12.	Partai Persatuan Nahdlatur Ummah Indonesia	12.	Partai Jambu
13.	Partai Amanah Nasional	13.	Partai Jambu
14.	Partai Karya Peduli Bangsa	14.	Partai Jambu
15.	Partai Kebangkitan Bangsa	15.	Partai Jambu
16.	Partai Keadilan Sejahtera	16.	Partai Jambu
17.	Partai Bintang Reformasi	17.	Partai Jambu
18.	Partai Demokrasi Indonesia Perjuangan	18.	Partai Jambu
19.	Partai Damai Sejahtera	19.	Partai Jambu
20.	Partai Golkar	20.	Partai Jambu
21.	Partai Patriot Pancasila	21.	Partai Jambu
22.	Partai Sarikat Indonesia	22.	Partai Jambu

23.	Partai Persatuan Daerah	23.	Partai Jambu
24.	Partai Pelopor	24.	Partai Jambu

Dakwaan

Jaksa Penuntut Umum Ramos Hutapea, S.H., dengan Surat Dakwaan Kejaksaan Negeri Jakarta Pusat No. Reg. Perkara : PDM-1201/JKT.PST/07/2004 menuntut terdakwa dengan beberapa dakwaan :

---- PERTAMA :

telah melanggar ketentuan sebagaimana dimaksud dalam Pasal 22 huruf a Jo. Pasal 50 Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi, yaitu setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi. Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).

---- KEDUA :

Pasal 22 huruf b Jo. Pasal 50 Undang-Undang RI. No. 36 Tahun 1999 tentang Telekomunikasi yaitu setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi akses ke jasa telekomunikasi. Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6

(enam) tahun dan atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).

--- KETIGA :

Pasal 22 huruf c Jo. Pasal 50 Undang-Undang UU RI. No. 36 Tahun 1999 tentang Telekomunikasi yaitu setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi khusus. Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).

--- KEEMPAT :

Pasal 38 jo. Pasal 55 Undang-Undang RI Nomor 36 Tahun 1999 tantang Telekomunikasi yaitu setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi. Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 38, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).

Jaksa Penuntut Umum Ramos Hutapea, S.H., dalam tuntutan pidana dengan Nomor Registrasi Perkara No : PDM-1201/JKT.PST/07/2004

M E N U N T U T :

Agar Majelis Hakim Pengadilan Negeri Jakarta Pusat, yang memeriksa dan mengadili perkara ini memutuskan :

1. Menyatakan bahwa terdakwa **Dani Firmansyah, bersalah melakukan tindak pidana sebagaimana diatur dalam Pasal 22 huruf c jo. Pasal 50 UU RI No.36 Tahun 1999 tentang Telekomunikasi** ;
2. Menjatuhkan pidana terhadap terdakwa Dani Firmansyah dengan pidana penjara selama 1 (satu) tahun dikurangi selama terdakwa berada di tahanan dengan perintah terdakwa tetap ditahan dan denda sebesar Rp. 10.000.000,- (sepuluh juta rupiah) subsider 3 (tiga) bulan kurungan.
3. Menetapkan barang bukti berupa satu unit CPU HP Vectra, satu unit kotak kardus berisi buku program, buku *hacking expose*, buku CC exam, satu tas berisi 41 piece CD Program, satu tas berisi dokumen kantor PT. Danareksa, satu unit handphone merek Siemens M 55, satu unit keyboard komputer, tiga lembar print out berita detik.com tanggal 21 April 2004, satu buah router Cisco 1700, satu buah hard disk mesin PC windows back up firewall, print out log file RPT 01 dan RPT 02 tanggal 16 dan 17 April 2004 sebanyak 340 lembar, satu bundel print out log PT. Danareksa, satu unit server warna.net, dua piece CD Log PT. Danareksa dirampas untuk dimusnahkan.
4. Agar terdakwa membayar biaya perkara sebesar Rp. 3.000,- (tiga ribu rupiah).

Penyajian Putusan dan Analisis

1) Nomor Registrasi Perkara No : PDM-1201/JKT.PST/07/2004

P U T U S A N

NOMOR : 1322/PID.B/2004/PN.JKT.PST

DEMI KEADILAN BERDASARKAN KETUHANAN YANG MAHA ESA.

Pengadilan Negeri Jakarta Pusat yang memeriksa dan mengadili perkara-perkara pidana dengan acara pemeriksaan secara biasa, telah menjatuhkan Putusan sebagai tersebut dibawah ini dalam perkara atas nama Terdakwa Dani Firmansyah. Majelis menyimpulkan bahwa bentuk dakwaan penuntut umum disusun secara alternatif. Setelah majelis mempelajari secara seksama dakwaan penuntut umum yang disusun secara alternatif tersebut diatas, menurut hemat majelis terhadap dakwaan PERTAMA atau KEDUA atau KETIGA yang termuat dalam satu pasal yang sama yaitu Pasal 22 huruf a, b, dan c Undang-undang No. 36 Tahun 1999 tentang Telekomunikasi, unsur pertama dan keduanya ternyata sama bunyinya. Sedangkan unsur ketiga dari masing-masing dakwaan tersebut berbeda, yaitu dakwaan pertama unsur ketiganya adalah ”akses ke jaringan telekomunikasi”, dakwaan kedua unsur ketiganya adalah ”akses ke jasa telekomunikasi” dan dakwaan ketiga unsur ketiganya adalah ”akses ke jaringan telekomunikasi khusus”.

Bahwa dari pertimbangan diatas dihubungkan dengan terdakwa Dani Firmansyah dengan identitas yang lengkap sebagaimana dakwaan

penuntut umum, menurut hemat majelis telah memenuhi ketentuan sebagaimana dakwaan penuntut umum, menurut hemat majelis telah memenuhi ketentuan sebagaimana dimaksud dari pada unsur pertama dakwaan pertama atau kedua atau ketiga tersebut, dengan demikian unsur pertama telah terbukti. Berdasarkan fakta-fakta hukum yang terungkap di persidangan, bahwa benar terdakwa telah berhasil melakukan *UPDATE* tabel (merubah tabel) dalam hal ini nama-nama partai peserta PEMILU tahun 2004 pada hari Sabtu tanggal 17 April 2004 sekitar pukul 11:34:27 WIB. Selanjutnya beberapa butir pertimbangan majelis dalam menjatuhkan putusan tersebut adalah sebagai berikut :

Menimbang, bahwa berdasarkan keterangan saksi-saksi dan dikuatkan dengan barang bukti yang diajukan oleh Penuntut Umum, dimana telah menjadi pengetahuan umum bahwa benar pada hari Sabtu tanggal 17 April 2004 sekitar pukul 11:24:16 sampai dengan pukul 11:34:27 WIB telah terjadi perubahan tampilan di layar siaran televisi nasional yang berisikan siaran atau berita yang berasal dari Pusat Tabulasi Nasional Pemilu 2004 terutama perubahan nama-nama peserta pemilu.

Menimbang, bahwa terdakwa dalam keterangannya telah mengakui bahwa motivasi *hacking* yang ia lakukan terhadap situs KPU adalah sekedar iseng karena penasaran dan juga dalam rangka meningkatkan atau memberitahu kepada pejabat KPU bahwa sistem pengamanan IT milik KPU masih lemah dan tidak aman.

Menimbang, bahwa dalam Undang-undang No. 36 Tahun 1999 Tentang Telekomunikasi dijelaskan tentang unsur-unsur yang didakwakan kepada terdakwa.

Menimbang, bahwa dalam persidangan telah dihadirkan saksi ahli baik dari Penuntut Umum maupun penasehat hukum terdakwa yang telah memberikan keterangan tentang keahliannya dalam perkara ini.

Menimbang, bahwa cara pemberitahuan atau sekedar mengingatkan tentang kelemahan dan keamanan sistem pengamanan IT KPU yang dilakukan oleh terdakwa seperti ini tidak tepat dan tidak semestinya. Hal tersebut dapat dinilai dari status sosial terdakwa sebagai seorang intelektual atau dapat dikatakan ahli, tidak seharusnya cara tersebut dilakukan oleh terdakwa, dan sebaliknya akan lebih terhormat serta bertata krama yang baik apabila dilakukan oleh terdakwa secara langsung datang ke KPU atau sebelumnya melalui surat baik tertutup maupun surat terbuka kepada KPU.

Menimbang, bahwa terdakwa telah terbukti bersalah melakukan tindak pidana yang didakwakan.

Menimbang, bahwa dengan memperhatikan hal-hal sebagaimana yang telah Majelis pertimbangkan diatas, maka akhirnya Majelis sampai pada suatu kesimpulan bahwa pidana yang akan dijatuhkan kepada Terdakwa seperti tersebut dalam amar putusan ini merupakan suatu tindak pidana yang dianggap adil dan bijaksana sesuai dengan rasa keadilan ;

Memperhatikan pasal-pasal dari Undang-Undang dan Peraturan Hukum lain yang bersangkutan ;

M E N G A D I L I :

1. Menyatakan Terdakwa Dani Firmansyah telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana “Tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi khusus” ;
2. Menjatuhkan pidana terhadap Terdakwa oleh karena itu dengan pidana penjara selama 6 (enam) bulan dan 1 (satu) hari ;
3. Menetapkan lamanya Terdakwa dalam tahanan dikurangkan seluruhnya dari pidana yang dijatuhkan ;
4. Menetapkan barang bukti berupa :
   a. 1 (satu) unit CPU HP Vectra VL;
   b. 1 (satu) Kotak Kardus berisi : buku program, buku Hacking Exposed, buku CCNA Exam;
   c. 1 (satu) tas berisi 41 piece CD Program;
   d. 1 (satu) tas berisi dokumen kantor PT. Danareksa;
   e. 1 (satu) Unit Handphone merek SIEMENS M 55;
   f. 1 (satu) Unit keyboard komputer;
   g. 1 (satu) Lembar print out beritadetik.com tanggal 21 April 2004
   h. 1 (satu) router Cisco 1700;
   i. 1 (satu) buah Harddisk Scsi 36 MB;
   j. 1 (satu) buah Harddisk Mesin PC Windows Back Up Firewall;

k. 1 (satu) Unit Harddisk tipe IDE Merek Maxtor 3.5 S/N 6068-4422-0100 ik 40 GB;

l. 1 (satu) lembar Print out tampilan layar Tabulasi Nasional Pemilu 2004

m. 1 (satu) bendel print out log file PT. Danareksa;

n. 1 (satu) Unit server Warnet Warna.net;

o. 340 (tiga ratus empat puluh) lembar print out log file RPT 01 dan RPT 02 tanggal 16 dan 17 April 2004;

p. 2 (dua) Pcs CD Log file PT. Danareksa

5. Menghukum Terdakwa untuk membayar biaya perkara sebesar Rp. 3.000,- (tiga ribu rupiah) ;

Demikianlah diputuskan dalam rapat musyawarah Majelis Hakim Pengadilan Negeri Jakarta Pusat pada TANGGAL : 23 Desember 2004, oleh Kami : H. HAMDI, SH., M. Hum sebagai Hakim Ketua, H. Ridwan Masyur, SH.,MH dan Kusriyanto, SH., masing-masing sebagai Hakim Anggota.

Analisis Perkara

Dalam kasus kejahatan dunia maya yang dilakukan oleh Dani Firmansyah, bukti-bukti yang diajukan adalah berbentuk data atau informasi elektronik, yaitu *log server* PT. DANAREKSA, *log file* di Warnet Warna Yogyakarta, dan tampilan layar Tabulasi Nasional Pemilu

2004 milik KPU yang telah dirubah tampilannya. Dani Firmansyah telah menyembunyikan jejak elektroniknya (*electronic path*) yaitu menggunakan teknik *spoofing* (penyesatan) dengan melakukan *hacking* dari *IP* PT. DANAREKSA dengan menggunakan *IP Proxy* Thailand. Tetapi dengan ditemukannya bukti-bukti elektronik tersebut, POLDA METROJAYA berhasil menangkap Dani Firmansyah alias Xnuxer. Namun, permasalahan yang timbul adalah, apakah bukti-bukti elektronik yang ditemukan tersebut dapat membuktikan kesalahan yang dilakukan oleh Dani firmansyah.

Cara yang ditempuh oleh pihak kepolisian dan Kejaksaan Negeri Jakarta Pusat untuk "mensahkan" bukti elektronik tersebut di hadapan pengadilan adalah dengan cara memproses bukti elektronik tersebut dari bentuk elektronik yang dihasilkan dari sistem komputer menjadi *output* yang dicetak ke dalam media kertas. Yakni, bukti elektronik tersebut diubah perwujudannya dalam bentuk *hardcopy*, yaitu di-*print*, tanpa adanya modifikasi apapun dari manusia. Lalu untuk memperkuatnya, *print out* tersebut bisa diserahkan kepada saksi ahli untuk dianalisa dan disampaikan validitasnya di hadapan pengadilan. Dalam kasus ini, bukti-bukti elektronik yang berupa data-data digital tersebut di *print-out* dan dicetak ke dalam media kertas oleh Laboratorium Forensik Komputer di Australia dan ditandatangani oleh Ahli Forensik Komputer tersebut sehingga bukti elektronik pada prinsipnya diubah menjadi alat bukti surat, dan atau petunjuk. Hal ini dikarenakan pada saat itu Indonesia belum memiliki

Laboratorium Forensik Komputer dan antara Indonesia dengan Australia telah memiliki perjanjian hukum timbal balik (*Mutual Legal Assistance*) yang telah ditandatangani pada tahun 1995 dan diratifikasi dengan Undang-Undang Nomor 1 Tahun 1999 sehingga pengambilan dan pemanfaatan bukti elektronik yang berupa *print-out* data-data digital dari Laboratorium Forensik Komputer di Australia dapat dilakukan. *Computer log files* yang ditemukan pada kasus ini adalah bukti elektronik yang menurut Hakim Mohammed Chawki dari *Computer Crime Research Center* diklasifikasikan sebagai *Real Evidence* yaitu bukti langsung berupa rekaman otomatis yang dihasilkan oleh komputer itu sendiri dengan menjalankan *software* dan *receipt* dari informasi yang diperoleh dari alat (*device*) yang lain. Dengan putusan Majelis Hakim Pengadilan Negeri Jakarta Pusat ini, Majelis Hakim telah melakukan terobosan hukum dengan mengakui bukti-bukti elektronik (*electronic evidence*) yang diajukan ke muka persidangan sebagai alat bukti sah yang menjadi sumber keyakinan Hakim atas kesalahan terdakwa Dani Firmansyah. Alat bukti elektronik memang belum secara tegas diatur di dalam peraturan perUndang-undangan, namun secara yuridis Dani Firmansyah telah melanggar ketentuan yang telah diatur dalam delik formil Undang-undang Telekomunikasi yaitu melakukan suatu tindakan tanpa hak dan tanpa otoritas secara tidak sah.

B. Kasus Posisi II

Iqra Syafaat merupakan tersangka pelaku *hacking* situs (*deface*) dengan merubah tampilan situs *www.golkar.or.id* milik Golkar. Menurut Kepala Unit *Information Tecnology and Cyber Crime* Direktorat Ekonomi dan Khusus Badan Reserse Kriminal Mabes Polri Komisaris Besar Petrus Reinhard Golose, serangan (*deface*) perusakan situs Golkar, *www.golkar.or.id*, pertama kali terjadi pada tanggal 9 Juli 2006. Iqra Syafaat seorang lulusan SMU yang kerap berjualan buku elektronik (*e-book*) mengganti foto beberapa tokoh Golkar menjadi foto gorila putih tersenyum. Serangan berikutnya pada 10 Juli 2006, halaman muka situs Golkar diisi dengan foto mesum aktris *Hollywood* dengan tulisan "bersatu untuk malu". Penyerangan situs Golkar itu dilakukan pada tanggal 9-13 Juli 2006. Kemudian, pada tanggal 17 Juli 2006, Partai Golkar melalui pengacaranya Zulhendri Hasan melaporkan hal tersebut ke Mabes Polri. Situs Golkar selama kurun waktu tersebut telah diserang 1.257 kali dari 31 lokasi yang tercatat di *Internet Protocol Address* (*IP Address*) dari sejumlah kota seperti Jakarta, Bekasi, Bandung, Surabaya, Lampung, Palembang, Medan, dan Batam. Selain itu, berdasarkan *IP Address* yang tercatat, penyerangan juga terhubung dengan *hacker* asing dari luar negeri seperti Malaysia, Amerika Serikat, Brazil, Turky, dan Rumania. Namun, yang disidik polisi terkait perusakan dengan pola yang dilakukan Iqra.

Dakwaan

Jaksa Penuntut Umum pada kejaksaan Negeri Jakarta Barat dengan memperhatikan hasil sidang dalam perkara terdakwa Iqra Syafaat yang diajukan kedepan persidangan berdasarkan Surat Penetapan Hakim Pengadilan Jakarta Barat Nomor : 3254 / Pen. Pid / 2006 / PN. JKT. BAR. tanggal 13 Nopember 2006 dan Surat Pelimpahan Acara Pemeriksaan Biasa, tanggal 17 Oktober 2006 Nomor : B-3320 / 0. 1. 12. 3 / Ep. 1 / 10 / 2006 dihadapkan kedepan persidangan dengan dakwaan :

KESATU :

-- Bahwa terdakwa **Iqra Syafaat**, pada hari-hari sabtu tanggal 08 Juli 2006, sekira pukul 21.00 WIB., Minggu tanggal 09 Juli 2006, sekira pukul 01.00 WIB, Senin tanggal 10 Juli 2006 pukul 13.00 WIB, hari Selasa tanggal 11 Juli 2006 sekira pukul 11.00 WIB dan hari Jum'at tanggal 14 Juli 2006 sekira pukul 01.00 WIB atau setidak-tidaknya pada beberapa hari di bulan Juli 2006, dan perbuatan terdakwa sedemikian rupa sehingga harus dipandang sebagai satu perbuatan berlanjut, bertempat di warnet Barelang Jalan Raden Patah No. 81 dan di Bukit Timur RT. 04 / RW. 06 No. 4 Tanjung Uma Batam atau di Kantor Sekretariat DPP Golkar di Jalan Anggrek Nelli VI Jakarta Barat atau setidak-tidaknya di suatu tempat, yang berdasarkan ketentuan dalam Pasal 84 ayat (2) KUHAP, Pengadilan Negeri Jakarta Barat berwenang memeriksa dan mengadili perkara ini, **telah melanggar ketentuan sebagaimana dimaksud dalam pasal 22 huruf b UU RI. No. 36 Tahun 1999 tentang Telekomunikasi** yaitu

setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi akses ke jasa telekomunikasi, yang dilakukan terdakwa dengan cara sebagai berikut :

- Bahwa pada hari Sabtu tanggal 08 Juli 2006 bertempat di warnet Barelang Jalan Raden Patah No. 81 Batam dengan menggunakan *IP Address* 222.124.136.81 terdakwa telah mengganti tampilan muka (*homepage*) *www.golkar.or.id* yang semula dari wajah tokoh-tokoh partai Golkar diganti dengan gambar gorila putih yang sedang tersenyum yang didapat terdakwa dari google, kemudian terdakwa *link* ke suatu situs di internet;
- kemudian, pada hari Minggu tanggal 09 Juli 2006 sekira pukul 01.00 WIB dengan menggunakan komputer pribadi dan akses internet *wireless* dari *provider* Centrum Batam dengan IP *Address* 202.146.235.4 terdakwa melakukan lagi perubahan tampilan *website www.golkar.or.id* tersebut dengan gambar wanita cantik *sexy* sedang memegang buah dada disertai dengan tulisan bersatu untuk malu;
- selanjutnya, pada tanggal 13 Juli 2006 dengan menggunakan komputer pribadi dan akses internet *wireless* dari *provider* Centrum Batam dengan *IP Address* 202.146.235.4 terdakwa telah mengganti tampilan muka *website* Golkar nomor *www.golkar.or.id* dengan gambar gorila putih sedang tersenyum yang didapat terdakwa dari google, kemudian terdakwa *link* ke suatu situs di internet dengan tulisan bersatu untuk malu;

- pada saat melakukan perubahan tampilan muka *website* Golkar tersebut, terdakwa tidak mempunyai ijin dari pihak Golkar atau surat ijin dari pihak berwenang, oleh karena itu terdakwa serta barang buktinya dibawa ke kantor MABES POLRI untuk pemeriksaan selanjutnya;
- Berdasarkan hasil analisis dari Laboratorium Komputer Forensik BARESKRIM POLRI No. Lab 12 / VIII / 2006 / LABKOMFOR, tanggal 02 Agustus 2006, disimpulkan bahwa :
  1. Pada barang bukti nomor 65 / BB / 2006 / LKF didapatkan bukti-bukti kode / *scrift* program yang digunakan oleh penyerang untuk menyerang *website* *www.golkar.or.id*, dan *log http access* (bukti kunjungan) *website* *www.golkar.or.id*.----------
  2. Pada barang bukti nomor 63 / BB / 2006 / LKF didapatkan bukti-bukti bahwa barang bukti tersebut pernah digunakan untuk melakukan serangan terhadap *website* *www.golkar.or.id*. Hal ini dapat dilihat dari bukti *internet history*, dan *html Carver* (dengan hasil pemeriksaan dan *print out* terlampir) .----------
  3. Pada barang bukti nomor 64 / BB / 2006 / LKF tidak diketemukan bukti penggunaan barang bukti tersebut untuk melakukan serangan terhadap *website* *www.golkar.or.id*.

-- Perbuatan terdakwa **Iqra Syafaat**, sebagaimana diatur dan diancam pidana dalam **Pasal 22 huruf b jo. Pasal 50 UU RI No.36 Tahun**

1999 tentang Telekomunikasi jo. Pasal 64 ayat (1) KUHP.----------

atau,

KEDUA :

--------- Bahwa terdakwa Iqra Syafaat, pada hari-hari Sabtu tanggal 08 Juli 2006 sekira pukul 21.00 WIB., Minggu tanggal 09 Juli 2006 sekira pukul 01.00 WIB., Senin tanggal 10 Juli 2006 sekira pukul 13.00 WIB., Selasa tanggal 11 Juli 2006 sekira pukul 11.00 WIB dan hari Jum'at tanggal 14 Juli 2006 sekira pukul 01.00 WIB atau setidak-tidaknya pada beberapa hari dibulan Juli 2006, dan perbuatan terdakwa sedemikian rupa, sehingga harus dipandang sebagai perbuatan berlanjut, bertempat di warung internet/Warnet Barelang Jalan Raden Patah No. 81 dan di Bukit Timur RT. 04/RW. 06 No. 4 Tanjung Uma Batam atau setidak-tidaknya di suatu tempat, namun berdasarkan ketentuan dalam Pasal 84 ayat (2) KUHAP Pengadilan Jakarta Barat berwenang memeriksa dan mengadili perkara ini ***dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian milik orang lain***, yang dilakukan terdakwa dengan cara sebagai berikut :

- Bahwa pada hari Sabtu tanggal 08 Juli 2006 bertempat di warnet Barelang Jalan Raden Patah No. 81 Batam dengan menggunakan *IP Address* 222.124.136.81 terdakwa telah mengganti tampilan muka (*homepage*) www.golkar.or.id yang semula dari wajah tokoh-tokoh partai Golkar diganti dengan gambar gorila putih yang sedang

tersenyum yang didapat terdakwa dari google, kemudian terdakwa *link* ke suatu situs di internet;

- kemudian, pada hari Minggu tanggal 09 Juli 2006 sekira pukul 01.00 WIB dengan menggunakan komputer pribadi dan akses internet *wireless* dari *provider* Centrum Batam dengan IP *Address* 202.146.235.4 terdakwa melakukan lagi perubahan tampilan *website* *www.golkar.or.id* tersebut dengan gambar wanita cantik *sexy* sedang memegang buah dada disertai dengan tulisan bersatu untuk malu;
- selanjutnya, pada tanggal 13 Juli 2006 dengan menggunakan komputer pribadi dan akses internet *wireless* dari *provider* Centrum Batam dengan *IP Address* 202.146.235.4 terdakwa telah mengganti tampilan muka *website* Golkar nomor www.golkar.or.id dengan gambar gorila putih sedang tersenyum yang didapat terdakwa dari google, kemudian terdakwa *link* ke suatu situs di internet dengan tulisan bersatu untuk malu;
- pada saat melakukan perubahan tampilan muka *website* Golkar tersebut, terdakwa tidak mempunyai ijin dari pihak Golkar atau surat ijin dari pihak berwenang, oleh karena itu terdakwa serta barang buktinya dibawa ke kantor MABES POLRI untuk pemeriksaan selanjutnya;
- Berdasarkan hasil analisis dari Laboratorium Komputer Forensik BARESKRIM POLRI No. Lab 12 / VIII / 2006 / LABKOMFOR, tanggal 02 Agustus 2006, disimpulkan bahwa :

a. Pada barang bukti nomor 65 / BB / 2006 / LKF didapatkan bukti-bukti kode / *scrift* program yang digunakan oleh penyerang untuk menyerang *website* *www.golkar.or.id*, dan *log http access* (bukti kunjungan) *website* *www.golkar.or.id*.----------

b. Pada barang bukti nomor 63 / BB / 2006 / LKF didapatkan bukti-bukti bahwa barang bukti tersebut pernah digunakan untuk melakukan serangan terhadap *website* *www.golkar.or.id*. Hal ini dapat dilihat dari bukti *internet history*, dan *html Carver* (dengan hasil pemeriksaan dan *print out* terlampir) .----------

c. Pada barang bukti nomor 64 / BB / 2006 / LKF tidak diketemukan bukti penggunaan barang bukti tersebut untuk melakukan serangan terhadap *website* *www.golkar.or.id*.----------

-- Perbuatan terdakwa **Iqra Syafaat**, sebagaimana diatur dan diancam pidana dalam **Pasal 406 KUHP. jo Pasal 64 ayat (1) KUHP.**----------

SURAT :

- BAP. Lab.Krim. Laboratorium Komputer Forensik MABES POLRI No.12 / VIII / LABKOMFOR tanggal 22 Agustus 2006 pada kesimpulannya menerangkan bahwa :

  1. Pada barang bukti nomor 65 / BB / 2006 / LKF didapatkan bukti-bukti kode / *scrift* program yang digunakan oleh penyerang untuk menyerang *website* www.golkar.or.id, dan log http access (bukti kunjungan) *website* www.golkar.or.id.----------

2. Pada barang bukti nomor 63 / BB / 2006 / LKF didapatkan bukti-bukti bahwa barang bukti tersebut pernah digunakan untuk melakukan serangan terhadap *website* *www.golkar.or.id*. Hal ini dapat dilihat dari bukti *internet history*, dan *html Carver* (dengan hasil pemeriksaan dan print out terlampir) .----------
3. Pada barang bukti nomor 64 / BB / 2006 / LKF tidak diketemukan bukti penggunaan barang bukti tersebut untuk melakukan serangan terhadap *website* *www.golkar.or.id*.----------

PETUNJUK :

Berdasarkan fakta-fakta yang terungkap dalam persidangan, maka sampailah kami kepada pembuktian mengenai unsur-unsur tindak pidana yang didakwakan pada dakwaan kesatu, yaitu :

Pasal 22 huruf b jo. Pasal 50 UU RI No.36 Tahun 1999 tentang Telekomunikasi jo. Pasal 64 ayat (1) KUHP.

- **Pasal 22 huruf b jo. Pasal 50 UU RI No.36 Tahun 1999 tentang Telekomunikasi**, dengan unsur-unsur sebagai berikut :

1. ***Setiap orang* :**

   Bahwa yang dimaksud “unsur setiap orang” ialah Subyek Hukum yang kepadanya dapat diminta pertanggungjawaban atas semua perbuatannya dan dalam perkara ini, berdasarkan Berita Acara Penyidikan dalam Berkas Perkara dari Penyidik yang berkaitan erat dengan surat dakwaan Jaksa Penuntut Umum yang keseluruhannya

menunjuk pada diri terdakwa Iqra Syafaat. Dengan demikian, menurut kami unsur ini sudah terpenuhi.

2. ***dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi akses ke jasa telekomunikasi*** :

Berdasarkan keterangan saksi-saksi dan keterangan Ahli serta pengakuan terdakwa Iqra Syafaat dipersidangan, bahwa terdakwa telah melakukan *deface* atau perusakan tampilan terhadap *website* *www.golkar.or.id*. adalah dengan cara memanfaatkan *bugs mambo* yang didapat dari *milworm.com*., mencari target di *google.co.id*, dan kebetulan terdakwa dapat *www.golkar.or.id*. kemudian masuk ke servernya lalu meng-*upload file backdoor mod.access php* ke *folder* *http://www.golkar.or.id/modules/mod_access_php*; *Deface* tersebut pertama dilakukan pada tanggal 9 Juli 2006 jam 01.00 WIB dengan menggunakan *IP Address* 222.124.136.81, yaitu terdakwa mengganti halaman depannya yang semula gambar tokoh-tokoh Golkar, diganti dengan gambar wanita *sexy* berbaju renang dengan memegang buah dada, yang didapat dari *search engine* google dengan tulisan "Bersama untuk malu" dan yang kedua tanggal 10 Juli 2006 jam 13.00 WIB dengan menggunakan *IP Address* 222.124.136.101, dari Warnet Barelang di Jalan Raden Fatah No. 81 Batam dengan menggunakan komputer milik warnet tersebut, terdakwa mengganti lagi halaman depannya yang semula gambar tokoh-tokoh Golkar, diganti dengan gambar "Gorilla Putih" yang didapat dari *search*

engine google dengan tulisan ”Bersama untuk malu”. Semula terdakwa menggunakan *website* tersebut untuk *proxy*, tetapi tidak bisa, akhirnya iseng saja melakukan *deface* untuk menguji sistem keamanan *website* www.golkar.or.id. tersebut, dan terdakwa mengganti dengan gambar wanita *sexy* berbaju renang dengan memegang buah dada, karena gambar wanita tersebut cantik dan *sexy*, sedangkan gorilla putih karena lucu sebab gorilla tersebut sedang nyengir, sedangkan tulisan bersatu untuk malu merupakan plesetan dari kata bersatu untuk maju. Terdakwa tidak tahu akan sanksi serta akibatnya atas perbuatannya karena semula hanya iseng saja, terdakwa merasa menyesal telah melakukan perbuatan *deface* tersebut.

Dengan demikian, unsur ini telah terpenuhi.

- Pasal 64 ayat (1) KUHP, dengan unsur-unsur sebagai berikut :

Jika antara beberapa perbuatan, meskipun masing-masing merupakan kejahatan atau pelanggaran, ada hubungannya sedemikian rupa sehingga harus dipandang sebagai satu perbuatan berlanjut, maka hanya diterapkan yang memuat ancaman pidana pokok yang paling berat :

Berdasarkan keterangan saksi-saksi dan keterangan Ahli serta pengakuan terdakwa Iqra Syafaat dipersidangan, bahwa terdakwa telah melakukan *deface* atau perusakan tampilan terhadap website www.golkar.or.id. tersebut beberapa kali, yaitu pertama dilakukan pada tanggal 9 Juli 2006 jam 01.00 WIB dengan menggunakan *IP Address* 222.124.136.81, yaitu

terdakwa mengganti halaman depannya yang semula gambar tokoh-tokoh Golkar, diganti dengan gambar wanita *sexy* berbaju renang dengan memegang buah dada, yang didapat dari *search engine* google dengan tulisan “Bersama untuk malu” dan yang kedua tanggal 10 Juli 2006 jam 13.00 WIB dengan menggunakan *IP Address* 222.124.136.101, dari Warnet Barelang di Jalan Raden Fatah No. 81 Batam dengan menggunakan komputer milik warnet tersebut, terdakwa mengganti lagi halaman depannya yang semula gambar tokoh-tokoh Golkar, diganti dengan gambar ”Gorilla Putih” yang didapat dari *search engine google* dengan tulisan ”Bersama untuk malu”.

Bahwa perbuatan-perbuatan terdakwa tersebut mempunyai hubungan sedemikian rupa yang ditujukan terhadap satu sasaran yaitu serangan terhadap situs golkar, sehingga dapat dipandang sebagai satu perbuatan yang berlanjut.

Dengan demikian, unsur inipun telah terpenuhi.

Berdasarkan uraian-uraian seperti tersebut fakta perbuatan terdakwa telah terbukti secara sah dan meyakinkan terdakwa bersalah melakukan tindak pidana tanpa hak, tidak sah atau memanipulasi akses ke jasa telekomunikasi sebagaimana diatur dan diancam dalam **Pasal 22 huruf b jo. Pasal 50 UU RI No.36 Tahun 1999 tentang Telekomunikasi**, sesuai dengan dakwaan kesatu.

M E N U N T U T :

Agar Majelis Hakim Pengadilan Negeri Jakarta Barat, yang memeriksa dan mengadili perkara ini memutuskan :

1. Menyatakan terdakwa **Iqra Syafaat, melakukan tindak pidana tanpa hak, tidak sah atau memanipulasi akses ke jasa telekomunikasi sebagaimana diatur dalam Pasal 22 huruf b jo. Pasal 50 UU RI No.36 Tahun 1999 tentang Telekomunikasi** ;
2. Menjatuhkan pidana terhadap terdakwa **Iqra Syafaat**, dengan pidana penjara selama 2 (dua) tahun, dikurangi selama masa tahanan sementara, mewajibkan terdakwa membayar denda sebesar Rp. 5.000.000,- (Lima Juta Rupiah) subsidair 5 (lima) bulan kurungan ;
3. Menyatakan barang bukti berupa :

   - 1 (satu) keping kaset CD berisi Log File Golkar, 7 (tujuh) bundel Hard Copy, 1 (satu) buah Hard Disc, 1 (satu) eksemplar print out billing warnet dikembalikan kepada saksi pelapor, 1 (satu) unit CPU dan 1 (satu) unit Laptop dirampas untuk dimusnahkan.
4. Menetapkan supaya terdakwa membayar biaya perkara sebesar Rp. 1000,- (seribu Rupiah).

Demikian Tuntutan Pidana ini kami bacakan dan diserahkan dalam sidang hari ini Selasa tanggal 23 Januari 2007,-

Penyajian Putusan dan Analisis

1) Nomor Registrasi Perkara No. : 3205 / Jkt. Brt. / 10 / 2006

P U T U S A N

NOMOR : 3254/PID.B/2006/PN.JKT.BAR

DEMI KEADILAN BERDASARKAN KETUHANAN YANG MAHA ESA.

Pengadilan Negeri Jakarta Barat yang memeriksa dan mengadili perkara-perkara pidana dengan acara pemeriksaan secara biasa, telah menjatuhkan Putusan sebagai tersebut dibawah ini dalam perkara atas nama Terdakwa :

Nama	:	**IQRA SYAFAAT**
Tempat lahir	:	Batam
Umur/Tgl.lahir	:	27 Tahun/ 21 Juli 1979
Jenis Kelamin	:	Laki-laki
Kebangsaan	:	Indonesia
Tempat tinggal	:	Batu Merah Rt.15/04 Baru Merah, Batu Amper Batam
Agama	:	Islam
Pekerjaan	:	Swasta
Pendidikan	:	SMA

Terdakwa ditahan sejak tanggal 03 Agustus 2006 sampai sekarang;

Terdakwa tidak didampingi Penasehat Hukum ;

Pengadilan Negeri tersebut ;

Setelah membaca berkas perkara ;

Setelah mendengar keterangan saksi-saksi dan keterangan Terdakwa serta barang bukti yang diajukan di persidangan ;

Setelah mendengar Tuntutan Pidana dari Jaksa Penuntut Umum yang pada pokoknya memohon agar Majelis Hakim yang memeriksa dan

mengadili perkara ini menjatuhkan Putusan menyatakan terdakwa terbukti bersalah melakukan tindak pidana sebagaimana dakwaan Penuntut Umum Menghukum Terdakwa dengan pidana penjara selama 2 (dua) tahun potong tahanan dan denda sebesar Rp. 5.000.000,- (Lima Juta Rupiah) subsidair 5 (lima) bulan kurungan dengan perintah terdakwa tetap ditahan, barang bukti dirampas untuk dimusnahkan dan membebankan kepada Terdakwa untuk membayar biaya perkara sebesar Rp. 1.000,- (Seribu Rupiah) ;

Setelah mendengar pembelaan Terdakwa yang diajukan secara lisan pada pokoknya Terdakwa menyesali perbuatannya dan berjanji tidak mengulangi perbuatannya serta mohon keringanan hukuman ;

Setelah mendengar Dakwaan Jaksa Penuntut Umum yang pada pokoknya Terdakwa telah melakukan tindak pidana sebagaimana diatur dan diancam pidana dalam Pasal 22 huruf b jo. Pasal 50 Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi ;

Menimbang, bahwa dipersidangan atas persetujuan Terdakwa telah didengar keterangan saksi-saksi dan keterangan ahli yang telah memberikan keterangan bersesuaian dengan keterangannya dalam BAP Penyidik, yang ternyata dibenarkan oleh Terdakwa ;

Menimbang, bahwa dipersidangan Terdakwa telah memberikan keterangan-keterangan yang pada pokoknya bersesuaian dengan keterangannya dalam BAP Penyidik ;

Menimbang, bahwa berdasarkan keterangan saksi-saksi dan keterangan Terdakwa dihubungkan dengan barang bukti yang diajukan kepersidangan, maka telah terungkap fakta hukum dimana terdakwa telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana sebagaimana yang didakwakan oleh Penuntut Umum ;

Menimbang, bahwa oleh karena Terdakwa telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana, maka terhadap diri Terdakwa haruslah dijatuhi pidana yang setimpal dengan perbuatannya ;

Menimbang, bahwa selain pidana penjara terhadap Terdakwa juga dihukum untuk membayar denda yang besarnya sebagaimana akan disebutkan dalam amar putusan dibawah ini ;

Menimbang, bahwa oleh karena Terdakwa berada dalam tahanan, maka masa penahanan yang telah dijalani oleh Terdakwa dikurangkan seluruhnya dari pidana yang dijatuhkan ;

Menimbang, bahwa oleh karena Terdakwa terbukti bersalah dan dijatuhi pidana maka kepada Terdakwa harus pula dihukum untuk membayar biaya perkara ;

Menimbang, bahwa sebelum menjatuhkan putusan, perlu dipertimbangkan hal-hal sebagai berikut :

Yang Memberatkan :

- Perbuatan Terdakwa dikhawatirkan dapat menurunkan karakter / kredibilitas dari suatu instansi/badan atau partai tertentu ;

Yang Meringankan :

- Terdakwa mengakui terus terang akan perbuatannya ;
- Terdakwa merasa menyesal dan berjanji tidak akan mengulangi lagi akan perbuatan yang telah ia lakukan ;
- Terdakwa belum pernah dihukum ;

Menimbang, bahwa dengan memperhatikan hal-hal sebagaimana yang telah Majelis pertimbangkan diatas, maka akhirnya Majelis sampai pada suatu kesimpulan bahwa pidana yang akan dijatuhkan kepada Terdakwa seperti tersebut dalam amar putusan ini merupakan suatu tindak pidana yang dianggap adil dan bijaksana sesuai dengan rasa keadilan ;

Memperhatikan pasal-pasal dari Undang-Undang dan Peraturan Hukum lain yang bersangkutan ;

M E N G A D I L I :

1. Menyatakan Terdakwa Iqra Syafaat telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana “Tanpa hak, tidak sah memanipulasi akses jaringan telekomunikasi” ;
2. Menjatuhkan pidana terhadap Terdakwa oleh karena itu dengan pidana penjara selama 1 (satu) tahun dan 2 (dua) bulan ;
3. Menetapkan lamanya Terdakwa dalam tahanan dikurangkan seluruhnya dari pidana yang dijatuhkan ;
4. Memerintahkan agar Terdakwa tetap ditahan ;
5. Menetapkan barang bukti berupa :
   a. 1 (satu) keping kaset CD berisi log file Golkar ;

b. 7 (tujuh) bundle hard copy ;

c. 1 (satu) buah hard disk ;

d. 1 (satu) eksampler print out billing warnet ;

Dikembalikan kepada DPP Partai Golkar ;

Sedangkan 1 (satu) unit laptop dirampas untuk dimusnahkan ;

6. Menghukum Terdakwa untuk membayar biaya perkara sebesar Rp. 1.000,- (seribu rupiah) ;

Demikianlah diputuskan dalam rapat musyawarah Majelis Hakim Pengadilan Negeri Jakarta Barat pada hari : KAMIS, TANGGAL : 25 Januari 2007, oleh Kami : SOLAHUDDIN, SH, sebagai Hakim Ketua, NY. HANIZAH IBRAHIM, SH.MH dan SUTARTO KS, SH.MH, masing-masing sebagai Hakim Anggota, pada hari itu juga putusan tersebut diucapkan dalam persidangan yang terbuka untuk umum oleh Hakim Ketua tersebut dengan dihadiri Hakim-Hakim Anggota tersebut, dibantu : MURATNO, SH, Panitera Pengganti Pengadilan Negeri Jakarta Barat, dengan dihadiri SUWASTI, SH, Jaksa Penuntut Umum dan Terdakwa dan Penasehat Hukumnya,-

Analisis Perkara

Berdasarkan pemeriksaan dan analisa laboratorium komputer forensik di BARESKRIM MABES POLRI, penyidik menemukan pola serangan dari Batam menggunakan tiga *IP Address* yaitu 222.124.136.52,

222.124.136.81, 222.124.136.101. Ketiganya diketahui milik PT Inforsys Indonesia. Petrus Reinhard Golose menambahkan, berdasarkan pemeriksaan teknisi IT PT. Inforsys Indonesia, *IP Address* 222.124.136.81 digunakan oleh Warnet Barelang. Selain di warnet, Iqra juga melancarkan penyerangannya (*deface* atau merubah tampilan *website*) di rumahnya kawasan Tanjung Uma, Batam dengan menggunakan laptop pribadi yang dengan putusan pengadilan berkekuatan hukum yang tetap dirampas untuk dimusnahkan. Menurut Reda Manthovani, *Internet Protocol* (*IP*) adalah sebuah "Tanda Bukti Diri" yang memberikan identitas diri di internet atau pengguna komputer. Dengan nomor *IP* inilah pengguna komputer dikenal di internet dan dengan nomor tersebut pengguna komputer dapat terdeteksi karena melakukan kejahatan di internet. Selain itu, menurut beliau, nomor *IP* dapat juga dinamakan dengan alamat *IP* karena dengan nomor tersebut dapat menunjukkan keberadaan pengguna komputer itu sendiri. Dengan meneliti dan memeriksa pemilik nomor *IP* akan dapat diketahui lokasi pengguna *IP* tersebut.[112] Seperti halnya penyidik Polri dalam hasil analisa Laboratorium Komputer Forensik yang menemukan lokasi Iqra Syafaat. Undang-Undang No.36 Tahun 1999 tidak mengatur mengenai alat bukti tersendiri atau alat bukti tambahan selain yang diatur dalam KUHAP, sehingga alat bukti yang digunakan ialah yang diatur dalam KUHAP, yaitu keterangan saksi, surat, keterangan ahli, petunjuk, keterangan terdakwa. Sedangkan alat bukti yang ada dalam kasus Iqra Syafaat ini merupakan

[112] Reda Manthovani, 2006, *Problematika dan Solusi Penanganan Kejahatan Cyber di Indonesia*, Malibu, Jakarta, Hal. 78

alat bukti elektronik (*digital evidence*) yang berupa angka-angka digital dan data-data elektronik, seperti *log file* di Warnet Barelang, *print out billing* warnet, dan *log file* Golkar. Dalam kasus ini, data-data digital dan bukti elektronik tersebut di *print out* dan dicetak didalam kertas oleh Laboratorium Forensik Komputer BARESKRIM MABES POLRI dan dihadirkan di persidangan berupa 7 (tujuh) bundel *Hard Copy* sehingga data digital tersebut dikategorikan menjadi alat bukti surat dan/atau petunjuk. Keterangan saksi dalam kasus Tindak Pidana Telekomunikasi ini terdapat hubungan satu sama lain sehingga mendukung terjadinya Tindak Pidana Telekomunikasi. Hal ini dapat dilihat dari keterangan saksi-saksi dari DPP Golkar yang melihat sendiri bahwa *website* Golkar telah dirubah tampilan situsnya beberapa hari tertentu. Keterangan saksi ini didukung oleh *electronic evidence* berupa *hard disc* milik partai Golkar yang semula berisi *data base* dari *file-file* Golkar telah rusak karena perbuatan *deface*. Bahwa berdasarkan hasil analisa Laboratorium Komputer Forensik MABES POLRI, akses *log file* menerangkan pada suatu peristiwa pidana yang mengarah kepada terdakwa Iqra Syafaat. Mengenai keterangan saksi yang diberikan oleh Agus Haryanto dengan *nickname* "hantu", ia dan terdakwa *chatting*/berdiskusi via internet sehingga untuk keperluan penyelidikan dan penyidikan, ia diminta keterangannya sehubungan dengan kejahatan *deface* ini. Keterangan ini dalam hukum acara kita dikenal sebagai *testimonium de auditu* atau *hearsay evidence*, dimana keterangan saksi tersebut didapat dari orang lain

atau tidak dialami/dilihat/didengar sendiri mengingat pelaku dalam kejahatan dunia maya ini bersifat *virtual anonymous* (dengan nama yang tak dikenal/*nickname*). Keterangan ini tidak memiliki kekuatan pembuktian yang sah sebagai alat bukti keterangan saksi, namun dapat dijadikan bahan pertimbangan keyakinan hakim sebelum menjatuhkan putusan. Keterangan saksi yang menghasilkan informasi hasil interaksi via *internet* (*chatting*) harus ada persesuaiannya dengan keterangan saksi yang lain atau dengan alat bukti lain yang sah di persidangan. Berdasarkan keterangan ahli dari Freddy Harris, modus operandi yang dilakukan terdakwa ialah dengan cara mencari kelemahan dalam sistem operasi yang digunakan karena terdakwa tidak memiliki *password* atau bukan orang yang berwenang dan mempunyai hak untuk merubah tampilan *website* tersebut.

Walaupun dalam hukum positif Indonesia, penggunaan bukti elektronik (*digital evidence*) tidak tegas diatur sebagaimana diatur oleh beberapa negara, namun bukti-bukti elektronik (*electronic evidence*) dalam pemeriksaan di Pengadilan Jakarta Barat tersebut setelah dianalisa Laboratorium Komputer Forensik MABES POLRI dan dituangkan dalam BAP, maka dapat dikategorikan alat bukti Surat sebagaimana diatur didalam Pasal 187 KUHAP. Sepanjang surat digital ini diperoleh dari sebuah sistem jaringan komputer yang *secure* dan *trustworthy* (aman dan layak dipercaya) yaitu dari Laboratorium Komputer Forensik MABES POLRI, informasi yang tertera meskipun dalam bentuk digital memiliki

kekuatan pembuktian yang sama dengan alat bukti surat berdasarkan pasal 187 KUHAP. Hal ini dikarenakan tidak merubah isi dan esensi dari informasi tersebut. Berdasarkan pernyataan terdakwa dan setelah dilakukan *cross evidence* dengan keterangan saksi, semula terdakwa menggunakan *website* tersebut untuk *proxy*, tetapi tidak bisa, akhirnya iseng saja melakukan *deface* untuk menguji sistem keamanan *website* golkar tersebut.

BAB V

KESIMPULAN DAN SARAN

A. Kesimpulan

1. Berdasarkan kasus-kasus yang diteliti penulis, Bukti-bukti Elektronik (*Electronic Evidence*) yang digunakan untuk membuktikan perkara kejahatan dunia maya dalam pemeriksaan di Pengadilan adalah berupa Tampilan Situs yang Terkena *Deface* (yang dirubah tampilan *website*-nya) dan *Log-log File* (waktu terjadinya perbuatan tersebut) serta *Internet Protocol (IP)* yang dijadikan "Tanda Bukti Diri" yang dapat mendeteksi pelaku Kejahatan Dunia Maya dan dapat menunjukkan keberadaan pengguna komputer itu sendiri. Dengan meneliti dan memeriksa pemilik nomor *IP* akan dapat diketahui lokasi pengguna *IP* tersebut.
2. Bukti-bukti Elektronik yang ditemukan Penyidik dianalisa melalui Laboratorium Komputer Forensik yang dapat menerangkan pada suatu peristiwa pidana yang mengarah kepada Terdakwa dan menimbulkan akibat hukum.

   Bagi penyidik sangat penting untuk memperoleh informasi melalui *crime scene search* (penyidikan di tempat kejadian perkara) yang bertumpu pada komputer untuk menjaga keaslian dan keotentikan dari Bukti Elektronik tersebut sebelum dianalisa oleh LABKOMFOR.
3. Bukti-bukti Elektronik yang ditemukan tersebut setelah dianalisa Laboratorium Komputer Forensik kemudian dicetak ke dalam media

kertas oleh LABKOMFOR dan dihadirkan di persidangan melalui Metode Penafsiran Ekstensif yang pada prinsipnya dikategorikan sebagai Alat Bukti Surat dan/atau Petunjuk sebagaimana diatur dalam Pasal 184 KUHAP sebagai alat bukti yang sah di Muka Pengadilan.

4. Dalam pemeriksaan kejahatan dunia maya di Pengadilan, seorang Ahli memegang peranan yang sangat penting untuk memberikan keterangan yang berkaitan dengan rekaman/salinan data (*data recording*) yang menjadi Bukti Elektronik tersebut apakah sudah berjalan sesuai dengan prosedur yang berlaku (telah dikalibrasi dan diprogram) serta diperoleh dari sebuah sistem jaringan komputer yang *secure and trustworthy* (aman dan layak dipercaya) sedemikian rupa sehingga hasil *print-out* suatu Bukti Elektronik tersebut dapat terjamin keotentikannya dan dapat diterima dalam pembuktian perkara kejahatan dunia maya sebagai alat bukti yang sah dan yang dapat berdiri sendiri sebagai *Real Evidence*.

   Kedudukan seorang Ahli sebagai *Testamentary Evidence* ini sangat penting untuk memperjelas kejahatan dunia maya yang terjadi serta dapat menerangkan/menjelaskan validitas suatu Bukti Elektronik yang memberikan keyakinan Hakim dalam memutus perkara kejahatan dunia maya.

5. Dalam mengungkap kasus kejahatan dunia maya serta menemukan tersangkanya, penyidik menggunakan salah satu alat investigasi standart (*standart investigation tools*) antara lain teknik *Virtual Undercover* yang memberikan informasi sebagai dasar bagi suatu kasus, yaitu melakukan

chatting (interaksi via internet) untuk mendapatkan informasi yang berkaitan dengan perkara kejahatan dunia maya yang terjadi dan pelakunya.

Keterangan saksi ini dalam Hukum Acara Pidana kita dikenal sebagai *testimonium de auditu*, dimana keterangan saksi tersebut didapat dari orang lain/tidak dialami/dilihat/didengar sendiri mengingat pelaku kejahatan dunia maya bersifat *Virtual Anonymous* (dengan nama yang tak dikenal/*nickname*). Keterangan ini tidak memiliki kekuatan pembuktian yang sah sebagai alat bukti keterangan saksi. *Circumstantial Evidence* ini adalah bukti terperinci yang diperoleh berdasarkan ucapan/pengamatan dari kejadian yang sebenarnya yang mendorong untuk mendukung suatu kesimpulan, tetapi bukan untuk membuktikannya, melainkan dapat dijadikan bahan pertimbangan yang dapat memperkuat keyakinan Hakim sebelum menjatuhkan putusan dimana keyakinannya tersebut bersumber kepada minimal dua alat bukti sah yang dihadirkan di persidangan.

B. Saran

Adapun saran-saran yang diusulkan penulis atas dasar pemikiran yang didapat selama melakukan penelitian adalah sebagai berikut :

1. Apabila telah ada Undang-undang yang menerima keberadaan sistem *security* secara baik, maka sepanjang tidak dapat dibuktikan lain, Subyek Hukum yang tercatat oleh sistem tidak dapat menampiknya karena “telah dianggap” sebagai pihak yang telah terbukti melakukan perbuatan

kejahatan dunia maya dan dapat diminta pertanggungjawabannya atas informasi berupa bukti - bukti elektronik yang ditemukan tersebut. (Hasil wawancara dengan Edmon Makarim pada tanggal 19 April 2007)

2. Apabila kita melihat perkembangan zaman yang diikuti dengan berkembangnya modus operandi yang dilakukan oleh pelaku kejahatan dunia maya, namun belum ada regulasi yang secara jelas dan tegas mengatur mengenai bukti-bukti elektronik dalam hukum pembuktian di Muka persidangan, maka Penulis berpandangan bahwa seyogyanya hakim harus mencari dan menemukan hukumnya, yaitu melakukan penemuan hukum (*rechtsvinding*). Menurut Sudikno Mertokusumo dan A. Pitlo didalam bukunya "Bab-Bab tentang Penemuan Hukum" mengemukakan dalam penemuan hukum ini, hakim beraliran progresif yang berpendapat bahwa hukum dan peradilan merupakan alat untuk perubahan-perubahan sosial. Interpretasi atau penafsiran ekstensif merupakan salah satu bentuk perwujudan dari penemuan hukum. Hal ini diperlukan mengingat urgensi produk hukum di bidang kejahatan dunia maya yang akan memperluas pengertian dari peraturan perundang-undangan yang sudah ada serta alat buktinya. Apabila kejahatan tersebut dilakukan secara elektronik (*online*), otomatis maka alat-alat buktinya pun bersifat elektronik. Seandainya ternyata tidak ada produk hukum yang secara khusus dan tegas mengatur mengenai kejahatan dunia maya serta pembuktiannya yang berupa data-data digital, seyogyanya menurut Penulis, bukti elektronik yang diketemukan tersebut apabila melalui suatu tahap *Standart Operating*

Procedure seperti yang dilakukan oleh Laboratorium Komputer Forensik dan dibuktikan keotentikannya oleh seorang Ahli di persidangan dapat ditafsirkan secara Ekstensif, maka dapat dikategorikan sebagai alat bukti surat dan/atau petunjuk sebagaimana diatur dalam Pasal 184 KUHAP sebagai alat bukti yang sah. Interpretasi ekstensif inipun dilakukan sebagai langkah penegakan hukum yang menjurus pada kepastian hukum dan untuk mencari kebenaran materiil.

3. Pelaku kejahatan dunia maya sudah seharusnya dihukum lebih berat, karena dia menggunakan intelelektualitasnya dalam melakukan kejahatan konvensional dengan modus operandi yang begitu canggih. Pelaku kejahatan dunia maya melihat kesempatan untuk melakukan kejahatan yang oleh orang awam tidak disadari bahkan tidak diketahuinya. Mengacu pada teori prevensi umum dalam Hukum Pidana, tujuan pemidanaan ialah salah satunya untuk menimbulkan rasa jera pada orang lain dan mengacu pada teori prevensi khusus agar pelaku yang bersangkutan tersebut jera dan tidak mengulangi perbuatannya lagi.
4. Pemaparan Bukti Digital (*electronic evidence*)

   Pembuktian dalam pemeriksaan di persidangan memegang peranan yang sangat penting. Hukum Pembuktian mengenal salah satu alat ukur yang menjadi teori pembuktian, yaitu penguraian bagaimana cara menyampaikan alat-alat bukti kepada hakim di sidang pengadilan (*bewijsvoering*). Dalam persidangan, bukti digital akan diuji keotentikannya dengan cara mempresentasikan bukti digital tersebut untuk

menunjukkan hubungan bukti digital yang diketemukan tersebut dengan kasus kejahatan dunia maya yang terjadi. Dikarenakan proses penyidikan, penuntutan sampai dengan proses pemeriksaan di pengadilan memerlukan waktu yang relatif cukup panjang, maka sedapat mungkin bukti digital tersebut masih asli dan sepenuhnya sama (origin) dengan pada saat pertama kalinya diidentifikasi dan dianalisa oleh penyidik dalam hal ini melalui Laboratorium Forensik Komputer. Oleh karena itu, seyogyanya untuk menghemat waktu, menurut Penulis berdasarkan hasil wawancara dengan Edy Hartono pada tanggal 24 April 2007, bukti digital tersebut seyogyanya dapat dipresentasikan secara digital melalui laptop atau komputer tanpa harus dicetak ke dalam media kertas (*print out*).

5. Perlu dilakukannya forum-forum pertukaran pengetahuan dan pengalaman antara para pakar Teknologi Informasi, Aparat Penegak Hukum, dan para teknisi / profesional yang bekerja di bidang Teknologi Informasi.

   Tujuannya adalah untuk dapat mengetahui lebih mendalam perkembangan teknologi dan perkembangan modus operandi dalam kejahatan dunia maya. Hasil-hasil yang diperoleh dari forum-forum tersebut sangat bermanfaat untuk dijadikan masukan bagi Departemen Komunikasi dan Informasi, Departemen Hukum dan HAM dan anggota DPR untuk melakukan perumusan (tahap formulasi) dalam pembentukan dan/atau penyempurnaan RUU Kejahatan Dunia Maya.

   Sebagai contoh yang konkrit, aparat penegak hukum dalam jajaran kepolisian, kejaksaan, para Hakim bahkan para pengacara dapat mengikuti

suatu program peningkatan pengetahuan dan penerapan bukti digital dalam aspek Hukum Pembuktian kejahatan dunia maya. Hal ini menurut Penulis perlu dilakukan supaya interpretasi terhadap penerapan bukti digital dalam Hukum Pembuktian tidak saling bertentangan. Dengan memberikan edukasi mengenai peningkatan pengetahuan di beberapa profesional tertentu dapat meningkatkan kesadaran hukum agar tidak menyalahgunakan pengetahuannya dan/atau ilmunya untuk melakukan kejahatan dunia maya atau bahkan dapat membantu mencegah adanya pelanggaran pidana sebagai tindakan preventif. Hal ini pun dapat difasilitasi melalui Departemen Komunikasi dan Informasi dan juga Departemen Hukum dan HAM. INTERPOL *Secretary General* 'Ronald K. Noble' dalam konferensi Internasional mengenai *cybercrime* di New Delhi, India pada tanggal 12 September 2007 dengan tema "*Upcoming Capacity of Cyber-Police*" menyatakan untuk menghadapi ancaman kejahatan dunia maya diperlukan aparat penegak hukum yang mempunyai keahlian dan kemampuan di bidang *cyber- security* untuk menghadapi dan menanggulangi kejahatan dunia maya yang bersifat transnational. Aparat penegak hukum memiliki peran yang esensial untuk mencegah dan mengusut kejahatan juga termasuk didalamnya kejahatan dunia maya (*cybercrime*) yang dilakukan secara *online* dengan porsi yang sama seperti aparat penegak hukum melindungi warga negaranya dari kejahatan konvensional.

6. RUU ITE (RUU Informasi dan Transaksi Elektronik) telah memberikan tempat agar suatu informasi elektronik dapat diterima dan memberikan prosedur tertentu sebagai pedoman bagi Hakim dalam pemeriksaan dan pembuktian kejahatan dunia maya. Maka, Penulis berharap agar RUU ITE segera disahkan menjadi Undang-undang Informasi dan Transaksi Elektronik yang akan menjadi payung hukum bagi kejahatan dunia maya. (Hasil wawancara dengan Edmon Makarim pada tanggal 19 April 2007)

DAFTAR PUSTAKA

A. Buku

Arief, Barda Nawawi, 2005, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*, Citra Aditya Bakti, Bandung

Arief, Barda Nawawi, 2001, *Masalah Penegakan Hukum dan Penanggulangan Kejahatan*, Citra Aditya Bakti, Bandung

Hamzah, Andi, 2005, H*ukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta

Hamzah, Andi, 1989, *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta

Harahap, M. Yahya, 2006, *Pembahasan Pernasalahan dan Penerapan Hukum Edisi Kedua*, Sinar Grafika, Jakarta

Indradi, Ade Ary Syam, 2006, *Carding Modus Operandi, Penyidikan, dan Penindakan*, Pensil, Jakarta

Krisnawati, Dani dan Hiariej, Eddy O.S, dan Gunarto, Marcus Priyo dan Riyanto, Sigid dan Supriyadi, 2006, *Bunga Rampai Hukum Pidana Khusus*, Pena Pundi Aksara, Jakarta

KUFFAL, HMA, 2005, *Tata Cara Penggeledahan dan Penyitaan*, UMM Press, Malang

Makarim, Edmon, 2003, *Kompilasi Hukum Telematika*, Rajagrafindo Persada, Jakarta

Makarim, Edmon, 2005, *Pengantar Hukum Telematika*, Rajagrafindo Persada, Jakarta.

Makarao, Mohammad Taufik dan Suhasril, 2004, *Hukum Acara Pidana dalam Teori dan Praktek*, Penerbit Ghalia Indonesia, Jakarta

Moeljatno, 2000, *Asas - asas Hukum Pidana*, Rineka Cipta, Jakarta

Moeljatno, 2006, *KUHP*, Bumi Aksara, Jakarta

Poernomo, Bambang, *Pokok-pokok Tata Cara Peradilan Indonesia*, Liberty, Jogjakarta

Prodjodikoro, Wirjono, 2003, *Asas - asas Hukum Pidana*, Refika Aditama, Bandung

Raharjo, Agus, 2002, *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung

Sanusi, M. Arsyad, 2005, *Hukum dan Teknologi Informasi*, Tim KemasBuku, Jakarta

Subekti, 1995, *Hukum Pembuktian*, Pradnya Paramita, Jakarta

Sukismo, B., 2002, *Model Penelitian Hukum*

B. Jurnal

Golose, Petrus Reinhard, "Penegakan Hukum Cyber Crime dalam Sistem Hukum Indonesia" dalam *Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia*, 12 April 2007

Hiariej, Eddy O.S, 28 November 2005, *Materi Kuliah Hukum dan Teknologi*, FH UGM Jogjakarta

Hadiwidjojo, Widyopramono, "Cybercrime dan pencegahannya", *Jurnal Hukum Teknologi*, Volume II, nomor 1, 2005, LKHT FH UI

LKHT FHUI, "Tindak Pidana Telematika", *Jurnal Hukum teknologi*, 2001

Makarim, Edmon, "*Tindak Pidana terkait dengan Komputer dan Internet* : Suatu Kajian Pidana Materiil dan Formil", Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia, 12 April 2007

Polri, "Perkembangan Cyber Crime dan Upaya Penanganannya di Indonesia oleh POLRI ", *Buletin Hukum Perbankan dan kebanksentaralan*, Volume IV, Nomor 2, Agustus 2006

Panjaitan, Hinca IP, "Membangun Cyber Law Indonesia yang Demokratis", IMLPC, *Buletin Hukum Perbankan dan Kesentralan*, 2005

Setiadi, "Penegakan Hukum Terhadap Pelaku Tindak Pidana Internet Banking", *Jurnal Hukum Teknologi*, Volume II, Nomor 1, 2005

Utoyo, Donny Budi,"Kajian Sosial Komunitas Maya Hacker/Cracker", *Jurnal Hukum Teknologi LKHT FHUI*, Volume II, Nomor 1, 2005

C. Peraturan Perundang-undangan

Undang-Undang RI Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP)

Undang - Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang - Undang No. 20 Tahun 2001 tentang Perubahan Atas Undang - Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi

Undang - Undang Nomor 19 Tahun 2002 tentang Hak Cipta

Undang - Undang Nomor 25 Tahun 2003 tentang Pencucian Uang

Undang - Undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang

Keppres Nomor 8 Tahun 1997 tentang Dokumen Perusahaan

Rancangan Undang - Undang KUHP Buku II Tindak Pidana Tahun 2005

Rancangan Undang - Undang KUHAP Tahun 2007

Rancangan Undang - Undang Informasi dan Transaksi Elektronik Tahun 2005

D. Internet

LKHT FH UI, "*Kasus Klik-BCA.com"*, www.lkhtnet.com, diakses pada tanggal 28 Februari 2007

LKHT FH UI, "*Kejahatan dan Komputer"*, www.lkhtnet.com, diakses pada tanggal 28 Februari 2007

Mudiardjo, Rapin, "Data Elektronik sebagai Alat Bukti Masih Dipertanyakan", www.hukumonline.com, diakses pada tanggal 28 Februari 2007

Polri, "*Perusak Situs Golkar Tertangkap*", www.polri.go.id, 10 Agustus 2006, diakses pada tanggal 28 Februari 2007

Petrus Reinhard Golose, "*Rekapitulasi Kejahatan mempergunakan Internet yang dilidik/sidik Unit V IT & CyberCrime tahun 2006"*, *search engine google,* diakses pada tanggal 26 April 2007

Rahardjo, Trisno, Agustus 2006, "Perbandingan Kebijakan Kriminalisasi Tindak Pidana Mayantara", *www.rachdian.pacific.net.id*, diakses pada tanggal 28 Agustus 2007

UU Perdagangan Orang, 2007, www.legalitas.org/incl-php/buka.php?d=2000+7&f=uu21-2007.htm, diakses pada tanggal 27 Februari 2008

RUU KUHP Buku II Tindak Pidana, 2005, www.legalitas.org/database/rancangan/2005/BUKU%20KEDUA%20KUHP.pdf, diakses pada tanggal 27 Februari 2008

RUU KUHAP, 2007, www.legalitas.org/database/rancangan/2007/RUUKUHAP2007.pdf

RUU ITE, 14 Juni 2005, www.legalitas.org/database/rancangan/2005/RUU ITE.doc, diakses pada tanggal 27 Februari 2008

DIREKTORAT II EKONOMI DAN KHUSUS
UNIT V IT & CYBER CRIME
Jl. Trunojoyo No.3 Keb. Baru Jakarta Selatan

Jakarta, 21 Juni 2007

No. Pol. : B/ 01/VI/2007/Cyber Crime
Klasifikasi : Biasa
Lampiran : -
Perihal : Pemberitahuan telah selesai menyusun Skripsi (Penelitian) An. NUURLAILA F. AZIZAH

Kepada

Yth. **DEKAN FAKULTAS HUKUM**
UNIVERSITAS GAJAHMADA

di -

Jogjakarta

Up. DR. MARSUDI TRIHATMODJO, SH., LLM.

1. Rujukan Surat Fakultas Hukum Universitas Gajah Mada kepada Direktur II Ekonomi dan Khusus Nomor : 263/Dir. AA/Pd/2007, tanggal 30 Maret 2007, perihal Ijin Penelitian.

2. Sehubungan dengan perihal tersebut diatas, disampaikan kepada Dekan Fakultas Hukum Unversitas Gajah Mada bahwa mahasiswi yang bernama :

   Nama : NUURLAILA F. AZIZAH
   No. Mahasiswa : 03/169388/HK/16476
   Fakultas : Hukum Universitas Gajah Mada

   Telah selesai melakukan/mendapatkan pengetahuan dan informasi Kepolisian mengenai Cyber Crime pada kantor Unit V IT & Cyber Crime Direktorat II Ekonomi dan Khusus Bareskrim Polri yang akan digunakan untuk menyusun Skripsi dengan judul " Penggunaan Data Elektronik Dalam Pembuktian Perkara Kejahatan Dunia Maya

3. Demikian untuk menjadi maklum.

BADAN RESERSE KRIMINAL POLRI
DIREKTUR
DIREKTORAT II EKONOMI DAN KHUSUS

UNIT V IT & CYBER CRIME

PETRUS REINHARD GOLOSE
KOMBES POLISI NRP 65110481

DIREKTORAT II EKONOMI DAN KHUSUS
UNIT V IT & CYBER CRIME
Jl. Trunojoyo No.3 Keb. Baru Jakarta Selatan

Jakarta, 21 Juni 2007

No. Pol. : B/ 01/VI/2007/Cyber Crime
Klasifikasi : Biasa
Lampiran : -
Perihal : Pemberitahuan telah selesai menyusun Skripsi (Penelitian) An. NUURLAILA F. AZIZAH

Kepada

Yth. **DEKAN FAKULTAS HUKUM**
UNIVERSITAS GAJAHMADA

di -

Jogjakarta

Up. DR. MARSUDI TRIHATMODJO, SH., LLM.

1. Rujukan Surat Fakultas Hukum Universitas Gajah Mada kepada Direktur II Ekonomi dan Khusus Nomor : 263/Dir. AA/Pd/2007, tanggal 30 Maret 2007, perihal Ijin Penelitian.

2. Sehubungan dengan perihal tersebut diatas, disampaikan kepada Dekan Fakultas Hukum Unversitas Gajah Mada bahwa mahasiswi yang bernama :

   Nama : NUURLAILA F. AZIZAH
   No. Mahasiswa : 03/169388/HK/16476
   Fakultas : Hukum Universitas Gajah Mada

   Telah selesai melakukan/mendapatkan pengetahuan dan informasi Kepolisian mengenai Cyber Crime pada kantor Unit V IT & Cyber Crime Direktorat II Ekonomi dan Khusus Bareskrim Polri yang akan digunakan untuk menyusun Skripsi dengan judul " Penggunaan Data Elektronik Dalam Pembuktian Perkara Kejahatan Dunia Maya

3. Demikian untuk menjadi maklum.

BADAN RESERSE KRIMINAL POLRI
DIREKTUR
DIREKTORAT II EKONOMI DAN KHUSUS

UNIT V IT & CYBER CRIME

PETRUS REINHARD GOLOSE
KOMBES POLISI NRP 65110481

PENGADILAN NEGERI JAKARTA BARAT
JL. LET. JEN. S. PARMAN NO. 71 SLIPI
JAKARTA BARAT

SURAT KETERANGAN
NOMOR : W7.Db.Ht.04.10. 2282 /2007

Memenuhi maksud surat a.n. Direktur Administrasi Akademik Sekretaris **UNIVERSITAS GADJAH MADA**, Izin Memperoleh Data, dengan ini kami menerangkan bahwa benar Mahasiswa yang tersebut di bawah ini :

Nama	:	**NUURLAILA F. AZIIZAH**
No. Mahasiswa	:	03/169388/HK/16476
Fakultas	:	HUKUM
Judul	:	Penggunaan Data Elektronika dalam Pembuktian Perkara Kejahatan dalam Dunia Maya.

Demikianlah untuk dapat dipergunakan sebagaimana mestinya.

Jakarta, 10 Juli 2007
KETUA PENGADILAN NEGERI
JAKARTA BARAT
u.b.
WAKIL SEKRETARIS

PENGADILAN NEGERI JAKARTA BARAT

DRS. H. NASRULLAH
NIP : 04 0048743.