ADLN - Perpustakaan Unair

SKRIPSI

PENGGUNAAN ALAT BUKTI DIGITAL MENURUT UNDANG-UNDANG NOMOR 8 TAHUN 1981 TENTANG HUKUM ACARA PIDANA

Fh /07
Pra
1

OLEH :

NOVAN INDRA PRASETYO
NIM. 030115246

FAKULTAS HUKUM
UNIVERSITAS AIRLANGGA
2006

ADLN - Perpustakaan Unair

PENGGUNAAN ALAT BUKTI DIGITAL MENURUT UNDANG-UNDANG NOMOR 8 TAHUN 1981 TENTANG HUKUM ACARA PIDANA

SKRIPSI

Diajukan Untuk Melengkapi Tugas Dan Memenuhi Syarat
Untuk Mencapai Gelar Sarjana Hukum

OLEH :

NOVAN INDRA PRASETYO
NIM. 030115246

DOSEN PEMBIMBING,

Dr. H. Didik Endro Purwoleksono, S.H., M.H.
NIP. 131570341

PENYUSUN,

Novan Indra Prasetyo
NIM. 030115246

FAKULTAS HUKUM
UNIVERSITAS AIRLANGGA
2006

041926

Skripsi ini telah diuji dan dipertahankan dihadapan Panitia Penguji
Pada tanggal 4 September 2006

Panitia Penguji Skripsi :

Ketua : Dr. M. Zaidun, S.H., M.Si. .....

Anggota : 1. Dr. H. Didik Endro Purwoleksono, S.H., M.H. .....

2. Dr. Nur Basuki Minarno, S.H., M.Hum. .....

3. Bambang Suheryadi, S.H., M.Hum. .....

192

ADLN - Perpustakaan Unair

Tidak ada sesuatu yang lebih baik daripada akal yang sehat yang diperindah dengan ilmu dan ilmu yang diperindah dengan kebenaran (shidiq) dan kebenaran yang diperindah dengan kebaikan dan kebaikan yang diperindah dengan takwa.

Skripsi Penggunaan alat bukti digital menurut undang-undang nomor 8 tahun 1981 Nova Indra Prasetyo

KATA PENGANTAR

Puji dan syukur penulis panjatkan atas kehadirat Allah SWT atas segala nikmat dan rahmat yang telah diberikan kepada penulis. Berkat Allah SWT akhirnya penulis berhasil merampungkan skripsi ini. Kebaikan dan kelebihan dari tulisan skripsi ini merupakan rahmat-Nya, dan sebaliknya segala kekurangan yang ada pada tulisan ini tidak lain adalah kekhilafan dari penulis semata.

Penulis menyadari bahwa masih banyak kekurangan dan kelemahan dalam skripsi ini. Oleh karena itu penulis sangat mengharapkan adanya sumbangan saran serta kritik yang membangun dari pembaca yang dapat dijadikan koreksi dan perbaikan bagi penulis dilain waktu. Serta yang terakhir skripsi ini tidak akan terwujud seperti sekarang ini tanpa adanya bantuan dari berbagai pihak yang berperan secara langsung ataupun tidak langsung terhadap proses penyelesaian skripsi ini sampai pada saat proses ujian untuk mempertahankan skripsi ini. Oleh karena itu penulis ingin menyampaikan rasa terima kasih penulis kepada :

1. Fakultas Hukum Universitas Airlangga Surabaya tempat penulis menimba ilmu program studi (S1) ilmu hukum. Banyak sekali kenangan dan ilmu yang sangat bermanfaat yang penulis dapatkan di kampus yang tercinta ini.
2. Bapak Machsoen Ali, S.H.,M.S., selaku Dekan Fakultas Hukum Universitas Airlangga Surabaya.
3. Bapak Dr. H. Didik Endro Purwoleksono, S.H., M.H., selaku dosen pembimbing bagi penulis dalam penulisan skripsi ini.

4. Tim penguji skripsi Bapak Dr. M. Zaidun, S.H., MSi., Bapak Dr. Nur Basuki Minarno, S.H., M.Hum., Bapak Bambang Suheryadi, S.H., M. Hum.
5. Ibu Rr. Herini Siti Aisyah, S.H., MH., selaku dosen wali penulis yang selalu membimbing dalam menentukan mata kuliah yang akan penulis ambil.
6. Bapak dan Ibu Dosen Fakultas Hukum Universitas Airlangga yang telah membimbing dan membagi ilmunya sehingga penulis mempunyai bekal ilmu yang diharapkan dapat digunakan dan dibagi kepada masyarakat.
7. Bapak dan Mama yang telah bekerja keras, membesarkan dan tidak pernah putus asa dalam membimbing penulis dengan harapan agar penulis dapat dihargai oleh orang lain. Dalam kesempatan ini penulis mohon maaf karena belum bisa membalas jasa dan kebaikan beliau berdua bahkan penulis selalu mengecewakan beliau berdua. Terima kasih atas doa dan nasehat yang tidak pernah putus juga kepercayaan yang diberikan kepada penulis dan mohan maaf yang sebesar-besarnya.
8. Saudara-saudara penulis : Mami, Mbak Ayu, Tante Denok, Tante Ithuk, Tante Yeni, Om Tatang (yang akan membentuk keluarga baru) dan Bude, Pakde, Tante serta Om yang lain yang juga telah membimbing dan memberi nasehat kepada penulis.
9. Teman-teman penulis di Fakultas Hukum Unair : Udin (terima kasih atas bimbingan spiritualnya), Epik, Wahyu, Mita, Ata', Nita, anak-anak "Bambu" (Hendik, Rendy, Rustam, Sigia, Dini, Dian, Diah, Yayah, dsb), Jo, Risa, Yavet dan temen-temen yang tidak bisa disebutin satu-persatu karena keterbatasan

tempat.. Terimakasih atas semangat dan dorongan yang telah kalian berikan kepada penulis untuk menyelesaikan skripsi ini.

10. Teman-teman alumni dan anggota Paskibra SMAN 2 Malang : Bang Onal (terima kasih atas bimbingan dan nasehatnya), Diki R.S.D (yang telah memberikan nasehat, bimbingan spiritual dan doa), Agus (maaf belum bisa ke Sempu lagi), Windy, Windiarto, Dhimas S, Sari, Ipeh, Putu(Dewi), Gandhi, Mirzah, Irfan, Gading, Budi, Santi, Elma, Rachma, Lia, Wiena, Ribka, Wilis, Aldhita, Novan dan teman-teman lain yang tidak bisa disebutkan. Terima kasih atas dorongan, motivasi, nasehat dan doa yang sudah diberikan kepada penulis.
11. Dan semua pihak yang tidak dapat penulis sebutkan satu persatu karena keterbatasan tempat. Terima kasih atas segala doa, dukungan dan bantuan yang telah diberikan kepada penulis selama proses penulisan skripsi ini.

Surabaya, 23 Agustus 2006

Novan Indra Prasetyo
NIM. 030115246

ADLN - Perpustakaan Unair

DAFTAR ISI

HALAMAN JUDUL..... i

HALAMAN PENGESAHAN..... iii

KATA PENGANTAR..... vii

DAFTAR ISI..... ix

BAB I : PENDAHULUAN

1. Latar Belakang..... 1
2. Penjelasan Judul..... 12
3. Alasan Pemilihan Judul..... 12
4. Tujuan Penulisan..... 13
5. Metode Penulisan..... 13
   a. Pendekatan Masalah..... 13
   b. Sumber Bahan Hukum..... 14
   c. Prosedur Pengumpulan dan Pengolahan Bahan Hukum..... 14
   d. Analisis Bahan Hukum..... 15
6. Pertanggungjawaban Sistematika Penulisan..... 15

BAB II : PEMBUKTIAN ALAT BUKTI DIGITAL

1. Alat Bukti..... 17

Skripsi Penggunaan alat bukti digital menurut undang-undang nomor 8 tahun 1981 Nova Indra Prasetyo

1.1. Alat Bukti yang Diakui Hukum Acara Pidana..... 17

1.2. Alat Bukti Digital..... 20

2. Pembuktian..... 26

2.1. Sistem Pembuktian yang Dianut dalam KUHAP... 26

2.2. Penerapan Alat Bukti Digital..... 29

BAB III : NILAI HUKUM ALAT BUKTI DIGITAL

1. Pengolahan Alat Bukti Digital 33

2. *Digital Signature*..... 40

2.1. Penggunaan *Digital Signature*..... 40

2.2. *Digital Signature* sebagai Alat Bukti..... 47

BAB IV : PENUTUP

1. Kesimpulan..... 51

2. Saran..... 52

DAFTAR BACAAN

LAMPIRAN

BAB I

PENDAHULUAN

1. Latar Belakang

Keberadaan suatu informasi[1], dalam era informasi mempunyai arti dan peranan yang sangat penting dalam semua aspek kehidupan, serta merupakan suatu kebutuhan hidup bagi semua orang baik secara individual maupun organisasional, sehingga dapat dikatakan berfungsi sebagaimana layaknya suatu aliran darah pada tubuh manusia. *Information is the lifeblood that sustains political social and business decission.*[2] Informasi dapat dikategorikan sebagai suatu komoditi yang tidak pernah punya nilai bagi yang membutuhkannya dan merupakan suatu komoditi yang cukup mahal karena tidak semua pihak mampu memproses data[3] mentah menjadi suatu bentuk dan karakteristik informasi yang sesuai dengan kebutuhan manusia.[4]

Perubahan bentuk masyarakat yang bertahap dari masyarakat pra-sejarah, masyarakat agraris, masyarakat industri kemudian sekarang menjadi suatu masyarakat informasi (*information society*) memicu perkembangan teknologi

---

[1]Keseluruhan makna yang menunjang pesan yang terlihat di bagian-bagian pesan itu.

[2]Edmon Makarim. *Kompilasi Hukum Telematika*, PT. RajaGrafindo Persada, Jakarta, 2003, h. 24. dikutip dari Branscomb. Anne W (ed.)., *Toward a Law of Global Communication Network*, New York & London : Longman, 1986, h. 1.

[3]Kumpulan dari angka-angka maupun karakter-karakter yang tidak memiliki arti. Data dapat diolah sehingga menghasilkan informasi.

[4]Edmon Makarim, *Kompilasi Hukum Telematika*. PT. RajaGrafindo Persada, Jakarta, 2003, h. 24.

ADLN - Perpustakaan Unair

informasi (*information technology revolution*) menjadi kian pesat sehingga terciptalah perangkat-perangkat informatika yang semakin canggih dan jaringan sistem informasi yang kian rumit dan handal, serta mampu memenuhi permintaan semua lapisan masyarakat. Hal ini terlihat pada kenyataan sekarang ini, jika dahulu produk teknologi informatika (contoh: komputer dan perangkat komunikasinya) hanya bisa dinikmati terbatas pada kalangan organisasi bisnis atau perusahaan yang besar, sekarang sudah bisa dinikmati oleh perusahaan kecil dan bahkan sudah merambah ke dalam lingkungan rumah tangga. Semula komputer berukuran besar dan berharga mahal kini komputer menjadi kian kecil sehingga dapat dibawa kemana-mana juga semakin tinggi kemampuannya dan semakin murah pula harganya. Demikian pula dengan sistem informasi organisasional, yang semula bersifat tertutup (*proprietary*) sekarang bersifat terbuka (*open system interconnection*) serta semakin jauh lingkup jaringan komunikasinya (*global communication network)*, sehingga dunia dewasa ini terasa kian dekat dan sempit, terlebih dengan adanya jaringan pintar sedunia (*worldwide intelligent network*) dan IVIS (*Interactive Voice Information System*).[5]

Sekarang ini manusia telah berada dalam perkembangan teknologi elektronik yang berbasiskan lingkungan digital[6], dengan bermula dari diketemukannya semikonduktor[7] yang kini telah menjadi suatu bagian integral

---

[5]*Ibid*, h, 26, dikutip dari *Suara Pembaharuan (Jakarta)*, 28 November 1993, h. 5.

[6]Sinyal yang seperti pulsa, artinya antara bagian-bagian sinyal terlihat terputus-putus. Bagian yang di atas digambarkan sebagai 1 dan bagian yang di bawah digambarkan sebagai 0.

[7]Bahan utama yang digunakan untuk membuat sirkuit terpadu atau IC dan chip, yaitu bahan yang bukan merupakan konduktor maupun isolator yang baik.

dari kehidupan manusia sehari-hari, yang digunakan dalam komputer pribadi, mesin fax, jaringan-jaringan digital tanpa kabel, telepon selular serta membukakan pelayanan seperti TV Kabel, penggunaan kartu kredit dan lain sebagainya.[8] Dalam lingkup globalisasi sekarang ini, kecanggihan teknologi sistem telekomunikasi digital mengakibatkan proses-proses pada sistem informasi dapat dilakukan pada lokasi atau wilayah yang terpisah,[9] sehingga berkembanglah suatu bentuk administrasi perkantoran yang baru (*office automation system*) yang alur informasinya mampu mengalir secara eksternal organisasi (*global communication network*). Seiring dengan perkembangan teknologi informasi khususnya komputer sebagai perangkat pengolah informasi, maka suatu Sistem Informasi yang berbasiskan komputer (*computer based information system*) yang semula dikenal dengan istilah *Electronic Data Processing*[10], kini telah mengalami banyak perkembangan.[11]

Semula komputer hanya berkemampuan untuk mengolah data yang berbentuk untaian kata dan angka, maupun kombinasinya yang ternyata terus berkembang semakin majemuk seiring dengan perkembangan teknologi digital. Hal ini telah memungkinkan pengkonversian semua jenis atau bentuk data, baik

---

[8]Edmon Makarim, *op.cit.*, h. 27, dikutip dari Brian Fitzgerald, *"Conceptualising the Digital Environment"* dalam *Going Digital 2000: Legal Issues for E-Commerce, Software and the Internet*, diedit oleh Anne Fitzgerald, et.al, (New South Wales: Prospect MediaPty. Ltd. 1999), h. 1.

[9]*Ibid*, h. 35, dikutip dari OECD., *Trade in Information, Computer and Communication Services.*, Paris: Paris CEDEX. 1990., h. 45.

[10]Sering disingkat dengan EDP yang berarti pengolahan informasi yang dikerjakan secara elektronik oleh komputer.

[11]Edmon Makarim, *op.cit.*, h. 37.

ADLN - Perpustakaan Unair

yang berbentuk gambar, bunyi, gerak dan sebagainya, yang semula disampaikan dengan gelombang analog[12] menjadi bentuk digital (*digitalized*). Dewasa ini dapat dikatakan bahwa segala macam bentuk sesuatu yang dapat direpresentasikan sebagai input[13] ke dalam suatu sistem informasi (*computerized*) akan dapat diolah oleh sistem informasi tersebut untuk menghasilkan output[14] sebagaimana yang dikehendaki. Dengan tinjauan berdasarkan atas peranan dan fungsinya maka suatu sistem informasi adalah terdiri atas keberadaan fungsi-fungsi *Input, Process, Output, Storage* dan *Communication*.[15]

Menurut Edmon Makarim :

> Berkenaan dengan keberadaan komponen-komponen dalam suatu sistem informasi, maka secara garis besarnya suatu sistem informasi adalah terdiri dari 5 komponen utama, yaitu: (i) Perangkat Keras (*Hardware*); (ii) Perangkat Lunak (*Software*); (iii) Data dan/atau Informasi; (iv) Sistem dan Prosedur dan (v) Penggunanya (*Brainware*). Sehubungan dengan itu, perlu diketahui juga bahwa sistem penyimpanan data dan/atau informasi elektronik yang berbasiskan komputer, himpunan data yang disimpan dalam komputer dinamakan *databases* dan data yang dikomunikasikan melalui media telekomunikasi dinamakan *data messages*.[16]

---

[12]Bentuk dari komunikasi elektronik yang menggunakan gelombang elektromagnetik yang kontinu, seperti televisi dan radio.

[13]Informasi dari luar sistem komputer yang harus dimasukkan ke komputer untuk menyelesaikan beberapa pekerjaan. Alat masukan umumnya berupa keyboard atau magnetic disk, compact disk atau scanner.

[14]Informasi yang dihasilkan dari manipulasi atau pengolahan data komputer dan akan ditampilkan melalui monitor atau printer.

[15]Edmon Makarim, *op.cit.*, h. 8

[16]*Ibid.*, h. 38.

Semakin konvergennya perkembangan teknologi informasi dan komunikasi saat ini, telah mengakibatkan semakin beragam pula aneka jasa-jasa (*features*) fasilitas telekomunikasi yang ada, serta semakin canggihnya produk-produk teknologi informasi yang mampu mengintegrasikan semua media informasi. Ditengah globalisasi komunikasi yang semakin terpadu kini muncul Internet[17] dimana seakan telah membuat dunia semakin menciut (*shrinking the world*) dan semakin memudarkan batas-batas negara berikut kedaulatan dan tatanan masyarakatnya. Internet, yang didefinisikan oleh **The U.S Supreme Court** sebagai: *"international network of interconnected computers"* (Reno v. ACLU, 1997), telah menghadirkan kemudahan-kemudahan bagi setiap orang bukan saja sekedar untuk berkomunikasi tetapi juga untuk melakukan transaksi bisnis kapan saja dan dimana saja. Untuk lebih mengenal tentang Internet maka kita lihat sejarah terciptanya Internet.[18] Internet yang kita kenal sekarang ini berasal dari suatu jaringan (*network*)[19] yang diciptakan oleh Departemen Pertahanan Amerika Serikat pada awal tahun 1970-an. Jaringan ini bernama ARPAnet, dibangun oleh *Advanced Research Projects Agency* (ARPA) dengan tujuan untuk

---

[17]Istilah umum yang dipakai untuk menunjuk Network tingkat dunia yang terdiri dari komputer dan layanan servis atau sekitar 30 sampai 50 juta pemakai komputer dan puluhan sistem informasi termasuk e-mail, Gopher, FTP dan World Wide Web.

[18]Agus Raharjo, *Cybercrime : Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung, 2002, h. 61.

[19]Sekelompok komputer yang terhubung yang bisa saling berbagi sumber daya (seperti printer atau modem) dan data.

menghubungkan berbagai lokasi militer dan lokasi riset, disamping juga merupakan proyek tersendiri yang bertujuan untuk membangun sistem jaringan yang handal. Keterhubungan melalui jaringan internet dijalankan melalui beberapa metode protokol[20] yang diciptakan untuk memungkinkan terminal komputer yang berlainan jenis dan sistem untuk berkomunikasi antara yang satu dengan yang lainnya. Dari metode protokol ini dikembangkan metode pengiriman data melalui jalur komunikasi dengan menggunakan kelompok-kelompok data dengan tujuan masing-masing dalam suatu paket, metode ini sekarang dikenal dengan nama TCP/IP (*Transmission Control Protocol/Internet Protocol*)[21]. Pada akhir tahun 1980-an, *National Science Foundation* (NSF), yaitu lembaga yang didirikan di Amerika Serikat, secara bertahap mulai mengembangkan jaringannya sendiri yang dinamakan NSFnet dengan menggunakan teknologi yang dikembangkan oleh ARPAnet, dan juga mengembangkan *high-speed backbone network* yang semula digunakan untuk memungkinkan kampus-kampus dan lembaga-lembaga riset untuk menggunakan *network* tersebut dan penggunaan ini kemudian meningkat dengan diperkenalkannya *e-mail*[22] dan juga pengiriman data dan informasi antar lokasi. *E-mail* (*Electronic Mail*) ini merupakan fasilitas di

---

[20]Suatu kesepakatan mengenai bagaimana komunikasi akan dilakukan (Tanenbaum, 1992).

[21]Protokol komunikasi yang mula-mula dikembangkan oleh Departemen Pertahanan AS. TCP/IP menyediakan jalur transportasi data sehingga sejumlah data yang dikirim oleh suatu server dapat diterima oleh server yang lain. TCP/IP merupakan protokol yang memungkinkan sistem di seluruh dunia berkomunikasi pada jaringan tunggal yang disebut Internet

[22]Surat menyurat melalui Internet. Pengguna dapat saling bertukar berita. Berita-berita itu akan dikumpulkan dalam sebuah file untuk pengalamatan yang berupa mailbox, sehingga pengguna dapat membaca berita yang ditujukan kepadanya kapan saja.

Internet yang sangat penting sebagai sarana komunikasi, *e-mail* ini termasuk salah satu sarana komunikasi yang cepat, dan relatif murah.

Perkembangan teknologi informasi dan khususnya Internet ternyata tak hanya mengubah cara bagaimana seseorang berkomunikasi, mengelola data dan informasi, melainkan lebih jauh dari itu yaitu juga mengubah bagaimana seseorang melakukan bisnis. Banyak kegiatan bisnis yang sebelumnya tak terpikirkan, kini dapat dilakukan dengan mudah dan cepat dengan model-model bisnis yang sama sekali baru. Begitu juga, banyak kegiatan lainnya yang dulu dilakukan dalam lingkup terbatas kini dapat dilakukan dalam cakupan yang sangat luas, bahkan mendunia. Di sisi lain, perkembangan teknologi informasi dan internet ini juga telah sangat mempengaruhi hampir semua bisnis di dunia untuk terlibat dalam implementasi dan menerapkan berbagai aplikasi. Banyak manfaat dan keuntungan yang bisa diraih kalangan bisnis dalam kaitan ini, baik dalam konteks internal (meningkatkan efisiensi dan efektivitas organisasi), dan eksternal (meningkatkan komunikasi data dan informasi antar berbagai perusahaan pemasok, pabrikan, distributor) dan sebagainya.

Selain itu masyarakat pengguna internet (*internet global community*) seakan-akan mendapati suatu dunia baru yang dinamakan *cyberspace*[23] sebagaimana yang dipopulerkan oleh William Gibson dalam novel *science fiction*-nya yang berjudul *Neuromancer* yang mengambarkan bahwa ada suatu halusinasi

---

[23]Istilah yang berhubungan dengan kumpulan komputer yang data elektroniknya dapat diakses. Jika komputer berhubungan dengan Internet atau jaringan besar lainnya, maka komputer yang bersangkutan merupakan bagian dari *cyberspace*.

adanya alam lain, pada saat dipertemukannya teknologi telekomunikasi dan informatika.[24] Hal tersebut diyakini oleh para penggunanya (*netter*) sebagai suatu kehadiran alam baru yang tidak ada ketentuan hukumnya sama sekali, dan terlepas dari keberadaan sistem hukum yang selama ini berlaku. Hal ini karena tidak adanya suatu penguasa tunggal mutlak dalam jaringan komputer maha besar (*gigantic network*) tersebut, maka diyakini bahwa tidak ada satupun hukum suatu negara yang berlaku karena keberadaan hukum *network* tersebut adalah tumbuh sendiri dari kalangan masyarakat global para penggunanya.

Terkait dengan semua perkembangan tersebut, yang juga harus menjadi perhatian adalah bagaimana hal-hal baru tersebut, misalnya dalam kepastian dan keabsahan transaksi, keamanan komunikasi data dan informasi, dan semua yang terkait dengan kegiatan bisnis, dapat terlindungi dengan baik karena adanya kepastian hukum. Hal ini karena perangkat hukum yang ada tidak cukup memadai untuk menaungi semua perubahan dan perkembangan yang ada. Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi Internet ataupun komputer yang dalam istilah asing sering disebut dengan *cybercrime*. Dalam beberapa literatur yang ada, *cybercrime* sering diidentikkan dengan *computer crime* atau *computer-related crime*. Didasarkan pada Kongres Perserikatan Bangsa-Bangsa (PBB) ke-10 (Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offender) di Vienna, istilah yang digunakan PBB untuk *cybercrime* adalah *computer related crime* sebagaimana

---

[24]Edmon Makarim, *op.cit.*, h. 5.

terungkap dari hasil kongres itu sebagai berikut : *"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 the use or assistance of computer equipment."*[25] Sedangkan The US Department of Justice memberikan pengertian *computer crime* sebagai *"any illegal act requiring knowledge of computer for its perpetration, investigation, or prosecution"*, artinya "setiap perbuatan melanggar hukum yang memerlukan pengetahuan tentang komputer untuk menangani, menyelidiki dan menuntutnya".[26] Sedangkan Kepolisian Negara Republik Indonesia (Polri) melalui Lembaga Pendidikan dan Latihan Kepolisian Negara Republik Indonesia (Lemdiklat Polri) mendefinisikan *cybercrime* sebagai "suatu aktivitas yang dilakukan dengan sebuah alat (PC, *laptop*, *notebook*, *handphone*) yang terhubung dengan jaringan internet dan aktivitas tersebut melanggar UU."[27] Namun ada juga pendapat yang membedakan antara *cybercrime* dengan *computer crime* sebagaimana dikatakan oleh Nazura Abdul Manap sebagai berikut :

> *Defined broadly, 'computer crime' could reasonably include a wide variety of criminal offences, activities or issues. It also known as a crime committed using a a computer as a tool and it involves direct contact between the criminal nad the computer. For instance, a dishonest bank clerk who unauthorisedly transfers a customer's money to a dormant account for his own interest or a person without permission has obtained access to other*

---

[25]Agus Raharjo, *op. cit.*, h. 228, dikutip dari Dokumen A/CONF.187/5, h. 26

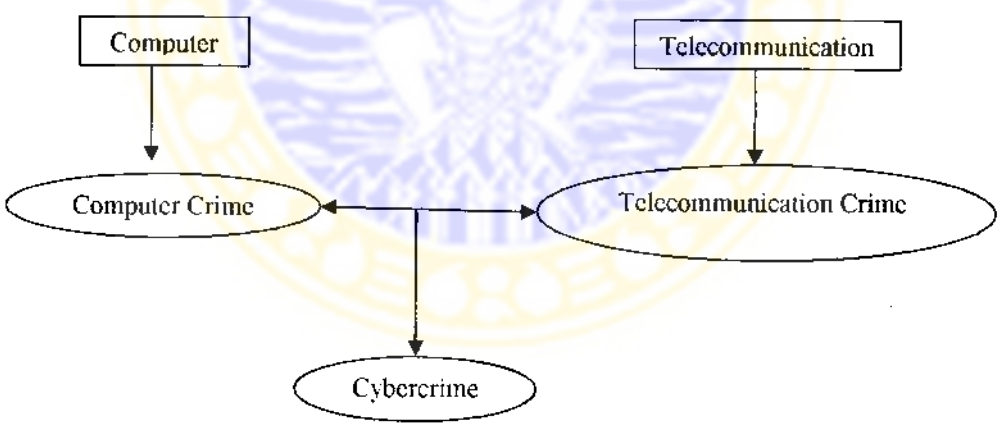
[26]Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, PT Refika Aditama, Bandung, 2005, h. 40.

[27]Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarso, ed., *Cyber Crime:Motif dan Penindakan*, Pensil-324, Jakarta, 2005, h. 20.

person's computer direcly to download information, which in the first place, are confidential. These situations require direct access by the hacker to the victim's computer. There is no Internet line involved, or only limited networking used such as the Local Area Network (LAN).
Whereas, cyber-crimes are crimes committed virtually through Internet online. This means that the crimes committed could extend to other countries, which is beyond the Malaysian Jurisdiction. Anyway, it causes no harm to refer computer crimes as cybercrimes or vice versa, they have same impact in law.[28]

Sedangkan Agus Raharjo secara sederhana membedakan antara *computer crime* dengan *cybercrime* yang didasarkan pada perpaduan antara teknologi komputer dan teknologi telekomunikasi yang menghasilkan Internet menggunakan bagan, sebagai berikut :

Pembedaan *Computer Crime* dan *Cybercrime*[29]



Sedangkan Barda Nawawi Arief menggunakan istilah "tindak pidana mayantara" untuk menyebut *cyber crime.*[30] Melihat belum adanya keseragaman definisi dari

---

[28]Agus Raharjo. *op. cit.*, h. 227, dikutip dari Nazura Abdul Manap. *Cyber-crimes: Problems and Solutions Under Malaysian Law*. Makalah pada Seminar Nasional *Money Laundering* dan *Cybercrime* dalam Perspektif Penegakan Hukum di Indonesia. diselenggarakan oleh Lab. Hukum Pidana Fakultas Hukum Universitas Negeri Surabaya. 24 Februari 2001, h. 3.

[29]Agus Raharjo. *op. cit.*, h. 228.

cybercrime maka untuk lebih memudahkan penulis memilih menggunakan istilah untuk *cybercrime* sebagai tindak pidana mayantara sesuai pendapat dari Barda Nawawi Arief dengan kedudukan dimana *cybercrime* berbeda dengan *computer crime*. Tindak pidana mayantara dalam perkembangannya menimbulkan permasalahan yang sangat rumit, terutama kaitannya dengan proses pembuktian tindak pidana (faktor yuridis). Apalagi penggunaan komputer untuk kejahatan itu memiliki karakteristik tersendiri atau berbeda dengan kejahatan yang dilakukan tanpa menggunakan komputer (kejahatan konvensional). Perbuatan atau tindakan, pelaku, alat bukti ataupun barang bukti dalam tindak pidana biasa, dengan mudah diidentifikasi, tetapi tidak demikian halnya untuk kejahatan yang dilakukan dengan menggunakan komputer. Pengaturan tentang tindak pidana mayantara di Indonesia jauh tertinggal jika dibandingkan dengan negara-negara lain, hal ini karena hingga saat ini Indonesia tidak memiliki perundangan (peraturan) yang khusus mengenai tindak pidana mayantara.

Berdasarkan uraian - uraian tersebut diatas, maka rumusan masalah adalah sebagai berikut :

1. Bagaimanakah penerapan pembuktian alat bukti digital berdasarkan Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana ?
2. Bagaimanakah nilai hukum suatu alat bukti digital ?

---

[30]Abdul Wahid. *op. cit.*, h. 43, dikutip dari Barda Nawawi Arief. *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung, 2003, h. 239.

2. Penjelasan Judul

Untuk memudahkan pemahaman mengenai permasalahan yang telah saya kemukakan di atas, maka penulisan skripsi ini diberi judul : " Penggunaan Alat Bukti Digital menurut Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana ".

Pengertian mengenai alat bukti tidak terdapat pada KUHAP yang merupakan dasar hukum keberadaan alat bukti itu sendiri, terutama pada Pasal 1 KUHAP yang merupakan bagian dari KUHAP yang memberikan tafsir otentik bagi hal-hal yang terkandung dalam KUHAP. Oleh karena itu maka penulis mengambil pengertian alat bukti dari kamus hukum[31] yaitu, yang dimaksud dengan alat bukti adalah "apa saja yang menurut undang-undang dapat dipakai untuk membuktikan benar atau tidaknya sesuatu (tuduhan)". Sedangkan yang dimaksud dengan digital menurut Kamus Teknologi[32] adalah "sinyal yang berarti pulsa, artinya antara bagian-bagian sinyal terlihat terputus-putus. Bagian yang diatas digambarkan sebagai 1 dan bagian bawah sebagai 0".

Jadi dengan pengertian di atas, maka judul penulisan skripsi saya jika dijelaskan adalah bahwa saya ingin mengetahui apakah penggunaan alat bukti digital dapat diterima dan digunakan di Indonesia terutama disesuaikan dengan Hukum Acara Pidana Indonesia.

3. Alasan Pemilihan Judul

---

[31]Yan Pramadya Puspa, *Kamus Hukum*, Aneka Ilmu, Semarang, h. 53.

[32]Wahyu Hidayat, *Kamus Teknologi Informasi (Komputer-Internet)*, Sarana Ilmu, Surabaya, h. 115.

Pilihan judul " Penggunaan Alat Bukti Digital menurut Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana " karena saya melihat di dalam perkembangan masyarakat sekarang ini telah muncul suatu bentuk kejahatan baru yang disebut sebagai *cybercrime* atau kejahatan yang memiliki keterkaitan erat dengan teknologi informasi[33]. Hal ini kemudian menimbulkan pertanyaan di masyarakat apakah peraturan perundang-undangan di Indonesia yang masih berlaku masih dapat menangani tindak pidana mayantara ataukah diperlukan peraturan perundang-undangan yang lebih spesifik mengenai tindak pidana mayantara terlebih dalam penggunaan alat bukti digital.

4. Tujuan Penulisan

Tujuan penulisan skripsi ini adalah untuk memenuhi persyaratan kelulusan untuk memperoleh gelar Sarjana Hukum (S1) pada Fakultas Hukum Universitas Airlangga. Tujuan lain dari penulisan skripsi ini adalah untuk menganalisa penggunaan alat bukti digital menurut Hukum Pidana Indonesia dalam penerapannya di dalam persidangan terutama dalam menangani perkara atau kejahatan yang berkaitan dengan komputer.

5. Metodelogi Penulisan

a. Pendekatan Masalah

---

[33]Edmon Makarim. *op.cit.*, h. 386.

Pembahasan masalah dilakukan secara yuridis normatif dengan melihat ketentuan pidana *materiil* di dalam dan di luar Kitab Undang-Undang Hukum Pidana khususnya perbuatan pidana.

b. Sumber Bahan Hukum

1. Bahan Hukum Primer

   a. Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana

   b. Undang-undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi jo. Undang-undang Nomor 20 Tahun 2001 tentang Perubahan Atas Undang-undang Nomor 31 Tahun 1999

   c. Putusan Pengadilan atau Yurisprudensi

2. Bahan hukum Sekunder

   a. Studi pustaka berkenaan dengan buku-buku Hukum Acara Pidana, Pembuktian, putusan-putusan pengadilan yang terkait dan *Cybercrime*;

   b. Penelusuran *website* yang berkaitan dengan *Cybercrime*, pembuktian, penggunaan alat bukti digital, *computer forensic*, misalnya : www.hukumonline.com; www.budi.insan.co.id; www.detik.com; www.komisihukum.go.id dan sebagainya;

   c. Pendapat Ahli.

c. Prosedur Pengumpulan dan Pengolahan Bahan Hukum

Prosedur pengumpulan bahan hukum dilakukan dengan cara mengumpulkan bahan hukum primer yaitu peraturan perundang-undangan yang terkait dengan permasalahan hukum yang ada terutama peraturan perundang-undangan yang lebih spesifik mengatur permasalahan hukum dalam penulisan skripsi ini,

sedangkan sumber bahan hukum sekunder diambil dari pendapat para ahli yang terdapat dalam berbagai literatur dan penelusuran *website* yang terkait dengan permasalahan hukum yang ada dalam skripsi ini.

Berdasarkan bahan hukum primer dan sekunder yang telah terkumpul kemudian ditelaah dan diklasifikasi berdasarkan fokus permasalahan yang terdapat dalam skripsi ini, kemudian disajikan dalam bentuk uraian yang terstruktur dan sistematis.

d. Analisis Bahan Hukum

Analisis terhadap pokok permasalahan yang terdapat di dalam skripsi ini dilakukan dengan cara mencari putusan-putusan pengadilan yang terkait dengan perkara yang termasuk dalam kategori *cybercrime* atau perkara-perkara lain yang terdapat alat bukti digital yang bisa dijadikan yurisprudensi.

6. Pertanggungjawaban Sistematika Penulisan

Agar penulisan skripsi ini menjadi terarah dan sistematis, maka penulis membagi dalam beberapa bab yang disesuaikan dengan pokok permasalahan yang akan dibahas.

Bab I tentang Pendahuluan, yang mengawali dari seluruh uraian dan pembahasan, sehingga merupakan pengantar pembahasan. Di dalam bab ini terdapat uraian dan penjelasan tentang permasalahan, latar belakang dan rumusannya. Dalam bab ini saya mengemukakan permasalahan mengenai penggunaan alat bukti digital menurut Hukum Acara Pidana Indonesia. Berkenaan

dengan hal tersebut, maka dijelaskan pada penjelasan judul, alasan pemilihan judul, tujuan penulisan dan metodelogi yang digunakan.

Bab II merupakan pembahasan dari pokok permasalahan pertama, yakni membahas tentang pembuktian menggunakan alat bukti digital dengan mendasarkan pada sistem pembuktian yang dianut dalam Hukum Acara Pidana Indonesia. Uraian dalam bab ini adalah sistem pembuktian yang dianut dalam Hukum Acara Pidana Indonesia, bentuk-bentuk alat bukti yang diakui Hukum Acara Pidana Indonesia dan mencari putusan-putusan pengadilan yang terkait dengan perkara yang termasuk dalam kategori *cybercrime* atau perkara-perkara lain yang terdapat alat bukti digital.

Bab III akan membahas tentang nilai hukum dari alat bukti digital. Nilai hukum yang dimaksud dalam hal ini adalah tentang keaslian dan keotentikan suatu alat bukti digital. Alat bukti digital yang dimaksud lebih ditujukan pada data elektronik. Pembahasannya akan dihubungkan dengan penggunaan *Digital Signature*.

Bab IV tentang Penutup berisi simpulan yang merupakan resume dari pokok permasalahan yang ada di dalam skripsi ini sebagaimana telah diuraikan pada bab-bab sebelumnya dan memberikan saran terhadap pokok permasalahan yang ada.

BAB II

PEMBUKTIAN TERHADAP ALAT BUKTI DIGITAL

1. Alat Bukti

1.1. Alat Bukti yang Diakui Hukum Acara Pidana

Bentuk-bentuk alat bukti yang sah yang diakui oleh Hukum Acara Pidana Indonesia secara jelas telah dicantumkan di dalam Pasal 184 ayat (1) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, yang selanjutnya akan disebut sebagai KUHAP. Alat bukti yang sah itu antara lain: keterangan saksi; keterangan ahli; surat; petunjuk; keterangan terdakwa. Dari urutan penyebutan alat bukti dapat disimpulkan bahwa pembuktian dalam perkara pidana lebih ditiitkberatkan pada keterangan saksi. Tetapi dalam *cybercrime*, jarang didapatkan adanya saksi atau bahkan tidak ada saksi sama sekali, karena para pelaku *cybercrime* sering melakukan kejahatannya seorang diri. Untuk lebih mengetahui tentang alat bukti, maka akan dibahas satu persatu. Yang pertama adalah keterangan saksi, pengertian keterangan saksi menurut Pasal 1 butir 27 KUHAP "adalah salah satu alat bukti dalam perkara pidana yang berupa keterangan dari saksi mengenai suatu peristiwa pidana yang ia dengar sendiri, ia lihat sendiri dan ia alami sendiri dengan menyebut alasan dari pengetahuannya itu".[34] Dari pengertian keterangan saksi tersebut di atas maka yang harus diterangkan oleh seorang saksi adalah : apa yang ia dengar sendiri; apa yang ia

---

[34]M. Karjadi dan R. Soesilo. *Kitab Undang-Undang Hukum Acara Pidana dengan Penjelasan Resmi dan Komentar*. Politeia. Bogor. 1997, h. 6.

lihat sendiri; dan apa yang ia alami sendiri, jadi jika disimpulkan, apa yang harus diterangkan oleh saksi adalah fakta yang menyangkut perbuatan yang dilakukan oleh seorang terdakwa, bukan pengambilan kesimpulan atau pendapat dari fakta yang menyangkut perbuatan yang dilakukan oleh seorang terdakwa. Keharusan tersebut sebagaimana yang diatur dalam Pasal 185 ayat (5) KUHAP yang berbunyi : "Baik pendapat maupun rekaan, yang diperoleh dari pemikiran saja, bukan merupakan keterangan saksi".[35] Alat bukti berikutnya adalah keterangan ahli, menurut Pasal 1 butir 28 KUHAP "keterangan ahli adalah keterangan yang diberikan oleh seorang yang memiliki keahlian khusus tentang hal yang diperlukan untuk membuat terang suatu perkara pidana guna kepentingan pemeriksaan".[36] Dari keterangan tersebut dapat disimpulkan bahwa keterangan ahli tidak dituntut suatu pendidikan formal tertentu, tetapi juga meliputi seorang yang ahli dan berpengalaman dalam suatu bidang tanpa pendidikan khusus. Alat bukti berikutnya adalah surat, dasar hukum keberadaan alat bukti surat adalah Pasal 184 huruf c KUHAP dan Pasal 187 KUHAP. Di dalam KUHAP tidak diberikan pengertian khusus tentang alat bukti surat ini. KUHAP hanya memberikan macam-macam surat sebagaimana disebutkan dalam Pasal 187 KUHAP yang berbunyi :

> Surat sebagaimana tersebut pada pasal 184 ayat (1) huruf c, dibuat atas sumpah jabatan atau dikuatkan dengan sumpah, adalah :
> a. berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat dihadapannya, yang memuat

---

[35] *Ibid*, h. 163.

[36] *Ibid*, h. 6.

ADLN - Perpustakaan Unair

keterangan tentang kejadian atau keadaan yang didengar, dilihat atau yang dialaminya sendiri, disertai dengan alasan yang jelas dan tegas tentang keterangannya itu;

b. surat yang dibuat menurut ketentuan perundang-undangan atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukkan bagi pembuktian sesuatu hal atau sesuatu keadaan;
c. surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai sesuatu hal atau sesuatu keadaan yang diminta secara resmi dari padanya;
d. surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.[37]

Dilihat dari macam-macam surat yang disebutkan didalam KUHAP dapat diambil kesimpulan bahwa surat yang dimaksud dalam Pasal 187 huruf a, b, dan c KUHAP adalah surat yang dibuat atas sumpah jabatan atau dikuatkan dengan sumpah atau bisa disebut sebagai surat resmi sedangkan surat yang dimaksud dalam Pasal 187 huruf d KUHAP adalah surat biasa, yang bisa dibuat oleh setiap orang. Tidak adanya pengertian tentang surat yang diberikan KUHAP mendorong munculnya beberapa pendapat dalam memberikan pengertian tentang surat. Pengertian surat menurut Sudikno Mertokusumo adalah sebagai berikut :

> Surat ialah segala sesuatu yang memuat tanda-tanda bacaan yang dimaksudkan untuk mencurahkan isi hati atau untuk menyampaikan buah pikiran seseorang dan dipergunakan sebagai pembuktian. Dengan demikian maka segala sesuatu yang tidak memuat tanda-tanda bacaan, atau meskipun memuat tanda-tanda bacaan, akan tetapi tidak mengandung buah pikiran, tidaklah termasuk dalam pengertian alat bukti tertulis atau surat.[38]

---

[37] *Ibid*, h. 165-166.

[38] Hari Sasangka dan Lily Rosita, *Hukum Pembuktian Dalam Perkara Pidana untuk Mahasiswa dan Praktisi*, Mandar Maju. Bandung. 2003. h. 62.

Sedangkan pengertian surat yang diberikan Asser-Anema adalah "Surat-surat ialah segala sesuatu yang mengandung tanda-tanda baca yang dapat dimengerti, dimaksud untuk mengeluarkan isi pikiran.".[39]

Alat bukti berikutnya adalah alat bukti petunjuk, dasar hukum alat bukti petunjuk diatur dalam Pasal 184 ayat (1) huruf d KUHAP dan Pasal 188 KUHAP. Menurut Pasal 188 ayat (1) KUHAP petunjuk adalah perbuatan, kejadian atau keadaan, 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. Sedangkan alat bukti petunjuk dapat diperoleh dari keterangan saksi; surat dan keterangan terdakwa. Penerapan tentang alat bukti petunjuk ini sepenuhnya diletakkan kepada hakim, dengan cara melakukan pemeriksaan secara cermat dan seksama. Alat bukti yang terakhir menurut KUHAP adalah alat bukti keterangan terdakwa. Pengertian keterangan terdakwa menurut Pasal 189 ayat (1) KUHAP ialah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri atau alami sendiri. Keterangan terdakwa yang dapat diakui sebagai alat bukti adalah keterangan terdakwa yang diberikan dalam persidangan.

1.2. Alat Bukti Digital

Alat bukti digital merupakan bentuk alat bukti yang tergolong baru, alat bukti digital muncul berkenaan dengan semakin berkembangnya dunia teknologi informasi. Alat bukti digital di Indonesia sendiri masih belum diakui

---

[39] *Ibid.*

keberadaannya menurut Hukum Acara Pidana yang berlaku tetapi dalam beberapa tindak pidana khusus, keberadaan alat bukti digital sudah diakui keberadaannya sebagai suatu alat bukti. Dalam dunia komputer dan internet, para penggunanya akan memasuki dunia digital yang hanya terdiri dari pulsa-pulsa listrik dan kumpulan logika angka 0 dan 1. Identitas seorang pelaku sangat sulit diketahui di dalam dunia digital ini karena sifatnya lebih global. Di dunia digital ini tidak ada sidik jari yang merupakan ciri khas dari setiap orang. Namun meski demikian proses kejahatan di dalamnya bukannya tidak berbekas sama sekali. Proses komunikasi dan komputasi digital juga bisa menghasilkan atribut-atribut khas atau yang disebut jejak kejahatan, yaitu benda-benda digital, yang bisa dijadikan sebagai alat bukti digital. Contoh benda-benda digital seperti misalnya sebuah file[40] dokumen, *log* akses, *e-mail header*[41] dan *log*[42], medan electromagnet pada piringan harddisk[43], *IP address*[44]. Benda ini hanya bisa dilihat, diukur satuannya, dan diproses lebih lanjut juga dengan menggunakan komputer.

---

[40]*File* terdiri dari sekumpulan *record-record* yang saling berhubungan. Setiap *record* memiliki nomor yang disesuaikan dengan posisinya dalam *file*.

[41]Suatu bagian dari pesan *e-mail* yang dihasilkan oleh protokol transmisi, dimana bagian tersebut berisikan informasi mengenai siapa yang membuat pesan, kapan pesan tersebut dikirimkan, jalur transmisi yang digunakan di Internet dan identifikasi mesin yang digunakan.

[42]Catatan yang merekam segala aktifitas suatu aplikasi dijalankan. terkadang Log juga digunakan untuk menganalisa status suatu aplikasi.

[43]Media penyimpanan data, terbuat dari bahan yang kaku berbentuk piringan berlapis magnetic oksida dengan kapasitas penyimpanan yang sangat besar. *Head* baca-tulisnya tidak menyentuh piringan secara fisik seperti halnya pada disket, tapi berjalan di atas bantalan udara tipis. Harddisk dipasang di dalam CPU dan identik dengan drive C.

[44]Alamat numeric unik dari sebuah komputer di Internet. IP address komputer Anda sama dengan nomor telepon Anda sendiri dalam fungsinya.

Contoh sederhananya adalah sebuah *e-commerce web server* yang memiliki *system logging* setiap kali *server*[45] tersebut diakses. Melalui *log* ini, semua orang yang mengakses *server* tersebut akan terekam dengan jelas keterangannya, biasanya berupa *IP address*, *port-port*[46] komunikasi yang digunakan, aktifitasnya di dalam *server* tersebut, dan banyak lagi. Dari log ini dapat diketahui *IP address* berapa yang melakukan "*carding*". Kemudian dapat dicari ISP (*Internet Service Provider*)[47] mana pemilik *IP address* ini. Setelah menghubungi ISP yang bersangkutan dan menyertakan bukti-bukti aktifitasnya.

Pengertian dari bukti digital di Indonesia masih belum ada, bahkan undang-undang untuk tindak pidana tertentu yang bisa dikatakan mengakui alat bukti digital hanya menyebutnya sebagai alat bukti lain (alat bukti diluar alat bukti yang diakui KUHAP). Ada sebuah kelompok kerja yang bernama *Standard Working Group on Digital Evidence* (SWDGE) mendefinisikan bukti digital sebagai semua informasi yang memiliki nilai pembuktian yang kuat yang disimpan atau ditransmisikan dalam bentuk sinyal-sinyal listrik digital.[48] Untuk membantu

---

[45]Sebuah komputer di Internet atau di jaringan lainnya yang menyimpan file dan membuat file tersebut tersedia untuk diambil jika dibutuhkan; Sebuah aplikasi jaringan komputer yang digunakan untuk melayani banyak pengguna dalam satu jaringan.

[46]Saluran dalam sistem komputer yang menghubungkan CPU dengan piranti masukan dan keluaran, merupakan sarana untuk masuk atau keluar dari sistem komputer.

[47]Perusahaan yang menawarkan dan menyediakan layanan akses Internet ke kalangan umum dengan mengenakan biaya. Contohnya : Telkomnet, Indosatnet. Centrin. Cbn. Wasantara. dll

[48]Hayri. "Bukti Digital. Kunci Penguak Kejahatan Cyber", www.PCMedia.com, diakses tanggal 7 April 2006.

mengetahui tentang alat bukti digital, sumber bukti digital dikelompokkan dalam 3 (tiga) kategori besar[49], yaitu:

a. *Open Computer System*

Perangkat-perangkat yang masuk dalam kategori jenis ini adalah apa yang kebanyakan orang pikir sebagai perangkat komputer. Sistem yang memiliki media penyimpanan, keyboard, monitor, dan pernak-pernik yang biasanya ada di dalam komputer masuk dalam kategori ini. Seperti misalnya, *laptop*[50], *desktop*[51], *server* dan perangkat-perangkat sejenis lainnya. Perangkat yang memiliki system media penyimpanan yang kian membesar dari waktu ke waktu ini merupakan sumber yang kaya akan bukti-bukti digital. Sebuah file yang sederhana saja pada sistem ini dapat mengandung informasi yang cukup banyak dan berguna bagi proses investigasi. Contohnya detail seperti kapan file tersebut dibuat, siapa pembuatnya, seberapa sering file tersebut diakses, dan informasi lainnya semua merupakan informasi penting.

b. *Communication System*

Sistem telepon, komunikasi tanpa kabel, Internet, jaringan komunikasi data, merupakan salah satu sumber bukti digital yang masuk dalam kategori ini. Sebagai contoh, jaringan Internet membawa pesan-pesan dari

---

[49] *Ibid.*

[50] Komputer pribadi berukuran kecil dan ringan sehingga mudah dijinjing dan masuk dalam tas.

[51] Salah satu model kemasan komputer yang sengaja dirancang untuk ditempatkan di atas meja kerja.

seluruh dunia melalui *e-mail*. Kapan waktu pengiriman *e-mail* ini, siapa yang mengirimnya, melalui mana si pengirim mengirim, apa isi dari *e-mail* tersebut merupakan bukti digital yang sangat penting dalam investigasi.

c. *Embedded Computer System*

Perangkat telepon seluler (ponsel), *personal digital assistant* (PDA), *smart card*, dan perangkat-perangkat lain yang tidak dapat disebut komputer tetapi memiliki sistem komputer dalam bekerjanya dapat digolongkan dalam kategori ini. Hal ini dikarenakan bukti-bukti digital juga dapat disimpan di sini. Sebagai contoh, navigasi mobil dapat merekam ke mana saja mobil tersebut berjalan. Sensor[52] dan modul-modul diagnosa yang dipasang, dapat menyimpan informasi yang dapat digunakan untuk menyelidiki terjadinya kecelakaan, termasuk informasi kecepatan, jauhnya perjalanan, status rem, posisi persneling yang terjadi dalam lima menit terakhir. Semuanya merupakan sumber-sumber bukti digital yang amat berguna.

Bukti-bukti digital biasanya didapat dalam bentuk "data mentah". Data mentah merupakan data yang belum diformat dan ditampilkan ke dalam bentuk yang dapat dibaca oleh mata dan pikiran manusia. Masalah ini bisa diselesaikan dengan menggunakan alat bantu yang akan mengubah data mentah menjadi format yang lebih dapat dimengerti. Alat bantu ini akan menjalankan berbagai rutin dan

---

[52]Elemen yang mengubah sinyal fisik menjadi sinyal elektronik yang dibutuhkan komputer.

algoritma[53] untuk menerjemahkan data mentah. Dalam proses penerjemahan ini, data mentah akan melewati sebuah *layer*[54] dimana akan diubah bentuknya menjadi format lain yang bisa dibaca oleh sebuah aplikasi. *Layer* ini sering disebut dengan istilah *abstraction layer*, contohnya adalah ASCII (*American Standard Code for Information Interchange*)[55], HTML (*Hyper Text Markup Language*)[56], paket-paket TCP/IP, *signature-signature intrution detection system*, dan banyak lagi. Data mentah kemudian diproses dengan algoritma dan seperangkat aturan pada *abstraction layer* untuk menghasilkan suatu data yang dapat dibaca. Tetapi, proses ini juga tentunya tidak luput dari kesalahan seperti misalnya, adanya *bug*[57] pada aplikasi[58], spesifikasi alat yang tidak tepat, konfigurasi yang salah, dan banyak lagi. Teknik mengumpulkan bukti-bukti digital ini berkembang seiring dengan perkembangan teknologi komputer. Pada masa awal dilakukannya penyelidikan bukti digital, para penyidik biasanya langsung menggunakan perangkat digital yang mengandung barang bukti dalam melakukan pengumpulan bukti. Biasanya pengumpulan dilakukan dengan melihat langsung isi sebuah file atau mengopinya ke tempat penyimpanan lain. Padahal

---

[53]Urutan langkah-langkah yang diperlukan untuk memecahkan perhitungan logika atau matematika.

[54]Lapisan (konsep) dalam networking. Berbagai model komunikasi seperti OSI dan TCP/IP terdiri atas beberapa layer yang menyusun protokol tersebut.

[55]Standar huruf dan tanda baca untuk komputer. ASCII merupakan kode berupa karakter 8 bit berbentuk angka 1 dan 0 untuk mewakili karakter-karakter alpha numerik.

[56]Format dokumen yang digunakan dalam World Wide Web (WWW). HTML merujuk pada tampilan halaman, jenis, huruf, elemen grafis, juga link hypertext ke dokumen lain di Internet.

[57]Kesalahan dalam program yang mengakibatkan jalannya program menjadi kurang baik.

[58]S*oftware* yang dibuat oleh suatu perusahaan komputer untuk mengerjakan tugas-tugas tertentu, misalnya Ms-Word, Ms-Excel.

ADLN - Perpustakaan Unair

tindakan seperti ini memiliki potensi yang sangat besar untuk dapat mengubah atau bahkan merusak bukti-bukti digital yang ada pada perangkat tersebut. Penyidikan terhadap *cybercrime* yang dilakukan pada era 1980-an kebanyakan masih berkutat seputar file sistem saja, seperti misalnya mencari *log-log*[59], menyelidiki runutan modifikasi sebuah file, melihat siapa yang terakhir mengakses, dan banyak lagi. Pada era ini belum terlalu dipedulikannya keaslian data yang dikumpulkan. Selain itu bukti-bukti yang dihapus dengan sengaja maupun tidak sengaja belum menjadi prioritas utama dalam penyidikan. Sampai pada era 1990-an, karena semakin meningkatnya *cybercrime* para penyidik mulai makin peduli terhadap keaslian bukti digital ini.

2. Pembuktian

2.1. Sistem Pembuktian yang Dianut dalam KUHAP

Sebelum membahas tentang sistem pembuktian yang dianut KUHAP sebaiknya kita terlebih dahulu mengetahui tentang bentuk-bentuk sistem pembuktian yang ada. Berbagai sistem pembuktian itu adalah[60]:

a. Conviction in Time

Hakim di dalam menjatuhkan putusan tidak terikat dengan alat bukti yang ada. Darimana hakim menyimpulkan putusannya tidak menjadi masalah. Hakim hanya boleh menyimpulkan alat bukti yang ada di dalam persidangan atau mengabaikan alat bukti yang ada di persidangan. Sehingga dalam

---

[59]Catatan yang merekam segala aktifitas suatu aplikasi dijalankan. terkadang Log juga digunakan untuk menganalisa status suatu aplikasi.

[60]Hari Sasangka, *op.cit.*, h. 14.

mengambil keputusan terhadap suatu perkara menjadi bersifat subyektif sekali, hakim tidak perlu menyebutkan alasan-alasan yang menjadi dasar putusannya. Sistem pembuktian ini biasa digunakan dalam sistem peradilan juri (jury rechtspraak) misalnya di Inggris dan Amerika.

b. Conviction in Raisone

Sistem pembuktian ini juga masih menyandarkan pada keyakinan hakim, dimana hakim tidak terikat pada alat-alat bukti yang telah ditetapkan oleh undang-undang, dimana hakim bisa mempergunakan alat-alat bukti di luar yang ditentukan oleh undang-undang. Namun demikian dalam mengambil keputusan terhadap suatu perkara hakim harus mendasarkan pada alasan-alasan yang jelas. Alasan yang dipakai hakim dalam mengambil putusan harus didasari dengan alasan yang logis dan dapat diterima oleh akal dan nalar, tidak semata-mata berdasarkan keyakinan yang tanpa batas.

c. Sistem Pembuktian Positif

Sistem pembuktian ini hanya menyandarkan pada pada alat-alat bukti yang telah ditentukan oleh undang-undang saja. Dalam sistem ini keyakinan hakim sama sekali diabaikan. Dalam mengambil keputusan hakim bersifat obyektif karena dalam mengambil keputusan tidak dipengaruhi nuraninya. Yang dicari dalam sistem pembuktian ini adalah kebenaran formal, oleh karena itu sistem pembuktian ini dipergunakan dalam hukum acara perdata.

d. Sistem Pembuktian Negatif

Dalam mengambil keputusan, hakim terikat pada alat-alat bukti yang telah ditentukan oleh undang-undang juga didasarkan pada keyakinan hakim

ADLN - Perpustakaan Unair

sendiri. Dalam sistem ini ada dua hal yang merupakan syarat untuk membuktikan kesalahan terdakwa, yakni adanya alat bukti yang sah yang telah ditetapkan oleh undang-undang dan adanya keyakinan hakim yang didasarkan pada alat-alat bukti yang ada. Alat bukti yang telah ditentukan undang-undang tidak bisa ditambah dengan alat bukti lain, serta berdasarkan alat bukti yang diajukan di persidangan seperti yang telah ditentukan oleh undang-undang belum bisa memaksa seorang hakim menyatakan terdakwa bersalah telah melakukan tindak pidana yang didakwakan.

Setelah mempelajari beberapa sistem pembuktian maka dapat diketahui sistem pembuktian yang dianut oleh KUHAP. Dalam KUHAP sistem pembuktian diatur dalam Pasal 183 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". Dari pasal tersebut dapat diketahui bahwa putusan hakim harus didasarkan pada 2 (dua) syarat, yaitu: minimum 2 (dua) alat bukti; dan dari dua alat bukti tersebut, hakim memperoleh keyakinan bahwa terdakwa bersalah melakukan tindak pidana. Jadi meskipun di dalam persidangan telah diajukan dua atau lebih alat bukti, namun bila hakim tidak yakin terdakwa bersalah, maka terdakwa tersebut akan dibebaskan. Dari uraian di atas dapat kita simpulkan bahwa KUHAP menganut sistem pembuktian negatif (negatief wettelijk).

2.2. Penerapan Alat Bukti Digital

Dalam pembahasan sebelumnya sudah kita bahwa sistem pembuktian yang dianut oleh KUHAP adalah sistem pembuktian negatif, hakim hanya terikat pada alat-alat bukti yang telah ditentukan oleh undang-undang. Dalam KUHAP sendiri belum mengakui keberadaan alat bukti digital hanya pada beberapa undang-undang yang mengatur tentang tindak pidana khusus saja keberadaan alat bukti digital sudah diakui. Sedangkan beberapa bentuk *cybercrime* sering diterapkan dalam bentuk-bentuk kejahatan yang terdapat didalam KUHAP yang mana belum mengakui keberadaan alat bukti digital. Mengingat kelemahan KUHAP itu terhadap perkembangan teknologi maka para penyidik harus cerdik dalam menggunakan alat bukti digital agar dapat diterima di persidangan. Untuk mengetahui lebih lanjut bagaimana penerapan alat bukti digital di persidangan maka penulis akan merujuk pada suatu kasus. Kasus ini didasarkan pada Putusan Pengadilan Negeri Jakarta Barat No. 1050/Pid/S/1989/PN.Jak.Bar[61]. Dalam kasus ini yang menjadi terdakwa adalah Budiman Hidayat. Kasus posisinya sebagai berikut: Budiman Hidayat merupakan karyawan Bank Bali di kantor P.T. Bank Bali Jl. Hayam Wuruk 84-85, Jakarta yang bertugas pada bagian Giro. Dia pada tanggal 10 Pebruari 1989 telah menggunakan komputer B-3 yang ditinggalkan oleh Ng Wie Hung ke bagian belakang untuk melihat hasil catatan data yang sudah di-*input*, *terminal computer* masih dalam keadaan terbuka. Mengetahui hal tersebut maka Budiman Hidayat mencoba untuk meng-*input* data yaitu seolah-

---

[61] Al. Wisnubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, Penerbitan Universitas Atma Jaya, Yogyakarta, 1999, h. 323. Lebih lanjut mengenai isi putusan dapat dilihat dalam lembar Lampiran pada skripsi ini.

olah ada setoran warkat sebesar Rp. 43.500.000,- (empat puluh tiga juta lima ribu rupiah) pada rekening No. A/C 00111.3618.4 atas nama Diana Kamdani yang merupakan kakak ipar dari Budiman Hidayat. Bahwa dalam meng-*input* data pada komputer B-3 tersebut Budiman Hidayat memakai kode teller 333 milik Imam Hartono dan *code user* milik Ng Wie Hung yang pada waktu ditinggalkan dalam keadaan terbuka. Kemudian Budiman Hidayat menemui Diana Kamdani dengan mengatakan bahwa ada setoran masuk pada rekening Diana Kamdani titipan dari teman Budiman Hidayat, dan kemudian ia meminta tolong pada Diana Kamdani agar menarik Giro Bilyet[62] sebanyak 2 (dua) lembar, masing-masing senilai Rp. 40.000.000,- (empat puluh juta rupiah) dan Rp. 3.000.000,- (tiga juta rupiah) serta 1 (satu) lembar cek senilai Rp. 500.000,- (lima ratus ribu rupiah). Kemudian Giro Bilyet dan cek tersebut dicairkan oleh Budiman Hidayat melalui dengan rincian Giro Bilyet No. 103791 tertanggal 13 Pebruari 1989 dengan nominal Rp. 40.000.000,- kemudian dimasukkan deposito atas namanya di Bank Buana Indonesia, Giro Bilyet No. 103790 tertanggal 13 Pebruari 1989 dengan nominal Rp. 3.000.000,- dimasukkan menjadi Tabanas di Bank Bali atas namanya, dan Cek No. 036728 tertanggal 13 Pebruari 1989 dengan nominal Rp. 500.000,- dipakai untuk kepentingannya sendiri. Dalam kasus ini barang bukti yang diajukan di persidangan adalah: 1 (satu) lembar Giro Bilyet No. 103791 nominal Rp. 40.000.000,-; 1 (satu) lembar Giro Bilyet No. 103790 nominal Rp. 3.000.000,-; 1 (satu) lembar cek No. 036.728 nominal Rp. 500.000; Photocopy

---

[62]Surat Giro

ADLN - Perpustakaan Unair

Transaction Journal[63] tanggal 10 Pebruari 1989; 1 (satu) lembar rekening koran[64] atas nama Diana Kamdani; 1 (satu) unit Komputer IBM No. 1025169 dan Monitor IBM No. 9704145; dan uang tunai sebesar Rp. 42.400.000,- yang dititipkan di Bank Indonesia cabang Jakarta Kota. Dari barang bukti yang digunakan di atas yang dapat dikategorikan sebagai alat bukti digital adalah data yang ada pada *terminal computer* P.T. Bank Bali yang secara rinci ada pada *transaction journal* dan data rekening dari Diana Kamdani pada tanggal 10 Pebruari 1989 dimana telah dilakukan manipulasi data dengan membuat seolah-olah telah ada setoran warkat sebesar Rp. 43.500.000,-.

Yang menjadi masalah sekarang adalah agar alat bukti digital tersebut dapat diterima dalam persidangan. Cara mengatasi masalah tersebut sebenarnya bisa dengan cara mengubah bentuk alat bukti digital yang berupa data komputer menjadi bentuk fisik yaitu *print-out* kemudian menggunakan ahli yang mengetahui tentang seluk beluk komputer dan sebaiknya ahli ini sudah dilibatkan dari awal penyidikan terutama berkaitan dalam pengumpulan alat bukti digital atau bisa dikatakan ahli ini adalah ahli forensik komputer. Dengan menggunakan cara tersebut maka data komputer yang berupa *transaction journal* dan rekening atas nama Diana Kamdani itu dijadikan bentuk fisik yaitu berupa *print-out*. Hasil *print-out* ini dapat kita kategorikan sebagai surat menurut Pasal 187 huruf d KUHAP yaitu surat lain yang hanya dapat berlaku jika ada hubungannya dengan

---

[63]Transaksi yang diposting sesuai jurnal aliran kas atau aktiva. Ada lembar pengesahan bisa dalam computer atau pada kertas legal.

[64]Ini adalah istilah perbankan yang berarti rekening pribadi atau perseroan di bank hubungan utang piutang yang secara periodik dilakukan penghitungan penyelesaian.

isi dari alat pembuktian yang lain. Dimana yang mengumpulkan dan mengolah data tersebut sebaiknya seseorang yang mempunyai pengetahuan dalam bidang forensik komputer dengan tujuan agar bukti yang ada tetap terjaga keasliannya. Tetapi pada persidangan kasus diatas yang diajukan menjadi saksi ada 5 (lima) orang sebagaimana terdapat pada putusan yang terlampir pada skripsi ini dan dari kelima orang tersebut tidak ada yang dijadikan sebagai ahli. Tetapi jika dilihat dari keterangan yang diberikan kelima saksi tersebut sebenarnya ada yang bisa kategorikan sebagai ahli yaitu saksi Albert Bambang hal ini bisa disimpulkan bahwa yang mengetahui adanya kejanggalan terhadap setoran warkat itu adalah Albert Bambang hal ini dikarenakan dia bertugas di bagian Finance Control pada Tim Emplimentasi Komputer, dalam persidangan dia juga yang memberikan keterangan bahwa *print-out transaction journal* tersebut merupakan cetakan hasil penginputan data pada komputer sebagaimana dilakukan oleh Budiman Hidayat sehingga kesaksian yang diberikan Albert Bambang sebenarnya bisa dikategorikan sebagai keterangan ahli hal ini sudah sesuai dengan pengertian keterangan ahli yang dijelaskan dalam Pasal 1 butir 28 KUHAP yang berbunyi "keterangan ahli adalah keterangan yang diberikan oleh seorang yang memiliki keahlian khusus tentang hal yang diperlukan untuk membuat terang suatu perkara pidana guna kepentingan pemeriksaan".

BAB III

NILAI HUKUM ALAT BUKTI DIGITAL

1. Pengolahan Alat Bukti Digital

Pada umumnya dalam suatu tindak pidana kita akan mendapatkan barang bukti dimana barang bukti ini haruslah benda yang berkaitan langsung dengan tindak pidana yang terjadi. Barang bukti ini bisa benda yang digunakan untuk melakukan suatu tindak pidana ataupun benda yang diperoleh setelah melakukan tindak pidana atau hasil dari suatu tindak pidana, dan jika diajukan pada persidangan sebagai alat bukti, barang itu mempunyai bentuk fisik, yang bisa dilihat dan disentuh secara langsung tanpa menggunakan perantara atau alat bantu. Itu adalah hal yang umum kita temui pada tindak pidana umum atau tindak pidana biasa. Tetapi hal itu berbeda dengan tindak pidana mayantara dimana benda-benda yang dapat dijadikan alat bukti biasanya tidak berbentuk fisik tetapi berupa data dalam bentuk digital dan masih berupa "data mentah" sehingga dibutuhkan alat bantu khusus atau dilakukan suatu pemrosesan agar "data mentah" tersebut dapat dibaca oleh orang awam. Proses yang dimaksud ini adalah forensik. Forensik sendiri adalah suatu cabang ilmu pengetahuan.

Menurut Susetyo Pramusinto:

> Ilmu forensik adalah ilmu pengetahuan yang menggunakan multidisiplin ilmu dengan menerapkan ilmu pengetahuan alam seperti kimia, fisika, biologi, psikologi, kedokteran, dan kriminologi dengan tujuan untuk

ADLN - Perpustakaan Unair

membuat terangnya suatu perkara pidana dan membuktikan ada tidaknya kejahatan atau pelanggaran dengan memeriksa barang bukti (*physical evidences*) dalam perkara tersebut.[65]

Dalam kaitannya dengan tindak pidana mayantara yang selalu memunculkan alat bukti digital, ilmu forensik ini juga bisa digunakan bahkan memunculkan berbagai bidang ilmu forensik yang berkaitan dengan tindak pidana mayantara ini, misalnya: forensik jaringan (*network forensic*) yang digunakan terhadap tindak pidana mayantara yang terjadi dalam jaringan internet; kemudian bidang forensik lainnya adalah forensik komputer (*computer forensic*). Orang yang dapat melakukan proses forensik ini dapat kita sebut sebagai seorang ahli forensik meskipun keberadaan ahli forensik dalam hal tindak pidana mayantara ini bukanlah dari aparat penegak hukum. Dalam pembahasan berikutnya maka penulis mengambil contoh dari penggunaan forensik komputer dalam mengumpulkan alat bukti digital. Terminologi dari forensik komputer atau yang meluas menjadi forensik teknologi informasi sendiri adalah suatu proses mengidentifikasi, memelihara, menganalisa, dan mempergunakan bukti digital menurut hukum yang berlaku.[66] Dalam melakukan forensik teknologi informasi ada beberapa elemen kunci, yaitu:

1. Identifikasi dari Bukti Digital

---

[65]Idam Wasiadi, "Saksi Ahli menurut KUHAP dan Peraturan-perundangan Lain", http://www.polri.go.id/riset/saksiahlibom.php, diakses tanggal 13 Juli 2006.

[66]Rahmadi Budiman, "Computer Forensic Apa dan Bagaimana", http://budi.insan.co.id/courses/ec7010/2003/rahmadi-report.pdf, diakses tanggal 2 Februari 2005.

ADLN - Perpustakaan Unair

Merupakan tahapan paling awal forensik dalam teknologi informasi. Pada tahapan ini dilakukan identifikasi di mana bukti itu berada, di mana bukti itu disimpan dan bagaimana penyimpanannya untuk mempermudah tahapan selanjutnya. Banyak pihak yang mempercayai bahwa forensik di bidang teknologi informasi itu merupakan forensik pada komputer. Sebenarnya forensik bidang teknologi informasi sangat luas, bisa pada telepon seluler, kamera digital, *smart cards*, dan sebagainya. Memang banyak kasus kejahatan di bidang teknologi informasi itu berbasiskan komputer. Tetapi perlu diingat, bahwa teknologi informasi tidak hanya komputer atau internet.

2. Penyimpanan Bukti Digital
   Termasuk tahapan yang paling kritis dalam forensik. Pada tahapan ini, bukti digital dapat saja hilang karena penyimpanannya yang kurang baik. Penyimpanan ini lebih menekankan bahwa bukti digital pada saat ditemukan akan tetap tidak berubah baik bentuk, isi, makna, dan sebagainya dalam jangka waktu yang lama. Ini adalah konsep ideal dari penyimpanan bukti digital.
3. Analisa Bukti Digital
   Pengambilan, pemrosesan, dan interpretasi dari bukti digital merupakan bagian penting dalam analisa bukti digital. Setelah diambil dari tempat asalnya, bukti tersebut harus diproses sebelum diberikan kepada pihak lain yang membutuhkan. Tentunya pemrosesan di sini memerlukan beberapa skema tergantung dari masing-masing kasus yang dihadapi.
4. Presentasi Bukti Digital
   Adalah proses persidangan di mana bukti digital akan diuji otentifikasi dan korelasi dengan kasus yang ada. Presentasi di sini berupa penunjukan bukti digital yang berhubungan dengan kasus yang disidangkan. Karena proses penyidikan sampai dengan proses persidangan memakan waktu yang cukup lama, maka sedapat mungkin bukti digital masih asli dan sama pada saat diidentifikasi oleh investigator untuk pertama kalinya.[67]

Dalam suatu proses forensik teknologi informasi, kita akan mendapatkan suatu informasi, dimana berdasarkan sifatnya, informasi ini terbagi menjadi dua jenis[68], yaitu:

---

[67] *Ibid.*

ADLN - Perpustakaan Unair

1. Data Volatil

   Merupakan data sistem yang bersifat *transien*[69] sehingga harus sesegera mungkin diambil atau dicatat setelah terjadi insiden. Data ini bersumber dari keadaan hubungan jaringan, tabel ***router***, tabel proses, *open port* dan *user*[70]. Untuk menangkap data ini diperlukan *tool*[71] khusus. Data volatil ini terdiri dari : data jaringan yaitu data komunikasi aktual antara sistem sasaran dengan sistem lainnya; daftar proses aktif yang berisi daftar program atau *daemon*[72] yang aktif pada sistem sasaran; daftar *logged-in user* yang berisi daftar pengguna pada sistem sasaran; *open file*[73] yaitu *file* (*hidden*) atau *Trojan* (*rootkit*) apa yang dimasukkan ke sistem sasaran.

2. Data non-volatil

---

[68]Suryani Alifah. "Ekstraksi Ciri Signifikan pada Analisa Forensik Jaringan Menggunakan Teknik Intelligensia Buatan". http://budi.insan.co.id/courses/cc7010/2003/report-suryani.pdf, diakses tanggal 25 Februari 2005.

[69]Keadaan dalam sistem ketika ada perubahan tiba-tiba dan dalam waktu singkat.

[70]Istilah dalam dunia komputer untuk menyebutkan seseorang yang menggunakan suatu sistem komputer, program atau stasiun atau terminal dalam jaringan.

[71]Menu yang tersedia hampir di semua program aplikasi, umumnya menyediakan sejumlah fasilitas pendukung yang sangat membantu pengguna ketika menyelesaikan tugas dengan aplikasi tersebut.

[72]Program yang dijalankan di sebuah komputer untuk memonitor port TCP/IP tertentu. Sebagai contoh server HTTP adalah daemon yang memonitor port 80.

[73]Jenis file dalam sistem yang memiliki kemampuan untuk dibaca atau ditulisi, bahkan dibaca dan ditulisi pada waktu yang sama.

ADLN - Perpustakaan Unair

Merupakan data atau informasi yang masih ada setelah proses *reboot*[74], yang terdiri dari : *configuration setting*; file data dan sistem; *registry setting*.

Suatu proses forensik terdiri dari beberapa tahap, yaitu: akuisisi dan pengintaian (*reconnaissance*) yang merupakan proses untuk mendapatkan atau mengumpulkan data volatil (jika bekerja pada sistem *online*[75]) dan data non-volatil (disk terkait) dengan menggunakan berbagai *tool*; analisa yang merupakan proses menganalisa data yang diperoleh dari proses sebelumnya, meliputi analisa *real-time* dari data volatil, analisa *log-file*, korelasi data dari berbagai divais pada jaringan yang dilalui serangan dan pembuatan *time-lining* dari informasi yang diperoleh; dan tahap terakhir adalah tahap recoveri yang merupakan proses untuk mendapatkan atau memulihkan kembali data yang telah hilang akibat adanya intrusi, khususnya informasi pada disk yang berupa file atau direktori.

Keberhasilan proses forensik sangat ditentukan oleh kualitas dan kuantitas informasi yang terkumpul. *Log file* dapat merupakan sumber informasi yang penting bagi proses forensik. *Log file* mengandung informasi tentang berbagai sumber daya sistem, proses-proses dan aktivitas pengguna. *Protocol*

---

[74]Melaksanakan booting ulang komputer dengan cara memutuskan aliran listrik kemudian mengulang prosedur booting; disebut juga sebagai warmboot.

[75]Keadaan ketika dua atau lebih mesin mengadakan hubungan komunikasi; segalaperangkat atau proses yang mengirimkan informasi secara langsung ke komputer untuk pengolahan dan hasil yang segera diperoleh.

analyzer, *sniffer*, *server SMTP* (*Simple Mail Transport Protocol*)[76], *DHCP* (*Dynamic Host Configuration Protocol*)[77], *FTP* (*File Transfer Protocol*)[78] dan *WWW* (*World Wide Web*)[79], *router*[80], *firewall*[81], dan hampir semua aktivitas sistem atau *user* dapat dikumpulkan dalam *log file*. Tetapi jika administrator sistem (*system administrator*)[82] tidak dapat mencatat, maka fakta yang diperlukan untuk menghubungkan pelaku dengan insiden tidak ada. Sayangnya penyerang dan penjahat yang pintar mengetahui hal ini dan tujuan pertamanya adalah merusak atau mengubah *log file* untuk menyembunyikan aktivitas mereka. Hal kedua yang penting tetapi sering dilupakan adalah sistem *clock*[83]. Pencatatan suatu file berhubungan dengan *time stamp* dan *date stamp* yang memungkinkan analis forensik untuk menentukan urutan kejadian. Tetapi jika sistem *clock* tidak dikoreksi atau dikalibrasi secara berkala dapat dimatikan dari mana saja dari

---

[76]Protokol ini untuk memproses pesan teks yang hanya berisi rangkaian karakter ASCII (A-Z, angka, dan tanda baca keyboard standar) serta alamat sasaran.

[77]Protokol yang secara dinamis memberikan alamat *Internet Protocol* baru pada komputer setiap kali ada yang melakukan *login*.

[78]Program yang memungkinkan kita memindahkan data di antara dua komputer yang berjauhan letaknya. Protokol yang dipakai pada Internet untuk mengirim file.

[79]Servis Internet yang dapat me-link dengan dokumen multimedia bersama dengan HyperText. Pemakai dapat melompat antara dokumen dengan menggunakan link untuk melihat text, grafik, video dan media lainnya.

[80]Alat penghubung antara LAN dan Internet yang merutekan transmisi antara keduanya.

[81]Sebuah *software* program yang dipasang pada sebuah jaringan dan bertugas memproteksi sistem komputer dengan tujuan mengamankan *Network Internal*. Kadang-kadang membutuhkan layanan Proxy untuk mengizinkan suatu akses pada Web.

[82]Orang yang menjalankan, mengelola dan mengawasi host atau jaringan, dikenal pula sebagai *network administrator* atau administrator jaringan.

[83]Sumber utama dari pulsa elektronik komputer. *Clock* digunakan untuk menyamakan operasi semua elemen komputer.

beberapa detik sampai beberapa jam. Hal ini menyebabkan masalah karena korelasi antara *log file* dari komputer yang berbeda akan menyulitkan bahkan tidak mungkin mengkorelasikan kejadian. Solusi yang sederhana untuk mensinkronisasi *clock* adalah seluruh server dan sistem berjalan pada suatu *daemon* seperti *UNIX ntpd daemon*, yang mensinkronisasi waktu dan tanggal sistem secara berkala dengan *atomic clock* yang disponsori pemerintah. Dari sekilas penjelasan tentang proses pengumpulan alat bukti digital atau proses forensik baik yang disebut forensik komputer ataupun forensik jaringan dapat dilihat bahwa banyak hal yang sangat asing bagi orang-orang awam yang diantaranya adalah aparat penegak hukum sendiri yang dalam kenyataan tidak mempunyai latar belakang pengetahuan dalam hal komputer atau teknologi informasi. Terlebih lagi data hasil forensik tersebut berupa kumpulan angka.

Setelah kita memperoleh suatu alat bukti digital sekarang yang menjadi permasalahan adalah bagaimanakah alat bukti digital itu dapat diterima dalam persidangan karena seperti yang kita ketahui bahwa dalam KUHAP alat bukti yang diakui hanya keterangan saksi; keterangan ahli; surat; petunjuk; dan keterangan terdakwa. Sedangkan alat bukti digital belum diakui, kecuali pada beberapa undang-undang yang mengatur tentang tindak pidana khusus, misalnya dalam tindak pidana pencucian uang, tindak pidana terorisme. Oleh karena itu kita harus dapat mencari celah hukum yang dapat dimanfaatkan agar suatu alat bukti digital dapat diterima dalam persidangan. Salah satu cara yang dapat dilakukan agar alat bukti digital dapat diterima dalam persidangan adalah dengan mengajukan hasil proses forensik dalam bentuk *print out* atau berbentuk dokumen

yang dicetak. Cara ini dapat dilakukan dengan mengklasifikasikan dokumen cetak itu pada kategori surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain. Dan juga harus dihadirkan seorang saksi ahli yang mengetahui tentang seluk beluk alat bukti digital yang telah dijadikan dalam bentuk *print out*, saksi ahli yang dimaksud dalam hal ini adalah ahli forensik yang melakukan proses forensik terhadap tindak pidana mayantara yang disidangkan, dan bisa juga ahli lain yang mengetahui tentang proses tindak pidana mayantara itu dengan maksud sebagai pembanding. Tetapi proses ini mempunyai kelemahan seperti rentan terhadap perubahan data dari alat bukti digital dalam penyimpanannya seperti terkena virus[84], adanya sabotase terhadap alat bukti digital.

2. *Digital Signature*

2.1. Penggunaan Digital Signature

Digital Signature atau tanda tangan digital adalah suatu sistem pengamanan yang menggunakan *public key cryptography system*, atau secara umum pengertiannya adalah *"A data value generated by public key algorithm based on the contents of a lock data and a private key, yielding so individualized crypto checksum"*.[85] Atau pengertian lain dari *digital signature* adalah "kode digital yang

---

[84]Suatu program yang dapat menggandakan dirinya sendiri pada suatu sistem komputer. Cara kerjanya adalah menetap dalam RAM dan menginfeksi semua file yang dibaca atau diakses komputer.

[85]Arrianto Mukti Wibowo, "Kerangka Hukum Digital Signature dalam *Electronic Commerce*", http://www.geocities.com/amwibowo/resource/hukum_ttd/hukum_ttd.html, diakses tanggal 2 Februari 2005.

ADLN - Perpustakaan Unair

dapat ditempelkan pada pesan yang dikirim secara elektronis, tanda tangan inilah yang menjadi identifikasi dari si pengirim pesan, seperti halnya tanda tangan tertulis, tujuan tanda tangan digital adalah untuk menjamin bahwa yang mengirimkan pesan itu memang benar-benar orang yang seharusnya."[86]

Tujuan dari suatu tandatangan dalam suatu dokumen adalah untuk memastikan otentisitas dari dokumen tersebut. Suatu *digital signature* sebenarnya bukan suatu tanda tangan seperti yang kita kenal selama ini, *digital signature* menggunakan cara yang berbeda untuk menandai suatu dokumen sehingga dokumen atau data sehingga *digital signature* tidak hanya mengidentifikasi dari pengirim, namun *digital signature* juga memastikan keutuhan bahwa dokumen tersebut tidak berubah selama proses transmisi. Suatu *digital signature* didasarkan dari isi dari pesan itu sendiri.

Berdasarkan sejarahnya, penggunaan *digital signature* berawal dari penggunaan teknik *kriptografi* yang digunakan untuk mengamankan informasi yang hendak ditransmisikan atau disampaikan kepada orang yang lain yang sudah digunakan sejak ratusan tahun yang lalu.[87] Dalam suatu *kriptografi* suatu pesan dienkripsi (*encrypt*)[88] dengan menggunakan suatu kunci (*key*). Hasil dari enkripsi

---

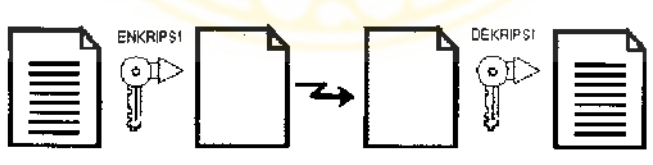
[86]Andino Maseleno. "Kamus Istilah Komputer dan Informatika", www.IlmuKomputer.com, diakses tanggal 18 Juni 2006.

[87] Arrianto Mukti Wibowo, *loc. cit.*

[88]Penerjemahan data menjadi kode rahasia. Enkripsi adalah cara yang paling efektip untuk memperoleh pengamanan data. Untuk membaca file yang dienkripsi, kita harus mempunyai akses terhadap kata sandi yang memungkinkan kita men-*dekrip* pesan tersebut. Data yang tidak dienkripsi disebut *plain text*, sedangkan yang dienkripsi disebut *chiper text*.

ini adalah berupa *chipertext* yang kemudian ditransmisikan atau diserahkan kepada tujuan yang dikehendakinya. *Chipertext* tersebut kemudian dibuka atau didekripsi (*decrypt*)[89] dengan suatu kunci untuk mendapatkan informasi yang telah dienkripsi tersebut. Terdapat dua macam cara dalam melakukan enkripsi yaitu dengan menggunakan kriptografi simetris (*symetric crypthography* atau *secret key crypthography*) dan kriptografi asimetris (*asymetric crypthography*) yang kemudian lebih dikenal sebagai *public key crypthography*.

Secret key crypthografi atau yang dikenal juga sebagai kriptografi simetris, menggunakan kunci yang sama dalam melakukan enkripsi dan dekripsi terhadap suatu pesan (*message*), disini pengirim dan penerima menggunakan kunci yang sama sehingga mereka harus menjaga kerahasian (*secret*) terhadap kunci tersebut. Salah satu algoritma yang terkenal dalam kriptografi simetris ini adalah *Data Encryption Standard* (*DES*)[90].



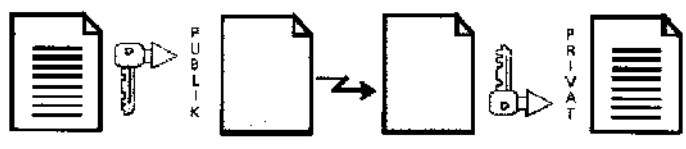
Gambar 1: kriptografi simetris

---

[89]Mengubah kembali hasil enkripsi ke bentuk aslinya sehingga informasi tersebut dapat dibaca.

[90]Metode pengacakan data dalam kode-kode standar untuk dikirimkan melalui suatu jaringan besar.

Public key crypthography atau yang dikenal juga sebagai kriptografi simetris, menggunakan dua kunci (*key*) yaitu satu kunci digunakan untuk melakukan enkripsi terhadap suatu pesan (*messages*) dan kunci yang lain digunakan untuk melakukan dekripsi terhadap pesan tersebut. Kedua kunci tersebut mempunyai hubungan secara matematis sehingga suatu pesan yang dienkripsi dengan suatu kunci hanya dapat didekripsi dengan kunci pasangannya. Seorang pengguna mempunyai dua buah kunci, yaitu sebuah kunci privat (*privat key*) dan juga sebuah kunci publik (*public key*). Pengguna (*user*) tersebut kemudian mendistribusikan atau menyebarluaskan kunci publik miliknya. Karena terdapat hubungan antara kedua kunci tersebut, pengguna dan seseorang yang menerima kunci publik akan merasa yakin bahwa suatu data yang diterimanya dan telah berhasil didekripsi hanya dapat berasal dari pengguna yang mempunyai kunci privat. Kepastian atau keyakinan ini hanya ada selama kunci privat ini tidak diketahui oleh orang lain. Kedua kunci ini berasal atau diciptakan sendiri oleh penggunanya. Salah satu algoritma yang terbaik yang dikenal selama ini adalah *RSA* (dinamakan sesuai dengan nama penciptanya Rivest, Shamir, Adleman).



Gambar 2 : kriptografi dengan menggunakan kunci publik

ADLN - Perpustakaan Unair

Pada saat dua orang hendak saling berkomunikasi atau saling bertukar data atau pesan secara aman, mereka kemudian saling mengirimkan salah satu kunci yang dipunyainya, yaitu kunci publiknya. Sedangkan mereka menyimpan kunci privat sebagai pasangan dari kunci publik yang didistribusikannya. Karena data atau pesan ini hanya dapat dienkripsi dan didekripsi dengan menggunakan kunci pasangannya maka data ini dapat dapat ditransmisikan dengan aman melalui jaringan yang relatif tidak aman (melalui internet). Contoh dari penggunaan *kriptografi* ini adalah jika Bob hendak mentransmisikan suatu data atau pesan rahasia kepada Alice maka ia akan melakukan enkripsi data tersebut dengan menggunakan kunci publik Alice. Selama Alice yakin bahwa tidak ada seorang pun yang mengetahui kunci privatnya, maka mereka dapat merasa yakin bahwa yang dapat membaca pesan tersebut hanyalah Alice.

Dalam *digital signature* suatu data atau pesan akan dienkripsi dengan menggunakan kunci simetris yang diciptakan secara acak (*randomly generated symmetric key*). Kunci ini kemudian akan dienkripsi dengan menggunakan kunci publik dari calon penerima pesan. Hasil dari enkripsi ini kemudian dikenal atau disebut sebagai *digital envelope* yang kemudian akan dikirimkan bersama pesan atau data yang telah dienkripsi. Setelah menerima *digital envelope* penerima kemudian akan membuka atau mendekripsi dengan menggunakan kunci privatnya. Hasil yang ia dapatkan dari dekripsi tersebut adalah sebuah kunci simetris yang dapat digunakannya untuk membuka data atau pesan tersebut.

Kombinasi antara *digital signature* dengan *message digest* menyebabkan seorang pengguna dapat "menandatangani secara digital" (*digitally sign*) suatu data atau pesan. Maksud dari menandatangani secara digital adalah memberikan suatu ciri khas terhadap suatu pesan. *Message digest* adalah suatu besaran (*value*) yang berasal dari suatu data atau pesan yang memiliki sifat yang unik yang menandai bahwa pesan tersebut mempunyai suatu besaran tertentu. *Messages digest* diciptakan dengan melakukan enkripsi terhadap suatu data dengan menggunakan menggunakan kriptografi satu arah (*one way crypthography*), yaitu suatu tehnik kriptografi yang terhadapnya tidak dapat dilakukan proses pembalikan (*reversed*). Pada saat *message digests* dienkripsi dengan menggunakan kunci privat dari pengirim dan "ditambahkan" kepada data atau pesan yang asli maka hasil yang didapat adalah *digital signature* dari pesan tersebut.

Penerima dari *digital signature* akan dapat mempercayai bahwa data atau pesan benar berasal pengirim. Dan karena apabila terdapat perubahan suatu data atau pesan akan menyebabkan akan merubah *message digests* dengan suatu cara yang tidak dapat diprediksi (*in unpredictible way*) maka penerima akan merasa yakin bahwa data atau pesan tersebut tidak pernah diubah setelah *message digest* diciptakan. Sebelum kedua belah pihak (pengirim atau penerima) hendak melakukan komunikasi diantaranya dengan menggunakan kriptografi kunci publik, masing-masing pihak harus merasa yakin akan keberaan mereka. Mereka kemudian akan melakukan otentifikasi terhadap keberadaan masing-masing pihak. Agar mereka dapat melakukan otentifikasi terhadap keberadaan mereka masing-

msing maka mereka menunjuk pihak ketiga yang akan memberikan otentifikasi terhadap kunci publik mereka. Pihak ketiga ini dikenal sebagai *Certification Authorithy*. *Certification authorithy* ini kemudian akan memberikan suatu sertifikat (*certificate*) yang berisi identitas dari pengguna (misalnya Alice), sertifikat ini ditandatangani secara digital oleh *certification authority* tersebut. Isi dari sertifikat tersebut selain identitas juga berisi kunci publik dari pemiliknya.

Digital signature ini mempunyai beberapa sifat seperti (a) *Authenticity* atau *ensured* yaitu keasliannya dapat terjamin karena *digital signature* ini diperoleh pihak yang berwenang mengeluarkannya, yaitu *certification authorithy* dimana untuk memperolehnya kita harus memberitahukan identitas, kewenangan, kedudukan hukum, dan status dari *user*, informasi dari pengguna ini harus benar dan akan diperiksa kebenarannya oleh pihak *certification authorithy*; (b) *integrity* yaitu berhubungan dengan masalah keutuhan dari data yang dikirimkan; (c) *non-repudiation* yaitu dengan adanya *digital signature* ini pengguna tidak dapat menyangkal bahwa ia tidak mengirimkan data tersebut, juga pengguna tidak dapat menyangkal bahwa isi dari data tersebut berbeda dengan data yang telah dikirimkannya; (d) *confidentiality* yaitu isi dari data tersebut bersifat rahasia.[91] *Digital signature* ini sering digunakan pada praktek *electronic commerce*, *internet banking*. Hal ini karena praktek transaksi dalam internet dapat dikatakan tidak aman, tetapi kelemahan dari internet ini dapat diminimalisasi dengan adanya

---

[91] Arrianto Mukti Wibowo, *loc. cit.*

penerapan teknologi penyandian informasi (*crypthography*) terhadap data dengan menggunakan sistem pengamanan seperti *digital signature*.[92]

2.2. *Digital Signature* sebagai Alat Bukti

Dari pembahasan pada sub bab sebelumnya dapat kita ketahui bahwa *digital signature* digunakan dalam praktek transaksi yang menggunakan internet sebagai sebagai media, terutama dalam melakukan pertukaran data yang dilakukan antara perusahaan atau apabila suatu perusahaan akan melakukan perbuatan hukum, terutama yang dilakukan melalui media internet. Maka jika suatu perusahaan akan melakukan suatu perbuatan hukum misalnya adalah jual beli maka pihak yang berwenang mewakili perusahaan tersebut adalah direksi, jadi yang dipergunakan adalah *digital signature* dari direksi tersebut. Untuk menerangkan judul sub bab ini maka penulis akan memberikan suatu contoh kasus. A adalah direksi Perusahaan Maju melakukan transaksi jual beli dengan B sebagai direksi dari Perusahaan Mundur dan dalam transaksi menggunakan dokumen elektronik yang menggunakan media internet sehingga kedua orang tersebut dalam menggunakan *digital signature*, kemudian setelah beberapa saat ternyata B atau Perusahaan Mundur menjadi korban penipuan dari A karena barang yang diberikan tidak sesuai dengan yang dijanjikan dalam perjanjian yang tertuang dalam dokumen elektronik. Berdasarkan kasus tersebut maka yang dapat dijadikan alat bukti adanya penipuan terhadap transaksi adalah dokumen perjanjian jual beli yang dalam format dokumen elektronik. Maka agar dokumen elektronik tersebut dapat

---

[92] *Ibid.*

diterima sebagai alat bukti maka harus dirubah dalam bentuk fisik yaitu dengan cara dicetak. Tetapi hal ini rawan dari proses perubahan data baik dari pihak A maupun pihak B. Tetapi karena dokumen tersebut telah dibuat dengan menggunakan sistem pengamanan *digital signature* maka dokumen elektronik tidak dapat dirubah. Tetapi walaupun begitu *digital signature* tidak sepenuhnya aman karena kunci pada *digital signature* tersebut masih bisa dicuri atau dibobol meskipun membutuhkan waktu yang lama. Hal ini karena *digital signature* terbentuk dari rangkaian algoritma yang sangat sulit untuk dirusak dan untuk merusak satu kunci algoritma saja dibutuhkan waktu yang lama. Sebagai contoh, secara teknis : suatu *cryptosystem* yang menggunakan kunci sepanjang 127-bit, bagi seorang *cryptanalyst* membutuhkan waktu 6 bulan untuk membobolnya, kalau kunci diganti dengan kunci sepanjang 128-bit, hanya ditambahkan 1 bit saja, diperlukan waktu selama 12 bulan untuk bisa membobolnya.[93]

Pembobolan kunci mungkin saja terjadi. Besar kecilnya kemungkinan ini ditentukan oleh panjangnya kunci. Semakin panjang kunci makin semakin sulit pula untuk membobolnya. Tetapi seiring dengan perkembangan teknologi yang cepat maka resiko pembobolan kunci-kunci kriptografi juga semakin besar. Hal ini digambarkan dalam tabel berikut:[94]

Tabel 1

Perkiraan Waktu Yang Dibutuhkan Untuk Membobol Kunci Dengan Harga Tertentu Pada Tahun 1995

---

[93] *Ibid.*

[94] *Ibid.*

	Panjang Kunci (bit)					
Asimetris (RSA)	-	384	512	768	1792	2304
Simetris (DES)	40	56	64	80	112	128
$100,000	2 detik	35 jam	1 tahun	70 000 tahun	10^14 tahun	10^19 tahun
$1,000,000	0,2 detik	3,5 jam	37 hari	7 000 tahun	10^13 tahun	10^18 tahun
$10,000,000	0,02 detik	21 menit	4 hari	700 tahun	10^12 tahun	10^17 tahun
$100,000,000	2 ms	2 menit	9 jam	70 tahun	10^11 tahun	10^16 tahun

(sumber: Arrianto Mukti Wibowo. "Kerangka Hukum Digital Signature dalam *Electronic Commerce*", http://www.geocities.com/amwibowo/resource/hukum_ttd/hukum_ttd.html. diakses tanggal 2 Februari 2005.)

Data tersebut merupakan penghitungan pada tahun 1995 dengan menggunakan hardware khusus untuk menjebol kunci simetris DES. Sedangkan kunci asimetris dalam kolom yang sama menunjukkan panjang kunci asimetris yang memiliki kekuatan yang sama dengan kunci simetrisnya. Jadi untuk membobol kunci asimetris 512-bit membutuhkan waktu komputasi yang kurang lebih sama untuk membobol kunci simetris sepanjang 64-bit. Dengan asumsi kemampuan komputer menjadi berlipat ganda setiap 18 bulan dengan harga yang sama, maka pada tahun 1999 estimasi tersebut akan menjadi:

Tabel 2

Perkiraan Waktu Yang Dibutuhkan Untuk Membobol Kunci Dengan Harga Tertentu Pada Tahun 1999

	Panjang Kunci (bit)					
Asimetris (RSA)	-	384	512	768	1792	2304
Simetris (DES)	40	56	64	80	112	128
$100,000	0,25 detik	4,4 jam	1,5 bulan	10 000 tahun	10^13 tahun	10^18 tahun
$1,000,000	25 ms	25 menit	4,5 hari	1 000 tahun	10^12 tahun	10^17 tahun
$10,000,000	2,5 ms	2,6 menit	12 jam	100 tahun	10^11 tahun	10^16 tahun
$100,000,000	0,25 ms	2 menit	1,1 jam	10 tahun	10^10 tahun	10^15 tahun

(sumber: Arrianto Mukti Wibowo. "Kerangka Hukum Digital Signature dalam *Electronic Commerce*", http://www.geocities.com/amw ibowo/resource/hukum_ttd/hukum_ttd.html, diakses tanggal 2 Februari 2005.)

Menurut pendapat penulis bentuk cetak dari dokumen elektronik mempunyai nilai hukum dalam pembuktian karena dapat dikategorikan sebagai surat yang dimaksud dalam Pasal 187 huruf b KUHAP karena direksi yang mewakili perusahaanya dapat dikatakan sebagai seorang pejabat. Dan sebagai alat bukti lainnya adalah dapat didatangkan seseorang yang mewakili pihak *certification authorithy* dengan tujuan untuk memberikan keterangan sebagai saksi ahli dalam hal kebenaran dari informasi yang terdapat dalam *digital signature* yang tercantum dalam dokumen elektronik yang dijadikan alat bukti adanya transaksi jual beli antara A dan B.

BAB IV

PENUTUP

1. Kesimpulan

Berdasarkan pembahasan pada bab-bab sebelumnya, maka dapat ditarik suatu kesimpulan sebagai berikut:

(1) Bahwa alat bukti digital belum diakui keberadaannya di dalam KUHAP. Tetapi dalam praktik sudah ada putusan pengadilan sebagaimana putusan pengadilan yang terlampir dalam lampiran yaitu putusan Pengadilan Negeri Jakarta Barat No. 1050/Pid/S/1989/PN.Jkt.Bar. Putusan pengadilan tersebut sudah dapat menerima keberadaan alat bukti digital dalam hal ini adalah *transaction journal* dimana *transaction journal* dirubah dalam bentuk *print out* atau dicetak, dimana *print out transaction journal* ini dapat dimasukkan dalam kategori surat yang dimaksud dalam Pasal 187 KUHAP huruf d. Dan harus dikuatkan dengan keterangan dari seorang ahli yang mempunyai pengetahuan tentang alat bukti digital yang diajukan dalam persidangan.

(2) Belum diakuinya keberadaan alat bukti digital dalam proses pembuktian berdasarkan KUHAP menimbulkan keraguan tentang nilai hukum suatu alat bukti digital. Keberadaan Forensik Komputer sangat diperlukan dalam mengumpulkan dalam alat bukti digital, hal ini hanya dapat dilakukan oleh orang yang mempunyai pengetahuan tentang Forensik Komputer. Alat bukti digital dalam pembahasan ini adalah suatu dokumen elektronik dalam suatu transaksi atau suatu perbuatan hukum dapat mempunyai nilai hukum jika

dalam dokumen elektronik menggunakan sistem pengamanan *digital signature*. Dengan adanya *digital signature* dapat diketahui siapa yang telah membuat dokumen elektronik tersebut, karena dalam pemilikan suatu *digital signature* harus memberikan identitas diri kepada pihak *certification authority* yang berwenang mengeluarkan suatu *digital signature*.

2. Saran

(1) Perlu segera dilakukan penyesuaian dari ketentuan yang diatur dalam KUHAP terutama dalam hal alat bukti. Hal ini karena perkembangan teknologi yang selalu berkembang terus sedangkan KUHAP masih belum berkembang. Sementara belum adanya pengakuan dari KUHAP tentang alat bukti digital hakim harus pintar dalam menyiasati agar alat bukti digital dapat diterima dalam persidangan. Hal ini bisa dilakukan dengan cara penemuan hukum atau mencari yurisprudensi. Para aparat penegak hukum juga perlu dibekali pengetahuan tentang teknologi agar dapat memahami tentang kejahatan yang memanfaatkan teknologi, sehingga dapat menentukan tindak pidana yang tepat serta sanksi pidana yang sesuai.

(2) Perlu adanya ketentuan perundangan yang mengakui keberadaan seorang ahli forensik komputer terutama dalam laporan hasil forensik yang telah dilakukan sebagaimana halnya pengakuan dari forensik kedokteran yang tercantum dalam *visum et repertum*. Bahkan jika perlu adanya pengakuan mengenai keberadaan forensik komputer sebagai sebuah profesi seperti halnya pengakuan terhadap forensik kedokteran. Pemerintah harus

ADLN - Perpustakaan Unair

melakukan pengaturan tentang keberadaan *certification authority* yang berwenang dalam menerbitkan *digital signature*. Pengembangan penggunaan *digital signature* dalam penyimpanan alat bukti digital dengan tujuan tidak berubahnya alat bukti digital, jika memang ada perubahan dapat diketahui perubahan itu. Selain itu untuk pembatasan akses terhadap alat bukti digital agar alat bukti digital tersebut tidak dirubah dan dapat diketahui siapa saja yang telah melakukan akses terhadap alat bukti digital itu.

DAFTAR BACAAN

BUKU

Hidayat, Wahyu, *Kamus Teknologi Informasi (Komputer-Internet)*, Sarana Ilmu, Surabaya.

Karjadi, M., dan R. Soesilo, *Kitab Undang-undang Hukum Acara Pidana dengan Penjelasan Resmi dan Komentar*, Politeia, Bogor, 1997.

Makarim, Edmon, *Kompilasi Hukum Telematika*, PT. RajaGrafindo Persada, Jakarta, 2003.

Puspa, Yan Pramadya, *Kamus Hukum*, Aneka Ilmu, Semarang.

Raharjo, Agus, *Cybercrime : Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung, 2002.

Sasangka, Hari, dan Lily Rosita, *Hukum Pembuktian Dalam Perkara Pidana untuk Mahasiswa dan Praktisi*, Mandar Maju, Bandung, 2003.

Sutanto, Hermawan Sulistyo, dan Tjuk Sugiarso, ed., *Cyber Crime : Motif dan Penindakan*, Pensil-324, Jakarta, 2005.

Wahid, Abdul dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, PT. Refika Aditama, Bandung, 2005.

Wisnubroto, Al., *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, Penerbitan Universitas Atma Jaya, Yogyakarta, 1999.

PERATURAN PERUNDANG-UNDANGAN

Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.

Undang-undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi jo Undang-undang Nomor 20 Tahun 2001 tentang Perubahan atas Undang-undang Nomor 31 Tahun 1999.

INTERNET

http://budi.insan.co.id/

www.geocities.com/amwibowo/

www.hukumonline.com

www.IlmuKomputer.com

www.PCMedia.com

www.polri.go.id

LAMPIRAN I

PUTUSAN

No. 1050/Pid/S/1989/PN.Jkt.Bar.

"DEMI KEADILAN BERDASARKAN KETUHANAN YANG MAHA ESA"

Pengadilan Negeri Jakarta Barat yang memeriksa dan mengadili perkara pidana pada tingkat pertama menjatuhkan putusan sebagai berikut, dalam perkaranya terdakwa:.....

BUDIMAN HIDAYAT, lahir di Jakarta, umur 30 th (lahir 30 Desember 1959), jenis kelamin: Laki-laki, Kebangsaan Indonesia, tempat tinggal di Jl. Tamansari X-137 RT-006/13 Tamansari Jakarta Barat, agama: Kristen, Pekerjaan: ex karyawan P.T. Bank Bali Jakarta, Pendidikan: SMA;...

Pengadilan Negeri tersebut;.....

Membaca berkas perkara beserta lampiran-lampirannya;.....

Mendengar keterangan saksi-saksi dan terdakwa;.....

Mendengar tuntutan Jaksa Penuntut umum yang pada pokoknya menyatakan terdakwa Budiman Hidayat bersalah melakukan kejahatan :

"Membuat surat palsu mengenai tanda hutang perseroan" sebagaimana diatur dalam Pasal 264 (1) KUHP termaksud dalam dakwaan alternatif pertama, dan menghukum terdakwa Budiman Hidayat dengan pidana penjara selama 1 (satu) tahun.....

Sedangkan barang bukti berupa 1 (satu) unit Computer IBM No. 1025169 dan monitor IBM No. 9704145 serta uang tunai sebesar Rp. 42.400.000,- dikembalikan kepada P.T. Bank Bali Jalan Hayam Wuruk Jakarta Barat. Dan barang bukti berupa 1 (satu) lembar rekening Koran atas nama Diana Kamdani, Giro Bilyet No. 103791 dan 103790, cheque No. 036728 serta photo copy Transsaction journal, tetap dalam berkas perkara.....

Serta menetapkan agar terdakwa dihukum membayar ongkos perkara Rp. 1.000,- (seribu rupiah);.....

Mendengar pembelaan dari penasehat hukum terdakwa;.....

Terdakwa berada di luar tahanan berdasarkan Penetapan Pengadilan Negeri Jakarta Barat No. 1050/Pen.Pid/S/1989?PN.Jkt.Bar. tgl 4 Oktober 1989;

Menimbang, bahwa Terdakwa menurut surat dakwaan Jaksa Penuntut Umum tgl. 29 September 1989 telah didakwa seperti diuraikan di bawah ini:

Dakwaan :

PERTAMA:

Bahwa ia terdakwa Budiman Hidayat pada tanggal 10 Pebruari 1989, setidak-tidaknya pada waktu yang lain tetapi masih dalam tahun 1989, bertempat di kantor P.T. Bank Bali Jl. Hayam Wuruk 84-85 Jakarta, setidak-tidaknya di tempat lain yang dapat diadili oleh Pengadilan Negeri Jakarta Barat;

telah membuat surat palsu mengenai surat hutang atau tanda hutang dari suatu perseroan yaitu berupa Transaktion Journal, yang dapat menerbitkan sesuatu hak, sesuatu perikatan atau kewajiban, atau yang dapat dipergunakan sebagai keterangan membuktikan sesuatu hal, dengan maksud akan mempergunakan atau menyuruh orang lain menggunakan surat itu seolah-olah asli dan tidak dipalsukan, perbuatan mana menimbulkan kerugian yang diderita P.T. Bank Bali Jakarta;

Perbuatan mana dilakukan terdakwa selaku karyawan P.T. Bank Bali Bagian Kliring dengan mengetahui atau menguji coba cara menggunakan computer B-3 yang kebetulan ditinggalkan petugas dalam keadaan terbuka, lalu terdakwa menginput seolah-olah ada setoran warkat Giro Bilyet atau warkat lainnya masuk ke rekening saksi Diana Kamdani No. A/C III-3618-4 seharga Rp. 43.500.000,- dan setelah terdakwa melihat hasil (output) nya benar telah masuk setoran warkat fiktif itu ke dalam rekening saksi Diana Kamdani telah menarik Giro Bilyet P.T. Bank Bali No. 103791 dan no. 36728 sehingga uang termaksud dalam Transaction Journal telah dimiliki terdakwa dengan cara Rp. 40.000.000,- dimaksudkan

menjadi deposito terdakwa pada Bank Buana Indonesia Jakarta, Rp. 3.000.000,- dimasukkan menjadi Tabanas pada P.T. Bank Bali Jakarta, sedangkan sisa Rp. 500.000,- telah habis dipergunakan terdakwa, mengakibatkan kerugian diderita P.T. Bank Bali sebesar Rp. 43.000.000,- setidak-tidaknya Rp. 1.100.000,- karena hasil tersebut sebesar Rp. 42.000.000,- berhasil diamankan dan akhirnya disita menjadi barang bukti dalam perkara ini; merupakan kejahatan yang diancam pidana sebagaimana diatur dalam pasal 264 ayat (1) KUHP; atau:

KEDUA:

Bahwa ia terdakwa Budiman Hidayat pada waktu dan tempat sebagaimana ditentukan dalam dakwaan alternatif pertama di atas,.....
dengan sengaja telah menggunakan surat palsu mengenai surat hutang atau tanda hutang dari suatu perseroan yaitu Transaction Journal seolah-olah asli dan tidak dipalsukan yaitu seolah-olah benar ada setoran warkat dan telah memiliki uang setoran warkat fiktif tersebut dengan cara dibantu saksi Diana Kamdani menarik dengan menerbitkan Giro Bilyet dan cheque tersebut dalam dakwaan alternatif pertama dan berhasil dicairkan sehingga uangnya berhasil dikuasai, dimiliki terdakwa yaitu sebesar Rp. 40.000.000,- dimasukkan menjadi deposito pada P.T. Bank Buana Indonesia Rp. 3.000.000,- dimasukkan menjadi Tabanas pada P.T. Bank Bali dan sisa Rp. 500.000,- telah habis dipergunakan terdakwa, akibat perbuatan mana menjadi kerugian P.T. Bank Bali Jakarta berupa uang tunai sebesar yang ditentukan itu, setidak-tidaknya sebesar Rp. 1.100.000,- karena

diantara hasil kejahatan tersebut ada yang dapat diamankan akhirnya disita menjadi barang bukti perkara ini sebesar Rp. 42.400.000,-; Merupakan kejahatan yang diancam dengan pidana sebagaimana diatur dalam pasal 264 ayat (2) KUHP; atau:

KETIGA:

Bahwa ia terdakwa Budiman Hidayat pada waktu dan tempat sebagaimana ditentukan dalam dakwaan alternatif pertama di atas Dengan maksud akan memiliki dengan melawan hukum, telah mengambil sesuatu barang berupa uang tunai sebesar Rp. 43.500.000,- yang seluruh atau sebagiannya bukan kepunyaan terdakwa, menjadi kerugian dari P.T. Bank Bali Jakarta; Perbuatan mengambil dapat dilakukan terdakwa melalui computer B-3, bahwa terdakwa selaku karyawan P.T. Bank Bali Bagian Kliring telah mengetahui karena sebab lain telah menggunakan (menginput) computer B-3 yang kebetulan ditinggalkan petugas dalam keadaan terbuka, lalu terdakwa menginput seolah-olah ada setoran warkat sebesar Rp. 43.500.000,- lalu dimasukkan ke rekening saksi Diana Kamdani yaitu kakak ipar terdakwa No. A/C 111-368-4 dan setelah melihat hasil (output dari computer tersebut) dalam transaction Journal benar, setoran fiktif telah masuk ke dalam rekening saksi Diana Kamdani tersebut diatas, selanjutnya terdakwa menghubungi dan minta bantuan saksi Diana Kamdani, lalu diterbitkan/ditarik Giro Bilyet No. 103790 dan no. 103791 serta cheque No. 036728, dan berhasil dicairkan, uang hasil pencairannya dapat dimiliki terdakwa dengan cara sebesar

Rp. 40.000.000,- dimasukkan menjadi deposito, sebesar 3.000.000,- dimasukkan menjadi Tabanas dan selebihnya Rp. 500.000,- habis dipergunakan terdakwa mengakibatkan kerugian diderita PT Bank Bali Jakarta setidak-tidaknya seharga lebih dari Rp. 250,-;

Merupakan kejahatan yang diancam pidana sebagaimana diatur dalam pasal 362 KUHP;

Menimbang, bahwa dipersidangan telah diperiksa saksi-saksi memberi keterangan dibawah sumpah sebagai berikut:

SAKSI I: DIANA KAMDANI

- Bahwa saksi adalah kakak ipar terdakwa;
- bahwa benar saksi menjadi nasabah P.T. Bank Bali Jl. Hayam Wuruk dengan nomer A/C.00111.3618.4;
- bahwa hal ini diketahui oleh terdakwa oleh karena sebagai karyawan Bank Bali yang setiap ada pengeluaran atau pemasukan dalam rekening tersebut, terdakwa selalu diminta untuk mengeceknya;
- bahwa pada bulan Pebruari 1989 saksi pernah menerima telepon dari terdakwa yang mengatakan bahwa ada teman akan menitipkan uang pada rekeningnya yang dalam hal ini saksi menyetujui asal betul ada uangnya;

- bahwa beberapa hari kemudian saksi diberitahu terdakwa bahwa uang sebesar Rp. 43.500.000,- sudah masuk ke rekening saksi dan kemudian atas permintaan terdakwa, saksi menarik Giro Bilyet sebanyak (dua) lembar dan 1 (satu) lembar cheque untuk mencairkan saldo tersebut, yaitu Giro Bilyet senilai Rp. 40.000.000,- dan Rp. 3.000.000,- serta dengan cheque sebesar Rp. 500.000,-;
- bahwa saksi mengakui tidak pernah mengadakan pengecekan di Bank Bali, ternyata apa yang dikatakan terdakwa adalah bohong;
- teman yang dikatakan oleh terdakwa sebenarnya tidak ada dan ternyata yang dikatakan teman terdakwa adalah terdakwa sendiri;

SAKSI II: I.C.SUDARMANTO G.OE.:

- bahwa saksi kenal dengan terdakwa karena sama-sama karyawan Bank Bali;
- bahwa saksi mengetahui adanya penyimpangan pada peng-inputan data komputer dari rekannya bernama Dongata dan Candra bagian Procesing; Atas dasar itu saksi kemudian lapor kepada atasan;
- bahwa terdakwa kemudian dipanggil dan ternyata terdakwa mengakui telah melakukan penyimpangan yaitu mengambil uang dengan penginputan data komputer seolah-olah ada setoran warkat kepada rekening nasabah Diana Kamdani No. A/C 00111.3618.4 sebesar Rp. 43.500.000,-;
- bahwa uang tersebut telah berhasil diambil oleh terdakwa melalui Giro Bilyet No. 103791 nominal Rp. 40.000.000,- didepositokan ke Bank Buana

Indonesia, Giro Bilyet No. 103790 nominal Rp. 3.000.000,- masuk Tabanas di Bank Bali atas nama terdakwa, dan cheque no. 036728 nominal Rp. 500.000,- atas nama terdakwa;

- bahwa akibat dari perbuatan tersebut terdakwa telah di-PHK-kan sejak bulan Juni 1989;

SAKSI III: NG WIE HUNG:

- bahwa saksi sebagai karyawan Bank Bali kenal dengan terdakwa dan bekerja pada suatu ruangan dengan terdakwa di bagian Giro;
- bahwa benar saksi pada tanggal 10 Pebruari 1989 telah menggunakan komputer B-3, menginput data; ternyata didalamnya terdapat saldo atas nama Diana Kamdani bertambah sebesar Rp. 43.500.000,-;
- bahwa benar pada waktu itu saksi sekitar jam 17.25 Wib. pergi ke bagian belakang untuk melihat hasil catatan data yang sudah diinput, sedangkan terminal Computer masih terbuka (tidak terkunci) karena komputer itu masih akan digunakan untuk menginput sesuai tugasnya;
- bahwa sesuai dengan pemberitahuan atasan, benar yang menginput data sehingga saldo atas nama saksi Diana Kamdani bertambah Rp. 43.500.000,- adalah terdakwa;
- bahwa saksi telah pernah mengijinkan terdakwa untuk menggunakan komputer tersebut dalam keadaan terbuka;

SAKSI IV: IMAM HARTONO

- bahwa saksi sudah kenal dengan terdakwa karena sama-sama sebagai karyawan P.T. Bank Bali yang mempunyai tugas menerima setoran nasabah dari nasabah dan menginput setoran dari nasabah;
- bahwa ternyata ada kejanggalan pada catatan Transaction Journal tanggal 10 Pebruari 1989 ada data inputan di kantor pusat kepada nama saksi (code teller:333) berupa setoran warkat sebesar Rp. 43.500.000,-;
- bahwa atas dasar itu kemudian saksi lapor ke bagian Kliring Jl. Thamrin dan kantor pusat Jl. Hayam Wuruk untuk diproses;
- bahwa saksi mengatakan hasil proses tersebut sejak diperiksa di kantor Polisi bahwa ternyata terdakwa menginput dengan komputer B-3 seolah-olah ada setoran warkat ke rekening No. 00111.3618.4 atas nama Diana Kamdani;
- bahwa benar transaction journal ini yang dimaksud saksi dengan catatan;

SAKSI V: ALBERT BAMBANG

- bahwa sebagai karyawan P.T. Bank Bali bertugas dibagian Finance Control pada Team Emplimentasi Computer;
- bahwa tanggal 10 Pebruari 1989 di dalam "Transaction Journal" ada setoran warkat sebesar Rp. 43.500.000,- yang ternyata tidak ada warkatnya, maka kemudian dicari dan diketahui rekening tersebut masuk ke rekening No. A/C 00111.3618.4 atas nama Diana Kamdani;

- bahwa uang sejumlah itu sudah dicairkan dengan dua kali penarikan, pertama dengan kliring dan kedua dengan cheque tunai;
- bahwa data tersebut di-input melalui komputer B-3 dengan User ID saksi Ng Wie Hung dan teller indentity No. 271;

Menimbang bahwa terdakwa dipersidangan telah memberi keterangan sebagai berikut:

- bahwa terdakwa bekerja di Bank Bali Jl. Hayam Wuruk sejak tahun 1984 dan bertugas di bagian Kliring sejak 2 (dua) tahun yang lalu;
- bahwa terdakwa mengaku benar telah menggunakan komputer B-3 pada saat mati dengan seijin petugasnya/ pemakai-nya;
- bahwa setelah mencoba menginput data dan telah masuk, kemudian hasilnya dilihat terdakwa pada layar komputer sebesar Rp. 43.500.000,- seolah-olah ada setoran warkat ke dalam rekening A/C 00111.3618.4 atas nama kakak ipar terdakwa yaitu saksi Diana Kamdani;
- bahwa kemudian terdakwa menemui kakak iparnya Diana Kamdani dengan mengatakan ada setoran masuk ke A/C-nya dan minta agar saksi mau menarik Giro dan cheque untuk mancairkan dana tersebut, ternyata saksi Diana Kamdani tidak berkeberatan asal setorannya bagus;
- bahwa komputer B-3 yang dipergunakan terdakwa menginput seolah-olah setoran warkat dengan teller No. 333 milik saksi Imam Hartono dan Code User I.D. milik saksi Ng Wie Hung;

- bahwa benar yang di input terdakwa adalah yang tertuang dalam bukti "Transaction Journal" tertanggal 10 Pebruari 1989 sekitar jam 17.19.39 Wib. melalui Komputer B-3 milik Bank Bali Pusat, seolah-olah ada setoran warkat sebesar Rp. 43.500.000,- ke rekening saksi Diana Kamdani No. A/C 00111.3618.4;
- bahwa saldo sebesar Rp. 43.500.000,- tersebut sudah dicairkan terdakwa melalui kliring Giro Bilyet No. 103791 tanggal 13 Pebruari 1989 nominal Rp. 40.000.000,- dan kemudian dimasukkan deposito terdakwa ke Bank Buana Indonesia, Giro Bilyet No. 103790 tanggal 13 Pebruari 1989 nominal Rp. 3.000.000,- oleh terdakwa dimasukkan menjadi tabanas di Bank Bali dan dengan cheque No. 036728 tanggal 13 Pebruari 1989 nominal Rp. 500.000,- yang dipakai untuk kepentingan terdakwa sendiri;
- bahwa uang sebesar Rp. 43.500.000,- hasil kejahatan yang dilakukan terdakwa tersebut seluruhnya sudah dikembalikan oleh terdakwa yaitu langsung ke Bank Bali sebesar Rp. 42.400.000,- melalui wesel yang dikirimkan oleh terdakwa tanggal 21 Oktober 1989 sebesar Rp. 1.100.000,-;
- bahwa yang mendorong terdakwa melakukan perbuatan tersebut di atas adalah karena terdakwa ingin membeli rumah;

Menimbang, bahwa barang bukti yang diajukan di persidangan adalah berupa:

1. 1 (satu) lembar Giro Bilyet No. 103791 nominal Rp. 40.000.000,-;
2. 1 (satu) lembar Giro Bilyet No. 103790 nominal Rp. 3.000.000,-;

3. 1 (satu) lembar cheque No. 036.728 nominal Rp. 500.000,-;
4. Photocopy Transaction Journal tanggal 10 Pebruari 1989;
5. 1 (satu) lembar rekening koran atas nama Diana Kamdani;
6. 1 (satu) Unit Computer IBM No. 1025169 dan Monitor IBM No. 9704145;
7. Uang tunai sebesar Rp. 42.400.000,- yang dititipkan di Bank Indonesia cabang Jakarta Kota;

Menimbang, bahwa oleh jaksa Penuntut Umum, terdakwa Budiman Hidayat telah didakwa:

- Pertama: melanggar Pasal 264 ayat (1) KUHP;
- Atau Kedua: melanggar Pasal 264 ayat (2) KUHP;
- Atau Ketiga: melanggar Pasal 362 KUHP;

Menimbang, bahwa terhadap dakwaan pertama: melanggar Pasal 264 ayat(1) KUHP, Pengadilan tidak sependapat dengan pendapat jaksa Penuntut Umum yang mengatakan perbuatan terdakwa telah memenuhi unsure dari pasal 264 ayat (1) KUHP tersebut yaitu melakukan tindak pidana "Membuat surat palsu mengenai surat hutang atau tanda hutang dari sesuatu Perseroan", oleh karena menurut hemat kami perbuatan terdakwa menginput data dengan menggunakan Komputer B-3 seolah-olah ada setoran warkat ke dalam rekening A/C 00111.3618.4 atas nama saksi Diana Kamdani uang sebesar Rp. 43.500.000,- yang hasilnya dapat dilihat pada layar komputer, tidak dapat diklasifikasikan

sebagai pemalsuan surat atau membuat surat palsu mengenai surat hutang dan tanda hutang dari sesuatu perseroan sebagaimana dimaksudkan oleh jaksa Penuntut Umum dalam tuntutannya/requisitoirnya;

Menimbang, bahwa menurut hemat kami perbuatan terdakwa sengan menginput data komputer, seolah-olah ada setoran warkat kepada rekening nasabah Diana Kamdani A/C 00111.3618.4 sebesar Rp. 43.500.000,- adalah salah satu cara yang dilakukan terdakwa untuk mengambil uang milik Bank Bali dimana terdakwa bekerja;

Menimbang, bahwa transaction journal tgl. 10 Pebruari 1989 yang memuat data penginputan berupa setoran warkat sebesar Rp. 43.500.000,- adalah bukan merupakan surat palsu, akan tetapi merupakan hasil cetakan atas penginputan data komputer yang dilakukan oleh terdakwa;

Menimbang, bahwa berdasarkan pertimbangan tersebut, jelas perbuatan terdakwa tidak memenuhi unsure pasal 264 ayat (1) KUHP sebagaimana didakwakan Jaksa Penuntut Umum pada dakwaan pertama, sehingga oleh karena terdakwa harus dibebaskan dari dakwaan pertama tersebut;

Menimbang, bahwa mengenai dakwaan alternatif atau Kedua melanggar Pasal 264 ayat (2) KUHP, menurut hemat kami berdasarkan atas keterangan saksi-saksi dan pengakuan terdakwa, perbuatan terdakwa terbukti tidak memenuhi

unsure pasal 264 ayat (2) KUHP yaitu dengan sengaja memakai surat yang isinya tidak benar dan dipalsu sehingga menimbulkan kerugian;

Menimbang, bahwa seperti telah diuaraikan diatas, "Transaction Journal" tanggal 10 Pebruari 1989 yang memuat warkat sebesar Rp. 43.500.000,- yang ternyata warkat tersebut tidak ada, bukanlah merupakan surat palsu, oleh karena menurut saksi Imam Hartono dan saksi Albert Bambang, Transaction Journal tersebut merupakan cetakan hasil penginputan data melalui Computer B-3 dengan User I.D. Saksi Ng Wie Hung dan Teller Identity No. 271 yang dilakukan oleh terdakwa;

Menimbang, bahwa dengan demikian pencairan uang sebesar Rp. 43.500.000,- oleh terdakwa melalui Giro Bilyet No. 103791 nominal 40.000.000,- Giro Bilyet No. 103790 nominal Rp. 3.000.000,- dan dengan cheque tunai nominal Rp. 500.000,- tidak dapat diklasifikasikan sebagai "dengan sengaja memakai surat yang isinya tidak benar dan dipalsu" sehingga menimbulkan kerugian dalam hal ini Bank Bali sebagaimana dakwaan Jaksa Penuntut Umum dalam dakwaan alternatif atau kedua, oleh karena sebenarnya perbuatan terdakwa tersebut hanyalah merupakan salah satu cara untuk mengambil uang milik Bank Bali;

Menimbang, bahwa oleh karena dalam dakwaan alternatif ketiga, terdakwa telah didakwa melanggar pasal 362 KUHP yang unsur-unsurnya:

1. Barang siapa;
2. Mengambil barang sesuatu;
3. Barang tersebut seluruhnya atau sebagian kepunyaan orang lain;
4. Dengan maksud untuk dimiliki secara melawan hukum;

ad.1. Tentang Unsur ke-1: "Barang siapa":

Menimbang, bahwa yang dimaksud barang siapa dalam perkara ini tiada lain adalah terdakwa Budiman Hidayat;

ad.2. Tentang Unsur ke-2: "Mengambil barang sesuatu";

Menimbang, bahwa barang menurut pengertian pasal 362 KUHP dapat berujud baik barang bergerak maupun barang berujud uang;

Menimbang, bahwa mengenai unsur kedua ini dapat dipertimbangkan sebagai berikut:

- bahwa di persidangan terdakwa telah mengakui benar pada tgl. 10 Pebruari 1989 telah mengambil uang kepunyaan P.T. Bank Bali, dimana ia terdakwa bekerja di bagian kliring sebesar Rp. 43.500.000,- dengan cara menginput data komputer dengan menggunakan komputer B-3 yang

dalam keadaan terbuka dan setelah data masuk, hasilnya dapat dilihat pada layar komputer sebesar Rp. 43.500.000,- seolah-olah ada setoran warkat kedalam rekening AC 00111.3618.4 atas nama kakak ipar terdakwa Diana Kamdani;

- bahwa kemudian terdakwa menemui saksi Diana Kamdani mengatakan ada setoran masuk ke AC. 00111.3618.4 atas nama Diana Kamdani dan minta agar saksi mau menarik Giro dan cheque untuk mencairkan dana tersebut, dan saksi Diana Kamdani tidak berkeberatan asal setorannya bagus;
- bahwa dengan cara demikian uang sebesar Rp. 43.500.000,- oleh terdakwa pada tanggal 13 Pebruari 1989 telah berhasil diambil melalui Giro Bilyet No. 103791 nominal Rp. 40.000.000,- didepositokan di Bank Buana Indonesia Giro Bilyet No. 103790 nominal Rp. 3.000.000,- oleh terdakwa dimasukkan Tabanas di Bank Bali atas nama terdakwa, dan cheque tunai No. 036,728 nominal Rp. 500.000,- untuk kepentingan terdakwa sendiri;
- bahwa menurut pengakuan terdakwa, penginputan data tersebut dilakukan dengan menggunakan Komputer B-3 dengan kode teller 333 milik saksi Imam Hartono dan Code User I.D. milik saksi Ng Wie Hung yang pada waktu itu ditinggalkan dalam keadaan terbuka;

Menimbang, bahwa menurut saksi Imam Hartono, akibat dari perbuatan terdakwa menginput data Komputer seolah-olah ada setoran warkat Rp.

43.500.000,- ke dalam rekening AC. 00111.3618.4 atas nama saksi Diana Kamdani, maka timbul kejanggalan pada catatan saksi yaitu dalam Transaction Journal tanggal 10 Pebruari 1989 ada data inputan di kantor Pusat kepada nama saksi (Code teller 333) berupa setoran warkat Rp. 43.500.000,- dan setelah diadakan pengecekan ternyata terdakwa telah mengakui menginput dengan komputer B-3 seolah-olah ada setoran warkat ke rekening No. 00111.3618.4 atas nama Diana Kamdani, padahal sebenarnya setoran warkat Rp. 43.500.000,- tersebut tidak ada;

Menimbang, bahwa berdasar atas uraian tersebut di atas jelas unsur kedua pasal 362 KUHP terpenuhi;

ad.3. Tentang Unsur ke-3:

"barang tersebut seluruhnya atau sebagian kepunyaan orang lain";

Menimbang, bahwa mengenai unsur ketiga dari pasal 362 KUHP bahwa barang tersebut seluruhnya atau sebagian kepunyaan orang lain, baik menurut pengakuan terdakwa maupun keterangan saksi-saksi dipersidangan, uang sebesar Rp. 43.500.000,- yang diambil terdakwa adalah bukan kepunyaan terdakwa sama sekali akan tetapi kepunyaan Bank Bali Jalan Hayam Wuruk Jakarta Barat;

ad.4. Tentang unsur ke-4:

"dengan maksud untuk dimiliki secara melawan hukum";

Menimbang, bahwa setelah terdakwa berhasil mencairkan uang sebesar Rp. 43.500.000,- dari P.T. Bank Bali pada tanggal 13 Pebruari 1989 melalui Giro Bilyet No. 103791 nominal dan cheque tunai No. 036.728 nominal 500.000,- maka uang sebesar Rp. 43.500.000,- tersebut oleh terdakwa telah didepositokan ke Bank Buana Indonesia sebesar Rp. 40.000.000,- dimasukkan Tabanas ke Bank Bali sebesar Rp. 3.000.000,- atas nama terdakwa, sedang yang Rp. 500.000,- telah habis dipergunakan untuk kepentingan terdakwa sendiri, sedangkan terdakwa mengetahui bahwa uang sebesar Rp. 43.500.000,- tersebut adalah bukan miliknya akan tetapi seluruhnya kepunyaan P.T. Bank Bali Jl. Hayam Wuruk Jakarta Barat;

Menimbang, bahwa dengan dimasukkannya uang sebesar Rp. 43.500.000,- kepunyaan P.T. Bank Bali ke dalam deposito Bank Buana Indonesia sebesar Rp. 40.000.000,- atas nama terdakwa, kedalam Tabanas sebesar Rp. 3.000.000,- ke Bank Bali dan dipergunakannya sebesar Rp. 500.000,- untuk kepentingan terdakwa, maka sudah jelas terdakwa bermaksud akan memiliki barang/uang tersebut secara melawan hukum, sehingga dengan demikian terbukti unsur keempat dari pasal 362 KUHP terpenuhi;

Menimbang, bahwa Penasehat Hukum terdakwa dalam pembelaannya yang disampaikan secara lisan mengatakan tidak sependapat dengan jaksa Penuntut Umum dalam requisitoirnya yang menyatakan terdakwa terbukti salah melanggar pasal 264 ayat (1) KUHP maupun pasal 264 ayat (2) KUHP, tetapi memenuhi unsur pasal 362 KUHP sebagaimana didakwakan Jaksa Penuntut Umum dalam

dakwaan alternatif atau ketiga. Dan selanjutnya Penasehat Hukum terdakwa tersebut mohon agar kepada terdakwa dikenakan hukuman yang seringan-ringannya oleh karena uang sebesar Rp. 43.500.000,- telah dikembalikan seluruhnya kepada P.T. Bank Bali, demikian juga dari pihak Bank sendiri telah menyatakan agar supaya kepada terdakwa diberi keringanan hukuman;

Menimbang, bahwa berdasar atas pertimbangan-pertimbangan seperti diuraikan di atas Pengadilan berpendapat perbuatan terdakwa Budiman Hidayat telah memenuhi semua unsur pasal 362 KUHP maka oleh karena itu telah terbukti dengan sah dan meyakinkan pula kesalahan terdakwa yaitu terdakwa telah melakukan tindak pidana "Pencurian" melanggar pasal 362 KUHP sebagaimana didakwakan Jaksa Penuntut Umum dalam dakwaan alternatif atau ketiga sebagai pertimbangan yang meringankan terdakwa;

Menimbang, bahwa sebelum pengadilan menjatuhkan pidana perlu dipertimbangkan keadaan yang memberatkan dan yang meringankan bagi terdakwa;

Keadaan yang memberatkan:

- Perbuatan terdakwa sudah merugikan Bank Bali, meskipun terdakwa sudah mengembalikan uang hasil kejahatannya kepada Bank tersebut;

- Terdakwa sebagai karyawan Bank Bali telah menggunakan kesempatan untuk mencari keuntungan bagi dirinya sendiri;

Keadaan yang meringankan:

- Uang sebesar Rp. 43.500.000,- Kepunyaan P.T. Bank Bali sudah dikembalikan seluruhnya oleh terdakwa;
- Terdakwa menyatakan sangat menyesal atas perbuatannya;
- Dari pihak Bank Bali menyatakan persoalannya sudah beres dan memohonkan keringanan kepada terdakwa;
- Terdakwa masih muda dan sudah di-PHK-kan dan belum pernah dihukum;
- Dipersidangan terdakwa bersikap sopan dan mengakui semua perbuatannya;

Mengingat, pasal 362 KUHP dan pasal-pasal dari peraturan perundang-undangan yang bersangkutan;

MENGADILI:

1. Menyatakan, terdakwa: BUDIMAN HIDAYAT

   Tidak bersalah atas dakwaan pertama dan dakwaan alternatif atau kedua dari jaksa penuntut umum, oleh karena itu membebaskan terdakwa dari dakwaan pertama dan dakwaan alternatif atau kedua tersebut;

2. Menyatakan Terdakwa bersalah melakukanh tindak pidana "PENCURIAN" sebagaimana didakwakan Jaksa Penuntut Umum dalam dakwaan alternatif atau ketiga;

3. Memidana oleh karena itu kepada terdakwa dengan pidana penjara selama: 6 (enam) bulan;

   Dengan ketentuan pidana tersebut tidak usah dijalani, kecuali jika dikemudian hari ada putusan Hakim yang menentukan lain disebabkan karena terpidana melakukan suatu perbuatan pidana sebelum masa percobaan selama 1 (satu) tahun dalam perintah tersebut habis;

4. Menghukum terdakwa membayar ongkos perkara sebesar Rp. 1.000,-

5. Menetapkan barang bukti berupa 1 (satu) Unit Computer IBM No. 1025169 dan Monitor merk IBM No. 9704145 serta uang tunai sebesar Rp. 42.400.000,- dikembalikan kepada P.T. Bank Bali Jalan Hayam Wuruk Jakarta Barat;

   Sedangkan barang bukti berupa Giro Bilyet No. 103791, No. 103790, cheque No. 036728 dan 1 (satu) lembar rekening Koran atas nama Diana Kamdani serta photocopy Transaction Journal, tetap dalam berkas perkara;

Demikianlah diputuskan oleh pengadilan Negeri Jakarta Barat pada hari: SENIN, tanggal 20 NOPEMBER 1989 dan pada hari itu juga diucapkan di dalam

persidangan yang terbuka untuk umum oleh kami: STEPHANUS KASIHAN, S.H. Hakim Pengadilan Negeri Jakarta Barat dan dihadiri oleh: R. SILABAN, S.H. Jaksa Penuntut Umum, serta Terdakwa dan Penasehat Hukumnya, dengan dibantu oleh Panitera Pengganti: Makmun Murtado, S.H.;

PANITERA PENGGANTI TSB., HAKIM TSB.,

ttd ttd

MAKMUN MURTADO, S.H. STEPHANUS KASIHAN, S.H.

NIP. 040032332 NIP. 040006629

Putusan ini telah mempunyai kekuatan hukum yang tetap tanggal 28 Nopember 1989, karena jaksa penuntut umum dalam masa pikir-pikir sampai tenggang waktu yang ditentukan, tidak mengajukan permohonan Banding;

PANITERA PENGGANTI TSB.,

ttd

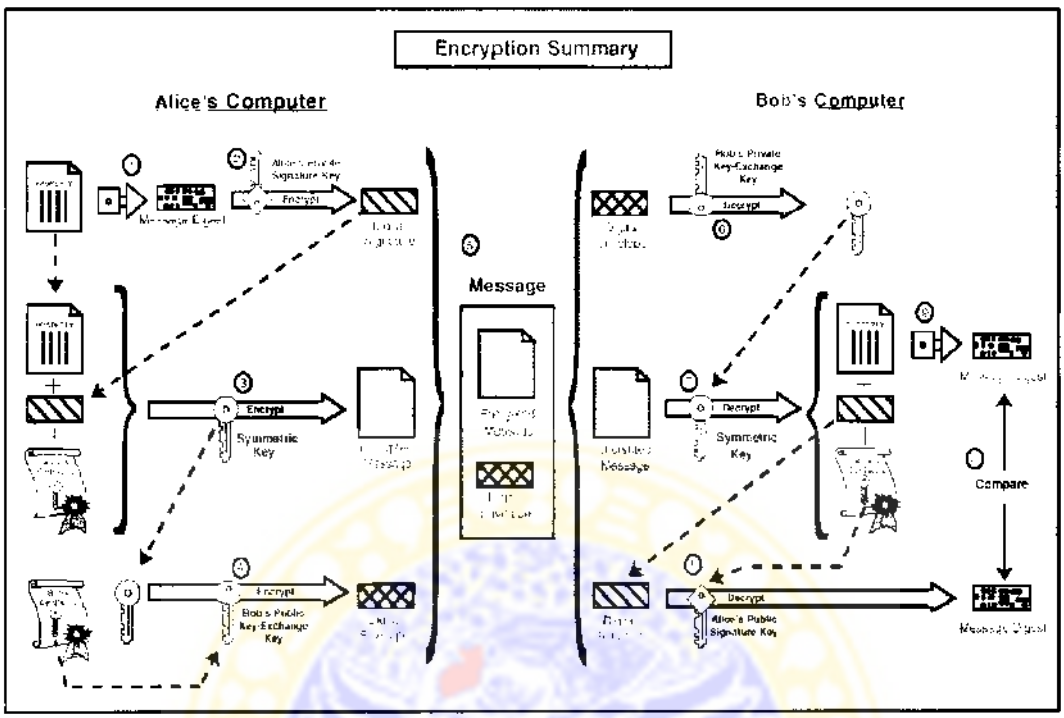
MAKMUN MURTADO, S.H.

NIP. 040032332

LAMPIRAN II

BENTUK PENGGUNAAN *DIGITAL SIGNATURE*

Contoh dari penggunaan *digital signature* adalah sebagai berikut, Alice akan membuat *message digest* dari data atau pesan yang hendak ia kirimkan. Kemudian *messages digest* tersebut dienkripsi dengan menggunakan kunci privat yang ia punyai, hasil yang didapat adalah *digital signature* dari data tersebut. Ia kemudian mentransmisikan data dan *digital signature* itu kepada Bob. Bob pada saat menerima pesan itu akan melihat *messages digest* dari pesan dan kemudian ia akan membandingkan hasilnya dengan hasil dari *digital signature*. Apabila hasil yang didapat dari keduannya adalah sama maka Bob akan merasa yakin bahwa pesan yang telah ditandatangani oleh Alice dengan menggunakan kunci privatnya adalah tidak pernah berubah sejak dibuat. Selanjutnya, diagram dibawah ini akan menunjukkan bagaimana suatu proses *enkripsi* berjalan apabila Alice ingin menandatangani suatu pesan dan mengirimkannya kepada Bob.



Gambar *encryption summary*

Gambar diatas menunjukan proses *kriptografi* yang terjadi dalam *digital signature*, langkah-langkah dalam melakukan *enkripsi* ini adalah sebagai berikut:

No	Penjelasan
1	Alice menjalankan (*runs*) data yang hendak ia kirimkan, melalui algoritma satu arah (*one way algorithm*) sehingga ia mendapat suatu nilai (*value*) yang unik dari data tersebut. Nilai ini disebut ***message digest***. Nilai adalah semacam sidik jari bagi data tersebut dan akan digunakan

dalam proses yang lebih lanjut untuk meneliti keutuhan (*integrity*) dari data tersebut.

2 Alice kemudian melakukan *enkripsi* terhadap *messages digest* tersebut dengan menggunakan kunci privatnya sehingga ia akan mendapatkan *digital signature* dari data tersebut.

3 Kemudian, Alice membuat (*generates*) suatu kunci simetris secara acak (*random*) dan menggunakan kunci itu melakukan *enkripsi* terhadap data yang hendak ia kirimkan, tandatangan (*signature*) miliknya, dan salinan dari sertifikat digitalnya yang berisi kunci publiknya. Untuk mendekripsi data tersebut Bob membutuhkan salinan dari kunci simetris tersebut.

4 Alice harus memiliki terlebih dahulu sertifikat milik Bob, sertifikat ini berisi salinan (*copy*) dari kunci publik milik Bob. Untuk menjamin keamanan transmisi dari kunci simetris maka kunsi tersebut dienkripsi dengan menggunakan kunci publik milik Bob. Kunci yang telah dienkripsi yang dikenal sebagai amplop digital (*digital envelope*) akan dikirimkan bersama-sama dengan data yang telah dienkripsi.

5 Alice kemudian akan mengirimkan data (*message*) tersebut yang berisi data yang telah dienkripsi dengan kunci simetris, tandatangan dan sertifikat digital, serta kunci simetris yang telah dienkripsi dengan kunci asimetris (*digital envelope*).

6 Bob menerima pesan (*messages*) dari Alice tersebut dan kemudian mendekripsi amplop digital dengan kunci privat yang dipunyainya, ia kemudian akan mendapatkan kunci asimetris.

7 Bob kemudian menggunakan kunci simetris tersebut untuk mendekripsi data itu (*property descryption*), tandatangan Alice, dan sertifikat miliknya.

8 Ia kemudian mendekripsi *digital signature* milik Alice dengan menggunakan kunci publik milik Alice, yang didapat Bob dari sertifikat milik Alice. Dari *dekripsi* ini akan didapatkan *message digest* dari data tersebut.

9 Bob kemudian memproses (*run*) data itu dengan menggunakan algoritma satu arah yang sama yang digunakan Alice untuk *message digest*.

10 Akhirnya Bob akan membandingkan antara *message digest* yang didapatkannya dari proses *dekripsi* diatas dengan *message digest* yang didapatkan dari *digital signature* milik Alice. Kalau hasil yang didapat dari perbandingan itu adalah sama maka, Bob dapat merasa yakin bahwa data tersebut tidak pernah dirusak (*altered*) selama proses transmisi dan data itu ditandatangani dengan menggunakan kunci privat milik Alice.

Kalau hasil dari perbandingan itu adalah tidak sama, maka data tersebut pastilah telah diubah atau dipalsukan setelah ditandatangani.