SKRIPSI

KODE SUMBER (*SOURCE CODE*) WEBSITE SEBAGAI ALAT BUKTI DALAM TINDAK PIDANA TERORISME DI INDONESIA

(STUDI KASUS WEBSITE ANSHAR.NET)

DIAJUKAN DALAM RANGKA MEMENUHI TUGAS AKHIR
UNTUK MENCAPAI GELAR SARJANA HUKUM
PADA FAKULTAS HUKUM UNIVERSITAS INDONESIA

OLEH:

AHMAD ZAKARIA
NOMOR POKOK MAHASISWA: 0503000166
BIDANG STUDI HUKUM ACARA

FAKULTAS HUKUM
UNIVERSITAS INDONESIA
DEPOK 2007

ABSTRAK

Ahmad Zakaria. 0503000166. Skripsi. Program Kekhususan III (Bidang Studi Hukum Acara). **Kode Sumber Website Sebagai Alat Bukti Dalam Tindak Pidana Terorisme di Indonesia (Studi Kasus Website Anshar.net)**

Terorisme merupakan kejahatan terhadap kemanusiaan dan peradaban serta merupakan salah satu ancaman serius terhadap kedaulatan setiap Negara. Upaya penanggulangan tindak pidana terorisme diwujudkan pemerintah dengan mengeluarkan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002, yang kemudian disetujui oleh DPR menjadi Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme. Diperlukannya undang-undang ini karena pemerintah menyadari tindak pidana terorisme merupakan suatu tindak pidana yang luar biasa (*extraordinary crime*), sehingga membutuhkan penanganan yang luar biasa juga (*extraordinary measures*). Dalam beberapa kasus, penguasaan terhadap teknologi sering kali disalahgunakan untuk melakukan suatu kejahatan. Diantara ragam kejahatan menggunakan teknologi, terdapat didalamnya suatu bentuk kejahatan terorisme baru, yaitu *cyberterrorism*. Penanganan *Cyberterrorism* berbeda dengan penanganan terorisme konvensional. Salah satu perbedaannya adalah penggunaan alat bukti berupa informasi elektronik. Bagaimana pengaturan penggunaan alat bukti berupa informasi elektronik dalam Hukum Acara Pidana di Indonesia? Dapatkah sebuah kode sumber website dijadikan alat bukti di persidangan Tindak Pidana Terorisme? Bagaimana dalam prakteknya penerapan ketentuan Hukum Acara Pidana Terhadap Informasi Elektronik (*Source Code Website*) di dalam Peristiwa Tindak Pidana Terorisme pada Kasus Website Anshar.net? Penggunaan alat bukti berupa informasi elektronik telah diakomodir oleh Pasal 27 Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme. Terkait hal tersebut diperlukan adanya Standar Operasional Prosedur dalam perolehan alat bukti berupa informasi elektronik tersebut.

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang

Hak untuk hidup adalah hak asasi yang paling dasar bagi seluruh manusia. Hak hidup merupakan bagian dari hak asasi yang memiliki sifat tidak dapat ditawar lagi (*non derogable rights*).[1] Artinya, hak ini mutlak harus dimiliki setiap orang, karena tanpa adanya hak untuk hidup, maka tidak ada hak-hak asasi lainnya. Hak tersebut juga menandakan setiap orang memiliki hak untuk hidup dan tidak ada orang lain yang berhak untuk mengambil hak hidupnya.

Dalam hal ini terdapat beberapa pengecualian seperti untuk tujuan penegakan hukum, sebagaimana yang diatur juga dalam *Article 2 European Convention on Human Rights* yang menyatakan:

---

[1] I Sriyanto dan Desiree Zuraida, *Modul Instrumen HAM Nasional: Hak Untuk Hidup, Hak Berkeluarga dan Melanjutkan Keturunan Serta Hak Mengembangkan Diri* (Jakarta: Departemen Hukum dan HAM RI, Direktorat Jenderal Perlindungan HAM, 2001) hal. 1

protection the right of every person to their life. The article contains exceptions for the cases of lawful executions, and deaths as a result of "the use of force which is no more than absolutely necessary" in defending one's self or others, arresting a suspect or fugitive, and suppressing riots or insurrections.[2]

Pengecualian terhadap penghilangan hak hidup tidak mencakup pada penghilangan hak hidup seseorang oleh orang lainnya tanpa ada alas hak yang berdasarkan ketentuan perundang-undangan yang berlaku. Salah satu contoh penghilangan hak hidup tanpa alas hak adalah pembunuhan melalui aksi teror. Aksi teror jelas telah melecehkan nilai kemanusiaan, martabat, dan norma agama. Teror juga telah menunjukan gerakannya sebagai tragedi atas hak asasi manusia.[3]

Terorisme merupakan kejahatan terhadap kemanusiaan dan peradaban serta merupakan salah satu ancaman serius terhadap kedaulatan setiap negara karena terorisme sudah merupakan kejahatan yang bersifat internasional yang menimbulkan bahaya terhadap keamanan, perdamaian dunia

---

[2] European Convention on Human Rights, <http://en.wikipedia.org/European_Convention_on_Human_Rights_files>, diakses 26 Desember 2006.

[3] Abdul Wahid, Sunardi, Muhamad Imam Sidik, *Kejahatan Terorisme: Perspektif Agama, HAM dan Hukum* (Bandung: PT. Refika Aditama, 2004), hal. 2.

serta merugikan kesejahteraan masyarakat sehingga perlu dilakukan pemberantasan secara berencana dan berkesinambungan sehingga hak asasi orang banyak dapat dilindungi dan dijunjung tinggi.[4] Pernyataan tersebut sejalan dengan tujuan bangsa Indonesia yang termaktub dalam Undang-undang Dasar 1945 yaitu melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia.[5]

Aksi terorisme di Indonesia mencuat ke permukaan setelah terjadinya Bom Bali I pada 12 Oktober 2002, Peristiwa ini tepatnya terjadi di *Sari Club* dan *Peddy's Club*, Kuta, Bali. Sebelumnya, tercatat juga beberapa aksi teror di Indonesia antara lain kasus Bom Istiqlal pada 19 April 1999, Bom Malam Natal pada 24 Desember 2000 yang terjadi di dua puluh tiga gereja, Bom di Bursa Efek Jakarta pada September 2000, serta penyanderaan dan pendudukan

---

[4] Indonesia, *Undang-undang Tentang Penetapan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme, Menjadi Undang-undang*, UU No. 15, LN. No. 45 Tahun 2003, TLN. No. 4284, Penjelasan umum Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme paragraf dua.(a)

[5] Indonesia, *Undang-undang Dasar 1945*, Pembukaan Alinea ke-4.

Perusahaan Mobil Oil oleh Gerakan Aceh Merdeka pada tahun yang sama.

Kembali pada kasus Bom Bali I. Aksi teror melalui peledakan bom mobil di Jalan Raya Legian Kuta ini semula direncanakan dilaksanakan pada 11 September 2002, bertepatan dengan peringatan setahun tragedi di Gedung World Trade Center New York, Amerika Serikat. Seperti diketahui, peristiwa 11 September 2002 ini mengawali "Perang Global" terhadap terorisme yang dipimpin oleh Amerika Serikat. Kebijakan Amerika Serikat yang berat sebelah seperti pemunculan jargon "Jihad adalah Terorisme" dalam memerangi terorisme telah menjadi alasan beberapa kelompok teroris untuk melakukan perlawanan, salah satunya dilakukan oleh Ali Imron, Ali Gufron, dan Amrozi.[6]

Indonesia sebagai negara hukum (*rechtstaat*) memiliki kewajiban untuk melindungi harkat dan martabat manusia. Demikian pula dalam hal perlindungan warga negara dari tindakan terorisme. Salah satu bentuk perlindungan negara terhadap warganya dari tindakan atau aksi terorisme adalah

---

[6] "Bom Bali Rencananya untuk Peringati Setahun Bom WTC", <http://www.kompas.com/kompas-cetak/0308/22/nasional/505322.htm>, diakses 7 Februari 2007.

melalui penegakan hukum, termasuk di dalamnya upaya menciptakan produk hukum yang sesuai.

Upaya ini diwujudkan pemerintah dengan mengeluarkan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002, yang kemudian disetujui oleh DPR menjadi Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme. Diperlukannya undang-undang ini karena pemerintah menyadari tindak pidana terorisme merupakan suatu tindak pidana yang luar biasa (*extraordinary crime*), sehingga membutuhkan penanganan yang luar biasa juga (*extraordinary measures*).[7] Undang-undang Nomor 15 Tahun 2003 ini selain mengatur aspek materil juga mengatur aspek formil. Sehingga, undang-undang ini merupakan undang-undang khusus (*lex specialis*) dari Kitab Undang-undang Hukum Pidana dan Kitab Undang-undang Hukum Acara Pidana. Dengan adanya undang-undang ini diharapkan penyelesaian perkara pidana yang terkait dengan terorisme dari aspek materil maupun formil dapat segera dilakukan.

---

[7] T. Nasrullah, *Sepintas Tinjauan Yuridis Baik Aspek Hukum Materil Maupun Formil Terhadap Undang-undang No. 15/2003 Tentang Pemberantasan Tindak Pidana Terorisme,* Makalah Pada Semiloka tentang "Keamanan Negara" yang diadakan oleh Indonesia Police Watch bersama Polda Metropolitan Jakarta Raya, Selasa 29 Maret, hal. 3.

Pada sebuah proses penyelesaian perkara pidana, proses pembuktian merupakan suatu proses pencarian kebenaran materiil atas suatu peristiwa pidana. Hal ini berbeda jika dibandingkan proses penyelesaian perkara perdata yang merupakan proses pencarian kebenaran formil. Proses pembuktian sendiri merupakan bagian terpenting dari keseluruhan proses pemeriksaan persidangan.

Hukum acara pidana di dalam bidang pembuktian mengenal adanya Alat Bukti dan Barang Bukti, di mana keduanya dipergunakan di dalam persidangan untuk membuktikan tindak pidana yang didakwakan terhadap terdakwa. Alat bukti yang sah untuk diajukan di depan persidangan, seperti yang diatur Pasal 184 Undang-undang Nomor 8 tahun 1981 Tentang *Hukum Acara Pidana* (KUHAP)[8] adalah:

a. keterangan saksi
b. keterangan ahli
c. surat
d. petunjuk
e. keterangan terdakwa

[8] Indonesia, *Undang-Undang Tentang Hukum Acara Pidana (KUHAP)*, UU No. 8, LN. No. 76 Tahun 1981, TLN. 3209, ps 184. (b)

Pada perkembangannya, alat bukti sebagaimana yang diatur dalam KUHAP tidak lagi dapat mengakomodir perkembangan teknologi informasi, hal ini menimbulkan permasalahan baru. Salah satu masalah yang muncul akibat perkembangan teknologi informasi adalah lahirnya suatu bentuk kejahatan baru yang sering disebut dengan *cybercrime,* dalam istilah yang digunakan oleh Barda Nawawi Arief disebut dengan tindak pidana mayantara.[9] Secara garis besar *cybercrime* terdiri dari dua jenis, yaitu kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas dan kejahatan yang menjadikan sistem dan fasilitas TI sebagai sasaran.[10]

Perkembangan teknologi dan perkembangan hukum telah menyebabkan tergesernya bentuk media cetak menjadi bentuk media digital (*paper less*). Perlu diperhatikan dalam kejahatan dengan menggunakan komputer, bukti yang akan mengarahkan suatu peristiwa pidana adalah berupa data elektronik, baik yang berada di dalam komputer itu sendiri

---

[9] Abdul Wahid, dan Muhammad Labib, *Kejahatan Mayantara (Cybercrime),* (Bandung: PT. Rafika Aditama 2005), hal. 26.

[10] Arif Pitoyo, ”Perlunya Penyempurnaan Hukum Pidana Tangani Cybercrime”,<http://gerbang.jabar.go.id/gerbang/index.php?index=16&idberita=680>, diakses 22 Januari 2007.

(*hardisk/floppy disc*) atau yang merupakan hasil *print out*, atau dalam bentuk lain berupa jejak (*path*) dari suatu aktivitas pengguna komputer.[11]

Tentu saja upaya penegakan hukum tidak boleh terhenti dengan ketidakadaan hukum yang mengatur penggunaan barang bukti maupun alat bukti berupa informasi elektronik di dalam penyelesaian suatu peristiwa hukum. Selain itu, proses mengajukan dan proses pembuktian alat bukti yang berupa data digital perlu pembahasan tersendiri mengingat alat bukti dalam bentuk informasi elektronik ini serta berkas acara pemeriksaan telah melalui proses digitalisasi dengan proses pengetikan (*typing*), pemeriksaan (*editing*), dan penyimpanan (*storing*) dengan menggunakan komputer. Namun, hasilnya tetap saja dicetak di atas kertas (*printing process*). Dengan demikian, diperlukan kejelasan bagaimana mengajukan dan melakukan proses pembuktian terhadap alat bukti yang berupa data digital.

Proses pembuktian suatu alat bukti yang berupa data digital ini juga menyangkut aspek validasi data digital yang dijadikan alat bukti tersebut. Aspek lain terkait

---

[11] Edmom Makarim, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian* (Jakarta: PT RajaGrafindo Persada, 2005) hal. 455.

adalah masalah menghadirkan alat bukti tersebut, apakah dihadirkan cukup dengan perangkat lunaknya (*software*) ataukah harus dengan perangkat kerasnya (*hardware*).

Sebagaimana telah dijelaskan terlebih dahulu, bukti digital tidak dikenal dalam Hukum Acara Pidana Umum (KUHAP). Namun, untuk beberapa perbuatan hukum tertentu, bukti digital dikenal dan pengaturannya tersebar pada beberapa peraturan perundang-undangan seperti Undang-undang Tentang Dokumen Perusahaan, Undang-undang Tentang Tindak Pidana Pencucian Uang, Undang-undang Tentang Kearsipan, Undang-undang Tentang Tindak Pidana Korupsi, dan Undang-undang tentang Pemberantasan Tindak Pidana Terorisme yang menjadi fokus penulisan ini.

Sebagai *lex specialis*, Undang-undang Nomor 15 Tahun 2003 memiliki kekhususan secara formil dibandingkan KUHAP. Salah satu kekhususan tersebut yang menjadi fokus dalam penulisan ini adalah terkait penggunaan alat bukti yang merupakan pembaharuan proses pembuktian konvensional dalam KUHAP. Pengaturan mengenai alat bukti pada Undang-undang Nomor 15 Tahun 2003 tersebut terlihat dalam Pasal 27, yaitu sebagai berikut.

Alat bukti pemeriksaan tindak pidana terorisme meliputi:

1. alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana;
2. alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan
3. data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada :
   1) tulisan, suara, atau gambar;
   2) peta, rancangan, foto, atau sejenisnya;
   3) huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.[12]

Alat bukti yang diatur dalam Pasal 27 ayat (2) dan (3) Undang-undang Nomor 15 Tahun 2003 tersebut berdasarkan KUHAP tidak diakui sebagai alat bukti, tetapi berdasarkan doktrin (ilmu hukum) dikategorikan sebagai Barang Bukti yang berfungsi sebagai data penunjang bagi alat bukti.[13] Akan tetapi dengan adanya Undang-undang Nomor 15 Tahun 2003 ini, kedua alat bukti tersebut dapat digunakan sebagai alat bukti yang sah dan mengikat serta memiliki kekuatan pembuktian sama dengan alat bukti yang diatur dalam KUHAP.

---

[12] Indonesia (a), *op. cit.*, ps. 27.

[13] Nasrullah, *op. cit*., hal. 16.

Meskipun demikian, prinsip *lex specialis derogat legi generalis* tetap berlaku. Dengan penafsiran secara *a contrario*, dapat diartikan hal yang tidak diatur dalam ketentuan khusus, dalam hal ini Undang-undang Nomor 15 Tahun 2003, berlakulah ketentuan umum, dalam hal ini KUHAP.

Penelitian ini bertolak dari permasalahan penggunaan bukti digital (*digital evidence*) sebagai alat bukti tindak pidana terorisme di Indonesia. Objek dari penelitian ini adalah *Source Code* atau Kode Sumber sebuah website yang merupakan media informasi teroris, yaitu website Al-Anshar dengan alamat di http://www.anshar.net. Dipilihnya kode sumber sebagai objek penelitian dikarenakan kode sumber adalah tampilan yang paling orisinal dari sebuah website. Segala tampilan yang ramah pengguna atau *user friendly interface* dari sebuah website dibangun dari baris kalimat pada kode sumber website tersebut. Sehingga apabila tampilan dari suatu website mengandung substansi yang merupakan upaya terorisme, maka harus dilihat dari kode sumber website tersebut. Selain itu, dari website tersebut kode sumber lah yang paling mungkin dijadikan alat bukti.

Situs www.anshar.net yang diduga dibuat oleh Agung Setyadi, dosen salah satu perguruan tinggi di Semarang, dan

M. Agung Prabowo Max Fiderman alias Kalingga alias Maxhaser, mahasiswa salah satu universitas di kota itu, dipakai untuk menyampaikan informasi terorisme atas pesanan Noordin M. Top sebagai media informasi perjuangannya.[14]

Isi dari informasi para teroris itu seputar materi-materi Tauziah Syaikh Mukhlas, Tauhid, Jihad, Wacana, Islamiah dan Askariah. Antara lain mengajarkan penyerangan dengan cara memanfaatkan antrean di jalan atau pintu masuk masuk atau keluar kantor, pusat perbelanjaan, hiburan, olahraga, hotel dan tempat pameran. Sejumlah lokasi, seperti Ancol, Planet Hollywood dan Jakarta Hilton Convention Center (JHCC) serta Senayan Golf Driving Range.[15]

Kasus tersebut saat ini tengah dalam proses persidangan di Pengadilan Negeri Semarang dengan Nomor Perkara 84/PID/B/2007 PN SMG. Hingga saat penelitian ini disusun, kasus tersebut telah mencapai tahap pembelaan (*pledoi*).

---

[14] "Pengacara TPM Dampingi Tersangka Pembuat Laman www.anshar.net", <http://www.antara.co.id/news>, diakses 1 November 2006.

[15] "Lewat Internet, Imam Samudera Rancang Pemboman," http://www.e-biskom.com, diakses 1 November 2006.

Untuk selanjutnya, pembahasan penelitian ini akan menjelaskan bagaimana kode sumber dari sebuah website dapat dijadikan alat bukti. Penjelasan tersebut akan dikaitkan dengan peraturan perundang-undangan di Indonesia yang memungkinkan penggunaan alat bukti digital dalam persidangan, khususnya Undang-undang Tentang Pemberantasan Tindak Pidana Terorisme. Selain itu dari penelitian ini akan terlihat sikap aparat penegak hukum, khususnya hakim dalam mempergunakan alat bukti yang ada.

B. Pokok Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, dapat diambil tiga pokok masalah, yaitu:

1. Bagaimana pengaturan penggunaan alat bukti berupa informasi elektronik dalam Hukum Acara Pidana di Indonesia?
2. Dapatkah sebuah kode sumber website dijadikan alat bukti di persidangan berdasarkan Pasal 27 Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme?

3. Bagaimana dalam prakteknya penerapan ketentuan Hukum Acara Pidana Terhadap Informasi Elektronik (*Source Code Website*) di dalam Peristiwa Tindak Pidana Terorisme pada Kasus Website Anshar.net?

C. Tujuan Penelitian

Tujuan penulisan ini dibagi menjadi dua, yaitu tujuan penulisan secara umum dan tujuan penulisan secara khusus, adapun tujuannya sebagai berikut.

1. Tujuan Umum

Tujuan umum penelitian ini adalah memberikan gambaran penggunaan informasi elektronik sebagai alat bukti dalam acara pembuktian pada Hukum Acara Pidana di Indonesia. Hal ini untuk mengakomodir semakin canggihnya tindak pidana yang menggunakan teknologi informasi, seperti cyberterrorism.

2. Tujuan Khusus

Tujuan khusus penelitian ini adalah sebagai berikut.

a. Mengetahui pengaturan penggunaan bukti digital dalam peraturan perundang-undangan di Indonesia, khususnya undang-undang terkait hukum pidana.
b. Mengetahui bagaimana sebuah kode sumber dijadikan alat bukti dalam tindak pidana terorisme berdasarkan Pasal 27 Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme.
c. Mengetahui penerapan bukti digital di dalam praktek persidangan terkait kasus website www.anshar.net.

D. Definisi Operasional

Dalam penulisan penelitian Kode Sumber (*Source Code*) Website Sebagai Alat Bukti di dalam Tindak Pidana Terorisme di Indonesia (Studi Kasus terhadap Website Al-Anshar.net) ini akan banyak digunakan istilah dalam bidang hukum dan bidang komputer. Untuk menghindari kesimpangsiuran pengertian mengenai istilah yang dipakai dalam penulisan

ini, berikut dijelaskan definisi operasional dari istilah tersebut:

Kode Sumber (Source Code) adalah:

> *The nonmachine language used by a computer programmer to create a program.*[16] *Source code (commonly just source or code) is any series of statements written in some human-readable computer programming language.*[17]

Terjemahan bebasnya adalah: Bahasa non-mesin yang digunakan oleh programer untuk menyusun suatu program. Kode sumber adalah serangkaian pernyataan yang ditulis dalam bahasa program yang dipahami manusia.

Website adalah:

> A website (or Web site) is a collection of web pages. A web page is a document, typically written in HTML, that is almost always accessible via HTTP, a protocol

---

[16] Bryan A. Graner, *Black's Law Dictionary Eighth Edition* (St. Paul: West Thomson, 2004).

[17] Wikipedia Online Encyclopedia, "Definiton of Source Code," <http://en.wikipedia.org/wiki/Source_code>, diakses 23 Desember 2006.

that transfers information from the website's server to display in the user's web browser.[18]

Terjemahan bebasnya adalah. Website (atau Web Site) sebuah kumpulan dari halaman web. Halaman web adalah sebuah dokumen yang biasanya ditulis dalam *Hyper Text Markup Language* (HTML) yang dapat diakses melalui protokol *Hyper Text Transfer Protocol* (HTTP) yang merupakan protokol untuk menyampaikan informasi dari sebuah pusat website untuk ditampilkan dihadapan pengguna program pembaca website.

Terorisme adalah: *The use or threat of violance to intimidate or cause panic, esp. as a means of affecting political conduct.*[19] Terjemahan bebasnya adalah, penggunaan atau upaya kekerasan untuk mengintimidasi atau menyebabkan kepanikan, khususnya dengan membawa dampak politik.

---

[18] Retrieved from <http://en.wikipedia.org/wiki/Website>, diakses 23 Desember 2006.

[19] Graner, *op. cit*.

Tindak Pidana Terorisme adalah, segala perbuatan yang memenuhi unsur-unsur tindak pidana sesuai dengan ketentuan dalam Peraturan Pemerintah Pengganti Undang-undang ini.[20]

Bukti Digital adalah:

> bukti yang di dapat dari kejahatan yang menggunakan komputer untuk mengarahkan suatu peristiwa pidana berupa data-data elektronik baik yang berada di dalam komputer itu sendiri (*hard disk/floopy disk*) atau yang merupakan hasil *print out,* atau dalam bentuk lain berupa jejak (*path*) dari suatu aktivitas penggunaan komputer.[21]

Informasi Elektronik adalah:

> Informasi elektronik adalah satu atau sekumpulan data elektronik diantaranya meliputi teks, simbol, gambar, tanda-tanda, isyarat, tulisan, suara, bunyi, dan bentuk-bentuk lainnya yang telah diolah sehingga mempunyai arti.[22]

Alat bukti adalah alat bukti yang terdapat dalam Pasal 184 ayat (1) KUHAP yaitu keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa.[23]

---

[20] Indonesia (a), *op. cit.,* ps. 1 ayat (1).

[21] Edmom Makarim, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian* (Jakarta: PT RajaGrafindo Persada, 2005), hal. 455.

[22] Indonesia (c), *Rancangan Undang-undang Tentang Informasi dan Transaksi Elektronik*, ps. 1 angka 3.

[23] Indonesia (b), *op. cit*., ps. 184 ayat (1).

Pembuktian adalah:

> ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang tata cara yang dibenarkan undang-undang untuk membuktikan kesalahan yang didakwakan kepada terdakwa.[24]

Hukum Pidana adalah:

> keseluruhan dari peraturan-peraturan yang menentukan perbuatan-perbuatan apa yang dilarang dan barangsiapa yang melanggar peraturan-peraturan itu diancam dengan suatu sanksi berupa pidana.[25]

E. Metode Penelitian

Penelitian merupakan penelitian yang berdasarkan studi kepustakaan yang bersifat yuridis-normatif, artinya penelitian hanya dilakukan dengan cara meneliti bahan pustaka atau data sekunder yang bersifat hukum.[26] Oleh

---

[24] M. Yahya Harahap, *Pembahasan Permasalahan dan Penerapan Kitab Undang-undang Hukum Acara Pidana (KUHAP) Jilid II*. Jakarta: Pustaka Kartini, 1988., *op. cit.*, hal. 793.

[25] Andi Hamzah, *Hukum Acara Pidana Indonesia Edisi Revisi* (Jakarta: Sinar Grafika, 2001), hal. 53

[26] Sri Mamudji *et al*. *Metode Penelitian dan Penulisan Hukum*, (Jakarta: Badan Penerbit Fakultas Hukum Universitas Indonesia, 2005), hal. 4-5.

karena itu, data yang digunakan adalah data sekunder yang didapatkan melalui studi dokumen.

Berkaitan dengan data yang digunakan, bahan hukum yang digunakan dalam penelitian ini meliputi bahan hukum primer, sekunder, dan tersier. Bahan hukum primer yang digunakan, peraturan perundang-undangan seperti Kitab Undang-undang Hukum Acara Pidana, dan Undang-undang Pemberantasan Tindak Pidana Terorisme. Selanjutnya, bahan hukum sekunder yang merupakan bahan hukum yang paling banyak digunakan dalam penelitian ini, meliputi buku, artikel ilmiah, jurnal *online* dari Pusat Data *West Law*, dan makalah terkait. Bahan hukum tersier yang digunakan antara lain kamus Hukum *Black's Law Dictionary* dan ensiklopedia online, antara lain *wikipedia* dan *Encarta*.

Tipologi penelitian yang digunakan dalam pembuatan laporan penelitian ini adalah penelitian berfokus masalah, yaitu suatu penelitian yang mengaitkan penelitian murni dengan penelitian terapan.[27] Dalam penelitian ini dijelaskan mengenai dasar teori pembuktian dan teori alat bukti sebagai ilmu murni dari hukum acara pidana dikaitkan

---

[27] *Ibid.*

dengan penerapan alat bukti berupa informasi elektronik dalam proses beracaranya. Penelitian ini juga merupakan penelitian yang dilakukan secara mono-disipliner, artinya laporan penelitian ini hanya didasarkan pada satu disiplin ilmu, yaitu ilmu hukum. Selanjutnya, metode analisis data yang digunakan adalah metode kualitatif.

F. Sistematika Penulisan

Penelitian hukum ini terdiri dari lima bab. Pada bab pertama akan dijabarkan mengenai latar belakang dilakukannya penelitian, tiga pokok permasalahan dari penelitian, tujuan dari penelitian ini baik tujuan umum maupun tujuan khusus, kemudian dijelaskan pula mengenai kerangka konsepsional yang berisi definisi operasional dari istilah dalam penelitian ini, serta metode penelitian.

Pada bab kedua dari penelitian ini akan dijabarkan mengenai pengertian tindak pidana terorsime yang meliputi pembahasan mengenai unsur tindak pidana dan subjek dalam tindak pidana, kemudian membahas bagaimana penerapan perumusan unsur tindak pidana dan subjek pidana dalam Undang-undang Nomor 15 Tahun 2003. Untuk memperkaya pembahasan, dalam bab ini juga akan dibahas bagaimana

pengaturan dan perumusan tindak pidana terorisme dibeberapa negara, antara lain di Australia dan Amerika Serikat. Pembahasan selanjutnya mengenai terorisme pada perkembangannya; mencakup pembahasan mengenai *cyberterrorism* serta terorisme berbasis teknologi informasi.

Sub bab terakhir dari bab dua ini adalah pembahasan hukum acara dalam Undang-undang Nomor 15 Tahun 2003, yang meliputi pembahasan Proses Penyelidikan, Penyidikan, dan Upaya Paksa Penangkapan, Penahanan, Penggeledahan, dan Penyitaan dalam Tindak Pidana Terorisme. Dalam sub-bab ini juga dibahas mengenai beban pembuktian, sistem pembuktian, dan alat bukti yang digunakan dalam Undang-undang Nomor 15 Tahun 2003.

Bab tiga penelitian ini memiliki fokus pada pembahasan teknis, yaitu pembahasan mengenai kode sumber, yang meliputi pembahasan mengenai macam bahasa pemerograman pada pembuatan website, pembahasan mengenai media penyimpanan (*storage*) sebuah website pada perusahaan webhosting (*webhosting compay*). Dalam bab ini juga akan dijabarkan mengenai bukti digital, yang akan menjelaskan definisi dari bukti digital, serta bagaimana cara melakukan otentifikasi

terhadap bukti digital. Selanjutnya, pembahasan terakhir pada bab tiga adalah mengenai kode sumber yang dijadikan bukti digital.

Bab empat berisi analisis mengenai alat bukti dalam tindak pidana terorisme terhadap penggunaan kode sumber sebagai alat bukti berupa informasi elektronik dalam kasus website alanshar.net. Pada bab ini akan dilihat bagaimana penerapan kode sumber sebagai alat bukti berupa informasi elektronik dalam tindak pidana terorisme dikuatkan oleh keterangan ahli, sebagai alat bukti, dan keterangan saksi dalam kaitan dengan alat bukti berupa informasi elektronik.

Bab lima merupakan bab terakhir dalam penulisan ini. Bab lima merupakan penutup penulisan yang berisi simpulan dari keseluruhan penelitian ini. Selain berisi simpulan, bab lima juga berisi saran yang diberikan oleh penulis terkait penyelesaian perakara pidana terorisme, khususnya terorisme yang melibatkan aspek Informasi Teknologi.

BAB II

TINJAUAN UMUM TINDAK PIDANA TERORISME BAIK DARI SEGI MATERIL MAUPUN SEGI FORMIL

A. Terorisme: Pengertian, Karakteristik dan Organisasi

Sebuah asas hukum menyatakan *nullum crimen sine poena*, yang artinya adalah tiada kejahatan yang boleh dibiarkan begitu saja tanpa hukuman.[28] Demikian pula dengan kejahatan terorisme yang harus dibuatkan suatu instrumen hukumnya. Saat ini, terorisme telah menjadi suatu kejahatan lintas negara, terorganisir, dan bahkan merupakan tindak pidana internasional yang mempunyai jaringan luas, yang mengancam perdamaian dan keamanan nasional maupun internasional.

Terorisme telah lama dianggap sebagai kejahatan bertaraf internasional, tetapi hingga saat ini tidak ada

[28] Granner, *op. cit.*

definisi mengenai terorisme yang dapat diterima secara universal. Kesulitan memberikan suatu definisi terhadap terorisme terkait dengan sensitifitas isu terkait terorisme ditambah juga banyaknya pihak yang berkepentingan (*stakeholder*) terhadap isu terorisme, baik itu orang perorang, organisasi, bahkan suatu negara.[29]

1. Pengertian Terorisme

Banyaknya pihak yang berkepentingan dalam isu terorisme terutama terkait dengan politik, telah melahirkan berbagai opini yang berpengaruh terhadap definisi terorisme, salah satunya opini Peter Rösler-Garcia, seorang ahli politik dan ekonomi luar negeri dari Hamburg, Jerman yang menyatakan tidak ada suatu negara di dunia ini yang secara konsekuen melawan terorisme.[30]

Sebagai contoh, Amerika Serikat sebagai negara yang paling gencar mempropagandakan isu “Perang Global Melawan

---

[29] Wahid, *op. cit.*, hal. 22.

[30] Peter Rösler-Garcia, ”Terorisme, Anak Kandung Ekstremisme”, <http://www.kompas.com/kompas-cetak/0210/15/opini/tero30.htm>, diakses 20 Februari 2007.

Terorisme”, membiayai kelompok teroris "IRA" di Irlandia Utara atau gerakan bersenjata "Unita" di Angola.[31] Selanjutnya, politikus Uni Eropa mendukung bermacam kelompok teroris di Afrika, Asia, Amerika Latin-termasuk gerakan teroris di Uni Eropa sendiri, sebagai "ETA" dari Spanyol. Ada juga pemerintah negara atau pemerintahan kotapraja Uni Eropa yang secara resmi melindungi kewakilan kelompok ekstremis itu di wilayah mereka, dan yang lain menerima kegiatan kelompok itu secara diam.[32]

Banyaknya kepentingan berlatar belakang politik, menyebabkan pemahaman mengenai pengertian terorisme juga terbias akibat perbedaan sudut pandang. Perbedaan sudut pandang ini terlihat dalam kasus invasi Amerika Serikat ke Irak pada 2003. Amerika Serikat melegitimasi tindakannya menginvasi Irak karena menganggap Irak sebagai teroris sebab Irak memiliki senjata pemusnah masal, namun disisi lain, banyak negara yang menyatakan Amerika sendiri lah yang merupakan negara teroris (*state terrorist*), karena

---

[31] Adjie Suradji, *Terorisme* (Jakarta: Pustaka Sinar Harapan, 2005), hal. 249.

[32] Rösler-Garcia, *loc. cit.*

telah melakukan invasi ke negara berdaulat tanpa persetujuan dari dewan keamanan PBB.[33]

Terlepas dari banyaknya pengaruh kepentingan politik dalam pendefinisian terorisme, ada hal lain yang mempengaruhi sulitnya memberikan definisi yang objektif. Kesulitannya terletak dalam menentukan secara kualitatif bagaimana suatu peristiwa dapat dikategorikan sebagai terorisme. Teror -yang merupakan kata dasar dari terorisme- bersifat sangat subjektif. Artinya, setiap orang memiliki batas ambang ketakutannya sendiri, dan secara subjektif menentukan apakah suatu peristiwa merupakan teror atau hanya peristiwa biasa.[34] Akibatnya, suatu perisitwa teror bagi seseorang belum tentu merupakan teror bagi orang lain. Jason Burke dalam bukunya *Al-Qaeda: The True Story of Radical Islam*, juga menyatakan sebagai berikut.

> *There are multiple ways of defining terrorism, and all are subjective. Most define terrorism as 'the use or threat of serious violence' to advance some kind of 'cause'. Some state clearly the kinds of group ('sub-*

---

[33] Wahid, *op. cit.*, hal. 23.

[34] Paul Wilkinson, *Terrorism and the Liberal State* (London: The Macmillan Press Ltd., 1977), sebagaimana dikutip oleh F. Budi Hardiman dalam F. Budi Hardiman dkk., *Terorisme, Definisi, Aksi dan Regulasi* (Jakarta: Imparsial, 2005), hal. 5.

> *national', 'non-state') or cause (political, ideological, religious) to which they refer.*[35]

Telah dijelaskan sebelumnya, hingga saat ini tidak ada definisi mengenai terorisme yang digunakan secara universial. Akan tetapi guna memperoleh pemahaman terhadap terorisme yang konsisten dalam penulisan, tetaplah perlu adanya suatu definisi. Agar mendapatkan suatu definisi tentang terorisme, perlu dikaji berbagai definisi mengenai terorisme.

Definisi pertama diberikan oleh *Encyclopedia of Britanica* sebagai berikut.

> *Terrorism is the systematic use of violence to create a general climate of fear in a population and thereby to bring about a particular political objective*.[36]

Terlihat dari definisi tersebut, terorisme masih erat kaitannya dengan kondisi kekerasan dalam hubungan politik. Selanjutnya definisi terorisme oleh *United State*

---

[35] Jason Burke, *Al-Qaeda: The True Story of Radical Islam* (London: TB. Tauris & Co. Ltd), ch. 2, p. 22.

[36] The Britanica On-line Encyclopedia, <http://www.britannica.com/eb/article-9071797/terrorism>, diakses 21 Februari 2007.

Departement of Defense (Departemen Pertahanan Amerika Serikat) yang menjelaskan:

> *Calculated use of unlawful violence to inculcate fear; intended to coerce or intimidate governments or societies in pursuit of goals that are generally political, religious, or ideological*.

Definisi yang diberikan Departemen Pertahanan Amerika Serikat meskipun masih menekankan tindakan terorisme pada motifnya, cakupan motif terorisme dalam definisi ini lebih luas yaitu tidak hanya aspek politik tetapi juga termasuk aspek keagamaan dan ideologi. Terkait penggunaan teror dalam kepentingan politik, maka teror menjadi salah satu bentuk apresiasi kepentingan politik yang paling serius untuk menekan lawan politik dengan memanfaatkan kelemahan negara menjalankan fungsi kontrolnya.[37] Kondisi kevakuman kekuasaan (*vacum of power*) yang menjadi tujuan akhirnya.

Definisi berikutnya yang didapat dari Kamus hukum *Black's Law* yang juga mendefinisikan *terrorism* dalam kaitannya dengan politik yaitu "*The use or threat of violance to intimidate or cause panic, esp. as a means of*

---

[37] Kontras, *Analisis Kasus Peledakan Bom di Bali: Mengapa "Teror" Terjadi?*, dalam F. Budi Hardiman dkk., *Terorisme, Definisi, Aksi dan Regulasi* (Jakarta: Imparsial, 2005), hal. 38.

affecting political conduct,[38] akan tetapi jika merujuk pada definisi *terroristic threat* terlihat kalau pendefinisian terorisme dalam *Black's Law* yang mengacu pada *Model Penal Code § 211*, tidak hanya terpaku pada motif melainkan juga proses serta tujuan dari terorisme tersebut.[39] Hal ini terlihat dalam definisi berikut.

> *Terroristic threat is a threat to commit any crime of violence with the purpose of (1) terrorizing another, (2) causing serious public inconvenience, or (4) reclessly disregarding the risk of causing such terror or inconvenience.*[40]

Secara bebas, definisi tersebut dapat diartikan suatu ancaman teror untuk melakukan kejahatan dan kekerasan dengan tujuan meneror orang lain, menimbulkan ketidaknyamanan atau gangguan terhadap publik, dengan mengabaikan akibat yang timbul dari teror tersebut. Dilihat dari tujuannya yaitu menimbulkan gangguan terhadap publik, terdapat kesamaan antara kejahatan biasa, peperangan, dan terorisme, tetapi sesungguhnya terdapat parameter perbedaan

---

[38] Graner, *op. cit.*

[39] American Law Institute, *Model Penal Code*, <http://myweb.wvnet.edu/~jelkins/crimlaw/basic/mpc.html>.

[40] *Ibid.*

antara terorisme, peperangan (*war*) dan nuansa kriminal biasa (*ordinary crime*).

William G. Cunningham, menggambarkan paramenter yang berbeda dari terorisme, peperangan, dan kejahantan biasa dalam sebuah tabel sebagai berikut.[41]

Primary Independent Variable	***Terrorism's Relationship to Variable***	***Secondary Independent Variables***	***Types of Activities / Contrast to Terrorism***
Crime	*Crime is viewed as economically motivated rather than politically motivated.*	*Organized Crime*	*Terrorizing victims for money or revenge*
		Individual Crime	*Murder for personal motive*
War	*War is usually perceived as more legitimate and purposeful than terrorism. It is instrumental and not symbolic violence. There are rules and laws of war to be followed by belligerents. Civilians and non-combatants should not be targeted.*	*Just War*	*Self defense. Used against tyranny or an aggressor*
		Legal War (declared inter-state)	*Terrorism is not undeclared war*
		War Crimes	*Terror and illegal acts committed during war by legal combatants*
		Civil War	*Intra-state between recognized belligerents*
		Guerilla War	*Guerilla's hold territory, fight combatants not civilians, wear uniforms, openly carry weapons*
		Insurgency / Low Intensity War	*Targets governmental control and power – may illegally target non-combatants*
Terrorism	*Terrorism is form of political violence. It is politically motivated to induce change by producing fear. It is illegal and not recognized as a legitimate form of political violence.*	*Revolution*	*Mass overthrow of system*
		Riots – Mass Violence	*Temporary, spontaneous*
		Assassination	*Target is single focus / act*
		State Repression	*Pervasive state terrorism*
		Terrorism	*Equivalent of War Crimes by illegal non-combatants*

Tabel 1. Perbandingan Parameter Terorisme, Peperangan, dan Kejahatan biasa

[41] William G. Cunningham *et. al.*, *Terrorism: Concepts, Causes, and Conflict Resolution* (Virginia: Defense Threat Reduction Agency Fort Belvoir, January 2003), p. 7.

Berdasarkan tabel 1 tersebut terlihat jelas paramentar yang berbeda antara terorisme, peperangan, dan kejahatan. Sebuah kejahatan biasa terutama memiliki motif ekonomi, yang bentuknya dapat berupa teror untuk mendapatkan harta orang lain, atau dapat berupa pembunuhan dengan alasan balas dendam atau untuk mempertahankan harta yang telah dirampas.

Dalam hal peperangan, terdapat motif serta tujuan yang lebih bersifat instrumental. Dalam peperangan juga ada banyak aturan, salah satunya tidak boleh menyerang rakyat yang tidak bersenjata (*non-combantans*). Selain itu, para pihak yang berperang merupakan suatu instansi resmi dimasing-masing pihak.[42] Sedangkan dalam terorisme hampir tidak ada aturan dan penyerangan dilakukan secara membabi buta. Dari keterangan tabel 1 tersebut terlihat kecocokan karakteristik terorisme yang diuraikan oleh William G. Cunningham dengan definisi *terorristic threat* dalam *Model Law* § 211.

[42] *Ibid.*, p. 8.

Para ahli selain memberikan definisi tentang pengertian terorisme juga memberikan kategorisasi tindakan terorisme untuk mempermudah pemahaman terhadap pengertian terorisme. Seorang ahli bernama Jack Gibbs menyatakan, suatu tindakan dapat didefinisikan sebagai terorisme apabila merupakan suatu kejahatan atau suatu ancaman secara langsung terhadap kemanusiaan atau terhadap objek tertentu.[43] Namun, hal tersebut menurut Gibbs masih merupakan definisi yang umum, artinya cakupan dari definisi tersebut masih terlalu luas dan masih mencakup juga definisi dari kejahatan biasa.[44]

Untuk mempermudah pemahaman terhadap definisi terorisme, Gibbs menambahkan beberapa ciri perbuatan yang merupakan terorisme dengan merujuk pada:

1. perbuatan yang dilaksanakan atau ditujukan dengan maksud untuk mengubah atau mempertahankan paling sedikit suatu norma dalam suatu wilayah atau suatu populasi;

---

[43] Jack Gibbs, “Definition of Terrorism”, <http://en.wikipedia.org/wiki/Definition_of_terrorism>, diakses 25 Februari 2007.

[44] Dengan pengertian tersebut, definisi itu mencakup kejahatan biasa seperti pembunuhan atau perusakan gedung, sehingga tidak terlihat perbedaan antara kejahatan biasa (*ordinary crime*) dengan terorisme.

2. memiliki kerahasiaan, tersembunyi tentang keberadaan para partisipan, identitas anggota, dan tempat persembunyian;
3. tidak bersifat menetap pada suatu area tertentu;
4. bukan merupakan tindakan peperangan biasa karena mereka menyembunyikan identitas mereka, lokasi penyerangan, berikut ancaman dan pergerakan mereka; serta
5. adanya partispan yang memiliki pemikiran atau ideologi yang sejalan sejalan dengan konseptor teror, dan pemberian kontribusi untuk memperjuangkan norma yang dianggap benar oleh kelompok tersebut tanpa memperhitungkan kerusakan atau akibat yang ditimbulkan.[45]

Berdasarkan ciri tersebut, suatu peristiwa dapat dirumuskan menjadi suatu deskripsi tentang terorisme yang paling mendekati nilai objektifitas. Disamping hal tersebut, untuk itu terorisme perlu pula dipandang dari dua pendekatan, yaitu pendekatan secara spesifik dan pendekatan secara umum. Pendekatan spesifik mengklasifikasikan

[45] Gibbs, *op. cit.*

kejahatan biasa yang telah ada sebagai terorisme, contohnya adalah mengklasifikasikan sebuah pembajakan pesawat atau penyanderaan yang semula sebagai kejahatan biasa menjadi terorisme.[46] Pendekatan ini dibuat tanpa perlu mendefinisikan atau menguraikan secara umum tindakan terorisme *per se*.[47] Dengan kata lain, dalam definisi ini peristiwa umum dijadikan hal khusus, sehingga pendekatan ini sering juga disebut sebagai pendekatan induktif.[48]

Sementara itu, pendekatan secara umum berusaha memberikan penjelasan umum mengenai terorisme, berdasarkan suatu kriteria seperti intensi, motivasi dan tujuan. Pendekatan ini merupakan upaya penjabaran peristiwa khusus terorisme kedalam peristiwa umum (metode deduktif).

Dalam prakteknya, pendekatan ini bisa digunakan kedua-duanya, atau dikombinasikan. Dalam sub-bab selanjutnya akan dijelaskan dan diberikan contoh mengenai penggunaan pendekatan definisi terorisime dibeberapa negara, termasuk di Indonesia.

---

[46] Ben Golder and George Williams, "What is 'Terrorism'? Problems of Legal Definition," *UNSW Law Journal Vol. 27(2)* (February 2003): 286.

[47] *Black's Law Dictionary* mengartikan Per se: *Of, in, or by itself; standing alone, without reference to additional facts*.

[48] Golder, *op. cit.*

2. Karakteristik Organisasi Terorisme

Apabila upaya untuk memberikan defini terhadap terorisme merupakan hal yang sulit, maka upaya untuk mencari karakteristik, pola operasi, dan sitem organisasi terorisme memiliki tingkat kesulitan yang sama. Hal ini dipengaruhi sifat dan kegiatan terorisme yang selalu berubah dari masa ke masa.[49] Meskipun demikan, secara umum karakteristik dari organisasi terorisme, dapat dijabarkan sebagai berikut.[50]

(1) *Nonstate-suported group*. Organisasi teroris semacam ini merupakan organisasi terorisme yang paling sederhana. Organisasi ini tidak didukung oleh salah satu negara. Organisasi terorisme yang memiliki karakter *nonstate-supported group* ini adalah kelompok kecil yang memiliki kepentingan khusus, seperti kelompok antikorupsi, kelompok anti globalisasi, dan lainnya. Hanya saja dalam menjalankan aksi "anti"-nya, kelompok ini

[49] R. Scott Moore, *Characteristics of Terrorism*, refer to Cunningham, *op. cit.*, p. 40.

[50] Suradji, *op. cit.*, hal. 16.

menggunakan cara teror seperti pembakaran, penjarahan, dan penyanderaan. Terlihat dari isu terornya, organisasi ini merupakan organisasi teror yang menekankan pada aspek perjuangan ideologi dengan menciptakan kekacuan ideologi (*ideology disorder*) dalam tatanan masyarakat.[51] Kelompok organisasi teroris dalam kategori ini, memiliki kemampuan terbatas dan tidak dilengkapi dengan infrastruktur yang diperlukan untuk memberikan dukungan, atau kontribusi lain demi kelangsungan kelompoknya dalam periode waktu tertentu.[52]

(2) *State-sponsored groups*. Organisasi terorisme jenis ini memperoleh dukungan baik berupa dukungan logistik, pelatihan militer, maupun dukungan administratif dari negara asing. Berbeda dengan jenis yang pertama, kelompok ini bersifat profesional, artinya memiliki struktur organisasi yang jelas meskipun bersifat rahasia atau tertutup

---

[51] Ali Khan, "A Legal Theory of International Terrorism," *Connecticut Law Review* (1982):6.

[52] Suradji, *op. cit.*

(*clandestine*).[53] Selain itu cara yang digunakan dalam melakukan teror lebih terorganisir dan terencana. Contoh kelompok teroris yang termasuk dalam kategori ini antara lain, *Provisional Irish Republican Army* (PIRA) yang dibentuk pada 1970, dengan jumlah anggota dua ratus hingga empat ratus yang memiliki daerah operasi di Irlandia Utara. PIRA merupakan kelompok teroris yang bertanggung jawab atas pembunuhan Rev. Robert Bradford, anggota Parlemen Inggris di Belfast dan juga pada peristiwa peledakan bom dipintu belakang Royal Courts. Kelompok ini mendapatkan sponsor dari Libya berupa pasokan senjata, tempat pelatihan, dan logistik dalam menjalankan aksinya.[54] Contoh teraktual dari kelompok dalam kategori ini adalah kelompok teroris yang diberi nama Jamaah Islamiah yang diduga memiliki hubungan erat dengan kelompok Al-Qaeda dan bertanggung jawab atas peledakan bom di Bali

---

[53] Humphreys, Adrian. "One official's 'refugee' is another's 'terrorist'", *National Post* (January 2006).

[54] Suradji, *op. cit.*, hal. 158.

tanggal 12 Oktober 2002 yang menewaskan kurang lebih dua ratus orang.[55] [56]

(3) *State-directed groups.* Organisasi kelompok teroris ini berupa organisasi yang didukung langsung oleh suatu negara. Berbeda dengan *state-sponsored groups*, negara memberikan dukungannya secara terang-terangan, bahkan negara tersebut yang membentuk organisasi teroris tersebut, meskipun negara tersebut tidak pernah mengklaim organisasi bentukannya merupakan organisasi teror. Contoh dari organisasi ini adalah organisasi *special force* yang dibentuk Iran pada 1984, untuk tujuan penyebaran paham Islam fundamentalis di wilayah Teluk Persia dan Afrika Utara.[57]

---

[55] Sumber berasal dari <http://www.state.gov/s/ct/c14151.htm>, diakses pada Juni 2006.

[56] Keberadaan kelompok Jamaah Islamiyah ini sesunguhnya belum bisa dibuktikan secara tepat, terutama kaitan kelompok ini dengan kelompok teroris internasional, Al-Qaeda. Penggunaan nama Jamaah Islamiyah pada kelompok ini menuai kritik dari beberapa kalangan intelektual muslim, karena penggunaan istilah Jamaah Islamiyah pada kelompok tersebut berarti “Kumpulan Umat Islam”, yang berarti merujuk pada seluruh orang yang menganut agama Islam. Lebih lanjut, lihat <http://www.hidayatullah.com/index.php?option=com_content&task=view&id=2356&Itemid=0>

[57] Karl A Seger, *The Anti Terrorism Handbook* (London: Greenhill Books, 1991) p. 6 sebagaimana dikutip dalam Suradji, *op. cit.*, hal. 18.

B. Terorisme di Indonesia dalam Undang-undang Nomor 15 Tahun 2003 dan dalam Ketentuan Dibeberapa Negara Lainnya

Pasca peledakan gedung *World Trade Center* (WTC) di Amerika pada 11 September 2002, peristiwa terorisme telah membuka mata dunia Internasional betapa sebuah konstruksi hukum mutlak diperlukan untuk melakukan perlawanan terhadap aksi terorisme.[58] Yang terjadi di Indonesia pun hampir sama, ketika terjadi peristiwa Bom Bali I pada 12 Oktober 2002, Indonesia diingatkan akan adanya ancaman terhadap perdamaian dan keamanan didepan mata. Sebagai langkah proaktif dari peristiwa itu dan juga merupakan langkah preventif dari peristiwa dimasa mendatang, pemerintah mengeluarkan Peraturan Pemerintah Nomor 1 Tahun 2002 yang kemudian diundangkan menjadi Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme.

Dalam penjelasan Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme, dinyatakan terorisme yang bersifat internasional merupakan kejahatan yang terorganisasi, sehingga pemerintah dan bangsa

---

[58] Jeffrey Record, "Bounding The Global War On Terrorism," *Strategic Studies Institute* (December 2003): 2.

Indonesia wajib meningkatkan kewaspadaan dan bekerja sama memelihara keutuhan Negara Kesatuan Republik Indonesia. Terlihat dalam penjelasan tersebut, pemerintah Indonesia menyadari terorisme telah menjadi isu internasional dan juga terlihat negara lain seperti Australia dan Amerika Serikat begitu fokus dalam upaya memerangi terorisme.[59] Untuk itu perlu dikaji mengenai pengaturan dimasing-masing negara.

1. Terorisme di Indonesia dan Pengaturannya dalam Undang-undang Nomor 15 Tahun 2003

Pada konsiderans Undang-undang Nomor 15 Tahun 2003, bagian menimbang, dijelaskan terorisme telah menghilangkan nyawa tanpa memandang korban dan menimbulkan ketakutan masyarakat secara luas, atau hilangnya kemerdekaan, serta kerugian harta benda, oleh karena itu perlu dilaksanakan langkah pemberantasan. Namun, peraturan perundang-undangan yang berlaku sampai saat ini belum secara komprehensif dan memadai untuk memberantas tindak pidana terorisme, sehingga

[59] *Ibid.*

Undang-undang Nomor 15 Tahun 2003 ini mutlak diperlukan. Tujuan utama lahirnya undang-undang ini adalah menjadikan terorisme sebagai suatu tindak pidana di Indonesia. Agar kejahatan terorisme dapat dikategorikan sebagai tindak pidana, perlu diuraikan terlebih dahulu mengenai unsur tindak pidana dan subjeknya.

(1) Tindak Pidana

Undang-undang Nomor 1 Tahun 1946 Tentang Kitab Undang-undang Hukum Pidana (KUHP) merupakan produk hukum Indonesia yang isinya dibentuk oleh Pemerintahan Kolonial Belanda, sehingga KUHP yang ada saat ini tidak lain adalah hasil alih bahasa yang dilakukan beberapa sarjana Indonesia.[60]

Jika melihat judul Undang-undang Nomor 15 Tahun 2003, yaitu tentang Pemberantasan Tindak Pidana Terorisme, terdapat suatu istilah yang menunjukan, peristiwa terorisme merupakan kejahatan, yakni istilah “Tindak Pidana”. Istilah tersebut telah digunakan oleh masing-masing penerjemah atau

[60] *Kitab Undang Undang Hukum Pidana*, Prof.Moeljanto, S.H., cet. 21, (Jakarta: Bumi Aksara, 2001).

yang menggunakan dan telah memberikan sandaran perumusan dari istilah *strafbaar feit* tersebut.[61]

Istilah *"het strabare feit"* sendiri telah diterjemahkan kedalam bahasa Indonesia sebagai:

a. perbuatan yang dapat/boleh dihukum,

b. peristiwa pidana,

c. perbuatan pidana, dan

d. tindak pidana.

Lebih lanjut, pembentuk undang-undang kita telah menggunakan istilah *strafbaar feit* untuk menyebut tindak pidana.[62] Oleh karena itu, timbul pertanyaan, istilah manakah yang paling tepat? Untuk menjawabnya, perlu diuraikan beberapa pendapat ahli Hukum Pidana. Pendapat pertama diberkan oleh Simons yang merumuskan *een strafbaar feit* sebagai berikut.

> *strafbaar feit* adalah suatu *handeling* (tindakan/perbuatan) yang diancam dengan pidana oleh undang-undang, bertentangan dengan hukum

---

[61] S.R Sianturi, *Asas-asas Hukum Pidana di Indonesia dan Penerapannya* (Jakarta: Alumni Ahaem – Petehaem, 1989) hal. 204.

[62] P.A.F Lamintang, *Dasar-dasar Hukum Pidana Indonesia* (Bandung: Sinar Baru, 1990), hal. 172.

(*onrechtmatig*) dilakukan dengan kesalahan (*schuld*) oleh seorang yang mampu bertanggung jawab.[63]

Kemudian Profesor van Hattum berpendapat, *strafbaar feit* adalah tindakan yang karena telah melakukan tindakan semacam itu membuat seseorang menjadi dapat dihukum.[64] Kedua ahli tersebut merujuk penggunaan istilah tindak pidana dalam merumuskan *strafbaar feit*. Berbeda dengan kedua ahli tersebut, Prof. Moeljatno mengartikan *strafbaar feit* sebagai perbuatan yang dilarang dan diancam dengan pidana barangsiapa melanggar larangan tersebut. Dari uraian tersebut terlihat Prof. Moeljatno merujuk istilah "perbuatan pidana" untuk merumuskan *strafbaar feit*.[65]

Berdasarkan beberapa pendapat ahli tersebut, dapat dibuatkan suatu simpulan mengenai tindak pidana, yaitu sebagai berikut.

a. Suatu perbuatan yang melawan hukum.

b. Orang yang dikenai sanksi harus mempunyai kesalahan (asas tiada pidana tanpa kesalahan).

---

[63] Sianturi, *op. cit.*, hal. 205

[64] Lamintang, *op. cit.*, hal. 175

[65] Moeljatno, *Asas-Asas Hukum Pidana,* cet. 7, (Jakarta: PT. Rineka Cipta, 2002), hal. 54.

Kesalahan sendiri terdiri dari kesalahan yang disebabkan secara sengaja dan yang disebabkan karena kelalaian.

c. Subjek atau pelaku baru dapat dipidana jika ia dapat bertanggung jawab dalam artian berfikiran waras.

Jika ingin mengklasifikasikan terorisme sebagai tindak pidana, maka unsur tersebut harus melekat dalam tindakan terorisme. Unsur yang pertama yaitu melawan hukum. Unsur melawan hukum dapat memiliki dua pengertian, yang pertama dalam artian melawan hukum secara formal yaitu, melakukan sesuatu terbatas pada yang dilarang oleh undang-undang.[66] Sedangkan yang dimaksud dengan melawan hukum secara materil adalah melakukan sesuatu yang dilarang dalam perundang-undangan maupun berdasarkan asas hukum yang tidak tertulis.[67]

Pencantuman unsur melawan hukum dalam suatu tindak pidana berpengaruh pada proses pembuktian. Apabila dalam suatu Pasal secara nyata terdapat unsur melawan hukum, maka

---

[66] J. M. van Bemmelen, *Hukum Pidana I: Hukum Pidana Material Bagian Umum*. Diterjemahkan oleh Hasan (tanpa tempat: Bina Cipta, 1984), hal. 102-103.

[67] Lamintang, *op. cit.*, hal. 184-185.

Penuntut umum harus membuktikan unsur tersebut, jika unsur tersebut tidak terbukti maka putusannya *vrijspraak* atau putusan bebas. Sedangkan, jika unsur melawan hukum tidak secara tegas merupakan unsur dari suatu tindak pidana maka tidak terbuktinya unsur tersebut menyebabkan putusannya lepas dari segala tuntutan hukum.[68]

Unsur yang kedua, yaitu unsur kesalahan (*schuld*). Kesalahan dipersamakan artinya dengan kesengajaan (*opzet*) atau kehendak (*voornawen*). *Geen straf zonder schuld* (tiada hukuman tanpa kesalahan), ini berarti orang yang dihukum harus terbukti bersalah. Kesalahan mengadung dua pengertian. Dalam arti sempit yang berarti kesengajaan (*dolus/opzet*) yang berarti berbuat dengan hendak dan maksud (atau dengan menghendaki dan mengetahui: *willen en wetens*), sedangkan dalam arti luas berarti *dolus* dan *culpa*.[69] *Culpa* sendiri berarti kealpaan, dimana pada diri pelaku terdapat kekurangan pemikiran, kekurangan pengetahuan, dan

---

[68] *Ibid.*

[69] Jan Remmelink, *Hukum Pidana: Komentar atas Pasal-Pasal Terpenting dari Kitab Undang-undang Hukum Pidana Belanda dan Padanannya dalam Kitab Undang-undang Hukum Pidana Indonesia* (Jakarta: PT Gramedia Pustaka Umum, 2003), hal. 173.

kekurangan kebijaksanaan yang diperlukan.[70] Unsur yang ketiga yaitu pertanggungjawaban subjek. Sesuatu dapat dikatakan sebagai tindak pidana apabila ada subjek (pelaku) dari tindak pidana itu sendiri. Agar dapat dipidana, dalam diri subjek atau pelaku pidana tidak terdapat dasar penghapus pidana, baik dasar pembenar maupun dasar pemaaf.

(2) Subjek Tindak Pidana

Pada awalnya dalam hukum pidana, yang dianggap sebagai subjek tindak pidana hanyalah manusia sebagai *natuurlijke-persoonen*, sedangkan badan hukum atau *rechts-persoonen* tidak dianggap sebagai subjek.[71] Meskipun demikian, pada perkembangannya terjadi perluasan terhadap subjek tindak pidana.

Pembuat undang-undang dalam merumuskan delik sering memperhitungkan kenyataan manusia melakukan tindakan di dalam atau melalui organisasi yang, dalam hukum keperdataan maupun di luarnya, muncul sebagai satu kesatuan dan karena dari itu diakui serta mendapat perlakuan sebagai badan

---

[70] Sianturi, *op. cit.*, hal. 192.

[71] *Ibid.*, hal. 219.

hukum/korporasi.[72] Dengan demikian, dalam hukum pidana saat ini subjek hukumnya tidak lagi terbatas pada manusia sebagai pribadi kodrati (*natuurlijke-persoonen*) tetapi juga mencakup manusia sebagai badan hukum (*rechts-persoonen*).

Terkait dengan subjek tindak pidana perlu dijelaskan, pertanggungjawaban pidana bersifat pribadi. Artinya, barangsiapa melakukan tindak pidana, maka ia harus bertanggung jawab, sepanjang pada diri orang tersebut tidak ditemukan dasar penghapus pidana. Selanjutnya, dalam pidana dikenal juga adanya konsep penyertaan (*deelneming*). Konsep penyertaan ini berarti ada dua orang atau lebih mengambil bagian untuk mewujudkan atau melakukan tindak pidana. Menjadi persoalan, siapa dan bagaimana konsep pertanggung jawaban pidananya?[73]

Dalam hukum pidana ragam bentuk pernyertaan diatur dalam Pasal 55-56 KUHP. Dalam KUHP terdapat terdapat lima bentuk penyertaan, yaitu sebagai berikut.

a. Mereka yang melakukan (*dader*). Satu orang atau lebih yang melakukan tindak pidana. Pertanggungjawaban masing-masing peserta dinilai atau dihargai sendiri-

[72] Remmelink, *op. cit.*, hal. 97.

sendiri atas segala perbuatan atau tindakan yang dilakukan, dimana masing-masing pihak berdiri sediri dan masing-masing pihak memenuhi seluruh unsur.[74]

b. Menyuruh melakukan (*doen plegen*). Dalam bentuk menyuruh-melakukan, penyuruh tidak melakukan sendiri secara langsung suatu tindak pidana, melainkan (menyuruh) orang lain. Pada prinsipnya, orang yang mau disuruh melakukan tindak pidana adalah orang-orang tidak normal, yaitu anak-anak dan orang gila. Namun, menurut doktrin, orang yang berada dibawah ancaman atau kekerasan (ada dasar penghapus pidana) juga masuk dalam golongan tidak normal. Yang bisa dipidana hanyalah orang yang menyuruh, karena yang mempunyai niat adalah orang yang menyuruh; walaupun yang memenuhi unsur tindak pidana adalah orang yang disuruh. Jadi, walaupun ada dua pihak yang menyebabkan terjadinya delik, yang dimintai pertanggungjawaban adalah yang menyuruh.[75]

---

[74] H.A.K. Moch. Anwar, *Beberapa Ketentuan Umum Dalam Buku Pertama KUHP*, (Bandung: Alumni, 1981), hlm 39.

[75] Sianturi, *op. cit.*, hal. 342.

c. Mereka yang turut serta (*medeplegen*). Adalah seseorang yang mempunyai niat sama dengan niat orang lain, sehingga mereka sama-sama mempunyai kepentingan dan turut melakukan tindak pidana yang diinginkan.[76] Pihak yang terlibat adalah satu pihak, yang dapat terdiri dari banyak orang, niat dimiliki semua orang dalam pihak tersebut, yang memenuhi unsur, pendapat pertama menyatakan cukup salah satu orang saja yang memenuhi unsur lalu semuanya dianggap memenuhi unsur pula. Pendapat kedua menyatakan tindakan berbeda yang dilakukan orang-orang itu jika digabungkan menjadi memenuhi unsur. Pertanggungjawaban pidana dipegang oleh semuanya. Hal ini dikarenakan kerjasama yang dilakukan bersama-sama secara sadar dan secara kerjasama fisik.

d. Penggerakan (*uitlokking*). Penggerakan atau dikenal juga sebagai *Uitlokking* diatur dalam pasal 55 ayat (1) ke-2 KUHP. Menurut Brigjen Pol. Drs. H.A.K. Moch. Anwar, S.H. Penggerakan adalah :

---

[76] Lamintang, *op. cit.*, hal. 588-589.

i. Setiap perbuatan menggerakan atau membujuk orang lain untuk melakukan sesuatu perbuatan yang dilarang atau diancam dengan hukuman;
ii. Dalam membujuk itu harus digunakan cara-cara atau daya upaya sebagaimana disebutkan dalam pasal 55 ayat (1) ke-2 KUHP.[77]

Dengan demikian di dalam *uitlokking* setidaknya ada dua pihak, yaitu pihak yang membujuk dan pihak yang terbujuk, dimana pihak yang membujuk melakukan penggerakan dengan cara-cara yang telah ditentukan dalam pasal 55 ayat (1) ke-2 KUHP untuk melakukan sesuatu perbuatan yang melawan hukum.

e. Pembantuan (*medeplichtigheid*). Pada pembantuan pihak yang melakukan membantu mengetahui akan jenis kejahatan yang akan ia bantu. Niat dari pelaku pembantuan adalah memberikan bantuan untuk melakukan kejahatan kepada pelaku. Tanpa adanya pembantuan tersebut, kejahatan tetap akan terlaksana. Pertanggungjawaban pidana pembantu hanya sebatas pada kejahatan yang dibantunya saja.[78] Wirjono Prodjodikoro membagi pembantuan menjadi dua golongan yakini, perbuatan bantuan pada waktu

---

[77] Anwar, *op. cit.*, hal. 32.

[78] Loebby Loqman, *Percobaan Penyertaan dan Gabungan Tindak Pidana* (Jakarta: Universitas Tarumanagara UPT Penerbit, 1995), hal. 80.

tindak pidana dilakukan, dan perbuatan bantuan sebelum pelaku utama bertindak, dan bantuan itu dilakukan dengan cara memberikan kesempatan, sarana atau keterangan. Pembantuan golongan pertama tersebut sering dipersamakan dengan turut serta. Sedangkan pembantuan golongan kedua sering dipersamakan dengan penggerakan.[79]

Setelah menguraikan pembahasan mengenai tindak pidana dan subjek tindak pidana, berikutnya akan diuraikan penerapan kedua unsur tersebut dalam Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme.

(4) Perumusan Tindak Pidana dan Subjek Dalam Undang-undang Nomor 15 Tahun 2003

Perumusan Tindak pidana dalam Undang-undang Nomor 15 Tahun 2003 terbagi menjadi dua, yaitu tindak pidana terorisme yang diatur dalam BAB III, dan tindak pidana lain yang terkait dengan tindak pidana terorisme yang diatur dalam BAB IV undang-undang tersebut. Dalam membuat suatu

---

[79] Wirjono Prodjodikoro, *Asas-asas Hukum Pidana di Indonesia*, cet. 3, (Bandung: PT. Rafika Aditama, 2003), hal. 126.

rumusan tindak pidana, terdapat tiga macam cara. Pertama, perumusan dilakukan dengan cara merumuskan unsur-unsurnya saja, dan tidak disebutkan kualifikasi atau namanya. Kedua, perumusan dilakukan dengan merumuskan kualifikasinya saja, tidak dengan perumusan unsur-unsur. Cara yang ketiga, perumusan dilakukan dengan merumuskan unsur-unsur dan juga diberikan klasifikasi atau nama dari tindak pidana tersebut.

Cara perumusan tersebut terkait dengan pedekatan yang digunakan dalam mendefinisikan terorisme. Telah dijelaskan dalam pembahasan sebelumnya, terdapat dua cara pendekatan dalam merumuskan tindakan terorisme, secara spesifik dengan mendefinisikan berbagai kegiatan kejahatan sebagai terorisme, dan pendekatan umum berusaha memberikan penjelasan atau menguraikan tindakan mengenai terorisme, berdasarkan suatu kriteria seperti intensi, motivasi dan tujuan. Pendekatan ini merupakan upaya penjabaran peristiwa khusus terorisme kedalam peristiwa umum (metode deduktif).

Perumusan tindak pidana terorisme sendiri dalam Undang-undang Nomor 15 Tahun 2003 menggunakan cara perumusan baik itu perumusan dengan cara merumuskan unsur-unsurnya saja maupun menggunakan cara perumusan dengan

menguraikan unsur-unsur dan memberikan klasifikasi terhadap tindak pidana tersebut. Contoh dari pasal yang menggunakan cara perumusan tindak pidana dengan menguraikan unsur-unsurnya saja tanpa memberikan kualifikasi tindak pidananya adalah Pasal 6 Undang-undang Nomor 15 Tahun 2003, yang isinya sebagai berikut.

> Setiap orang yang dengan sengaja menggunakan kekerasan atau ancaman kekerasan menimbulkan suasana teror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal, dengan cara merampas kemerdekaan atau hilangnya nyawa dan harta benda orang lain, atau mengakibatkan kerusakan atau kehancuran terhadap obyek-obyek vital yang strategis atau lingkungan hidup atau fasilitas publik atau fasilitas internasional, dipidana dengan pidana mati atau penjara seumur hidup atau pidana penjara paling singkat 4 (empat) tahun dan paling lama 20 (dua puluh) tahun.[80]

Secara rinci pasal tersebut dapat diuraikan sebagai berikut berdasarkan unsur subjektif dan unsur objektifnya.[81]

---

[80] Indonesia (a), *op. cit.*, ps. 6.

[81] Unsur subjektif adalah unsur yang berkaitan dengan si pelaku itu sendiri, sedangkan unsur objektif adalah unsur yang berkaitan dengan tingkah laku dan dengan keadaan di dunia luar pada waktu perbuatan itu dilakukan. Lebih lanjut lihat Bemmelen, *op. cit.*, hal 109-110.

a. Unsur subjektif.
   i. Setiap orang.
   ii. Dengan sengaja.
   iii. menggunakan kekerasan atau ancaman kekerasan menimbulkan suasana teror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal.
b. Unsur objektif.
   i. merampas kemerdekaan atau hilangnya nyawa dan harta benda orang lain,
   ii. atau mengakibatkan kerusakan atau kehancuran terhadap obyek-obyek vital yang strategis
   iii. atau lingkungan hidup atau fasilitas publik
   iv. atau fasilitas internasional.

Pasal 6 Undang-undang Nomor 15 Tahun 2003 tersebut hanya menguraikan unsur-unsur dari tindak pidana terorisme, tetapi tidak memberikan klasifikasi tindakan tersebut sebagai tindakan terorisme. Hal yang sama juga terdapat dalam Pasal 7 Undang-undang Nomor 15 Tahun 2003, yaitu:

> Setiap orang yang dengan sengaja menggunakan kekerasan atau ancaman kekerasan **bermaksud** untuk menimbulkan suasana teror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal dengan cara merampas kemerdekaan atau hilangnya nyawa atau harta benda orang lain, atau untuk menimbulkan kerusakan atau kehancuran terhadap obyek-obyek vital yang strategis, atau lingkungan hidup, atau fasilitas publik, atau fasilitas internasional, dipidana dengan pidana penjara paling lama seumur hidup.[82] [cetak tebal dari penulis]

Sekilas pengaturan dalam Pasal 7 Undang-undang Nomor 15 Tahun 2003 tersebut menyerupai ketentuan dalam Pasal 6 Undang-undang Nomor 15 Tahun 2003, akan tetapi terdapat perbedaan, yaitu adanya unsur “bermaksud...”. Unsur ini menandakan Pasal 7 Undang-undang Nomor 15 Tahun 2003 merupakan pasal tindak pidana tidak selesai atau percobaan tindak pidana.[83] Sehingga yang harus dibuktikan dalam Pasal 7 Undang-undang Nomor 15 Tahun 2003 adalah adanya maksud untuk menimbulkan suasana teror atau rasa takut yang meluas atau menimbulkan korban yang bersifat massal, walaupun ancaman kekerasan atau kekerasannya belum dilakukan. Syarat suatu percobaan tindak pidana adalah:

---

[82] Indonesia (a), *op. cit.*, ps. 7.

[83] Muchamad Ali Syafa’at, *Tindak Pidana Teror, Belenggu Baru bagi Kebebasan*, dalam Hardiman dkk., *op. cit.,* hal. 68.

a. Sudah ada niat. Menurut Mr. J. M. van Bemmelen, dikatakan “Niat melakukan kejahatan dalam percobaan, mengambil tempat yang diduduki kesengajaan dalam delik dengan sengaja yang diselesaikan”.[84] Selanjutnya menurut Jan Remmelink dikatakan niat dalam hal percobaan disamakan dengan sengaja (dolus) dalam semua gradasinya. Dengan demikian, untuk memenuhi unsur dari niat dari suatu percobaan, harus terbukti terlebih dahulu unsur dalam kesengajaan itu sendiri yaitu unsur mengetahui dan menghendaki (*willens en wetens*) dalam upaya untuk menimbulkan suasana teror atau rasa takut.

b. Permulaan pelaksanaan. Ada dua teori utama dalam hal ini yang menjelaskan mengenai permulaan pelaksanaan. Teori tersebut timbul akibat adanya permasalahan mengenai permulaan pelaksanaan itu sendiri, yaitu apakah permulaan pelaksanaan tersebut harus diartikan sebagai “permulaan pelaksanaan dari niat / maksud si pelaku” ataukah sebagai “permulaan pelaksanaan dari kejahatan

[84] Bemmelen, *op.cit.,* hal. 246.

yang telah dimaksud oleh si pelaku untuk ia lakukan”. Adapun kedua teori tersebut sebagai berikut:

Teori Subjektif. Dalam hal ini, permulaan pelaksanaan dihubungkan dengan *niat* yang mendahuluinya (permulaan pelaksanaan tindakan dari niat). Kesimpulan dari teori ini adalah, seseorang dikatakan melakukan percobaan oleh karena orang tersebut telah menunjukan perilaku yang tidak bermoral, yang bersifat jahat ataupun yang bersifat berbahaya.

Teori Objektif. Permulaan pelaksanaan dalam teori ini dihubungkan dengan pelaksanaan tindakan dari kejahatan secara nyata. Yaitu apabila dalam delik formil: jika tindakan itu merupakan sebagian dari perbuatan yang dilarang oleh Undang-undang. Sedangkan dalam delik materiil: tindakan tersebut langsung menimbulkan akibat yang dilarang oleh Undang-undang. Pendapat ini disampaikan oleh Simons. Selain Simons, van Bemmelen pun memberikan pendapat yang sama mengenai permulaan pelaksanaan yaitu “...permulaan pelaksanaan harus merupakan permulaan pelaksanaan dari kejahatan itu sendiri dan bukan hanya permulaan pelaksanaan dari

niat".[85] Dengan demikian dapatlah kita simpulkan, yang menjadi titik ukur teori ini mengenai permulaan pelaksanaan adalah kapan peristiwa kejahatan itu nyata terjadi, bukan pada kapan niat itu dilakukan. Dengan kata lain, yang dapat dihukum sebagai percobaan adalah suatu tindakan yang telah bersifat membahayakan kepentingan hukum pihak lain.

c. Gagalnya atau tidak selesainya tindakan pelaku tindak pidana adalah di luar kehendak pelaku tindak pidana. Yang tidak selesai itu itu kejahatan, atau kejahatan itu tidak terjadi sesuai dengan ketentuan dalam undang-undang, atau tidak sempurna memenuhi unsur-unsur dari kejahatan menurut rumusannya. Jika pelaku sama sekali tidak terkait dengan kegagalan perbuatan yang hendak dilakukannya, maka percobaannya untuk melakukan tindak pidana dapat diancam dengan pidana. Dengan kata lain ada hal di luar kehendak pelaku, baik keadaan fisik maupun keadaan psikis yang datangnya dari luar yang menghalangi atau menyebabkan tidak sempurna terselesaikannya kejahatan itu. Namun apabila tidak diselesaikannya

---

[85] *Ibid.*, hal. 248.

kejahatan disebabkan oleh keadaan-keadaan yang tergantung pada kehendak pelaku maka percobaan tidaklah muncul.

Pasal 7 dan Pasal 8 Undang-undang Nomor 15 Tahun 2003 adalah contoh pasal dalam undang-undang tersebut yang cara perumusannya hanya menguraikan unsur tindak pidananya tanpa memberikan klasifikasi nama. Kedua pasal tersebut juga menggunakan pendekatan secara umum, yaitu menjadikan serangkaian tindak pidana menjadi tindak pidana terorisme.

Untuk pasal yang menggunakan cara perumusan dengan menguraikan unsur dan memberikan klasifikasi tindak pidana, terdapat dalam Pasal 8 Undang-undang Nomor 15 Tahun 2003 yang terdiri dari delapan belas tindak pidana yang dikategorikan tindak pidana terorisme. Sebagai contoh, berikut dikutip Pasal 8 huruf a Undang-undang Nomor 15 Tahun 2003.

> Dipidana karena melakukan tindak pidana terorisme dengan pidana yang sama sebagaimana dimaksud dalam Pasal 6, setiap orang yang:
>
> a. menghancurkan, membuat tidak dapat dipakai atau merusak bangunan untuk pengamanan lalu lintas

udara atau menggagalkan usaha untuk pengamanan bangunan tersebut;[86]

Dalam pasal tersebut, terdapat uraian unsur-unsur yaitu menghancurkan membuat tidak dapat dipakai atau merusak bangunan untuk pengamanan lalu lintas udara atau menggagalkan usaha untuk pengamanan bangunan tersebut, hal mana perbuatan tersebut diklasifikasikan sebagai tindak pidana terorisme. Pasal ini menggunakan pendekatan spesifik, yaitu menjadikan tindak pidana biasa sebagai atau disamakan dengan tindak pidana terorisme.

Selanjutnya, selain tindak pidana terorisme, dalam BAB III Undang-undang Nomor 15 Tahun 2003 juga diatur mengenai tindak pidana yang berkaitan dengan tindak pidana terorisme. Contohnya hal intimidasi terhadap aparat penegak hukum yang sedang memeriksa atau mengadili kasus terorisme;[87] kesaksian, barang bukti, dan alat bukti palsu;[88] dan menggagalkan secara langsung atau tidak langsung penyidikan, penuntutan, dan pemeriksaan di

---

[86] Indonesia (a), *op. cit.*, ps. 8 huruf a.

[87] *Ibid.*, ps. 20.

[88] *Ibid.*, ps. 21

sidang pengadilan dalam perkara tindak pidana terorisme.[89] Dengan demikian, pasal yang termasuk tindak pidana yang berkaitan dengan tindak pidana teroris pada dasarnya merupakan tindakan yang terkait dalam upaya atau proses hukum dalam kasus tindak pidana terorisme, dan tidak berkaitan langsung dengan tindak pidana terorisme itu sediri.

Pembahasan selanjutnya adalah mengenai subjek dari tindak pidana terorisme yang termaktub dalam Undang-undang Nomor 15 Tahun 2003. Telah dijelaskan sebelumnya, dalam hukum pidana awalnya yang menjadi subjek hukum hanyalah manusia sebagai *naturelijk persoonen*, namun dalam perkembangannya badan hukum juga dapat menjadi subjek hukum

Jika membaca ketentuan dalam Pasal 1 angka 2 Undang-undang Nomor 15 Tahun 2003 dinyatakan sebagai berikut. “Setiap orang adalah orang perseorangan, kelompok orang baik sipil, militer, maupun polisi yang bertanggung jawab secara individual, atau korporasi.” Dari pasal tersebut dapat disimpulkan mengenai subjek dari tindak pidana

[89] *Ibid.*, ps. 22

terorisme yaitu tidak hanya terbatas pada manusia sebagai pribadi kodrati tetapi juga meliputi korporasi. Dengan demikian, Undang-undang Nomor 15 Tahun 2003 telah melakukan penafsiran secara ekstensif terhadap pemahaman mengenai subjek hukum. Selain itu, dalam Undang-undang Nomor 15 Tahun 2003 ini juga terdapat pengaturan mengenai konsep penyertaan. Hal ini terlihat dalam Pasal 13 Undang-undang Nomor 15 Tahun 2003, sebagai berikut.

> Pasal 13
> Setiap orang yang dengan sengaja memberikan bantuan atau kemudahan terhadap pelaku tindak pidana terorisme, dengan :
> a. memberikan atau meminjamkan uang atau barang atau harta kekayaan lainnya kepada pelaku tindak pidana terorisme;
> b. menyembunyikan pelaku tindak pidana terorisme; atau
> c. menyembunyikan informasi tentang tindak pidana terorisme,

Pasal 13 Undang-undang Nomor 15 Tahun 2003 ini mengatur hukuman terhadap tindak pidana dalam hal terjadi penyertaan berbentuk perbantuan (*medeplichtigheid*).[90] Bentuk penyertaan yang lainnya juga terlihat dalam Pasal 14

[90] Pengaturan hukuman terhadap pembantuan dalam Pasal 57 ayat (2) KUHP tidak ditentukan batas minimum pemidanaan. Berbeda dengan Pasal 13 Undang-undang Nomor 15 Tahun 2003 yang menentukan batas minimun dan batas maksimum pemidanaan.

Undang-undang Nomor 15 Tahun 2003 yang mengatur bentuk penyertaan penggerakan (*uitlokking*), hal tersebut terlihat dari kalimat “Setiap orang yang merencanakan dan/atau menggerakkan orang lain...”.

Demikian aspek pidana materil dalam Undang-undang Nomor 15 Tahun 2003. Hal lain terkait ketentuan pidana materil yang tidak diatur dalam Undang-undang Nomor 15 Tahun 2003 tetap merujuk kepada KUHP, hal ini berdasarkan penafsiran *a contrario* terhadap Aturan penutup KUHP dalam Pasal 103 KUHP yang menyatakan ketentuan dalam KUHP berlaku juga bagi undang-undang lain kecuali jika oleh undang-undang lain ditentukan lain (asas *lex specialis derogat legi generalis*).

2. Perumusan Tindak Pidana Terorisme di Beberapa Negara Lainnya

Pembahasan ini bertujuan untuk melihat pengaturan perumusan tindak pidana terorisme yang ada dibeberapa negara lain seperti Australia dan Amerika Serikat. Tujuannya adalah untuk memperkuat tesis, terorisme adalah kejahatan global dan universal sehingga pengaturan

ketentuan terorisme disuatu negara akan berpengaruh pada negara lainnya.

(1) Australia

Tidak semua negara bagian di Australia telah memiliki ketentuan khusus terkait terorisme. Negara bagian New South Wales, Victoria, Queensland dan daerah utara lainnya adalah beberapa daerah yurisdiksi di Australia yang telah memiliki ketetentuan spesifik tentang terorisme dalam ketentuan perundang-undangannya.[91] Baru setelah terjadinya serangan 11 September 2002 di Amerika Serikat, pemerintah federal Australia memberikan fokus khusus terhadap terorisme.

Untuk itu pemerintah federal Australia mengadakan amandement *Security Legislation Amendment (Terrorism) Act 2002 (Cth)* dengan memasukan definisi baru tentang "*terrorist act*" kedalam *Criminal Code Act 1995*. Adapun isi dari ketentuan tentang terorisme tersebut sebagai berikut.

---

[91] Nathan Hancock, "Terrorism and the Law in Australia: Legislation, Commentary and Constraints," *Research Paper No 12, Commonwealth Parliament* (02-2001) pt 1.4.1.

(1) *In this Part: …*

Terrorist act means an action or threat of action where:

(a) the action falls within subsection (2) and does not fall within subsection (3); and

(b) the action is done or the threat is made with the intention of advancing a political, religious or ideological cause; and

(c) the action is done or the threat is made with the intention of:

(i) coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country, or of part of a State, Territory or foreign country; or

(ii) intimidating the public or a section of the public.

(2) Action falls within this subsection if it:

(a) causes serious harm that is physical harm to a person; or

(b) causes serious damage to property; or

(c) causes a person's death; or

(d) endangers a person's life, other than the life of the person taking the action; or

(e) creates a serious risk to the health or safety of the public or a section of the public; or

(f) seriously interferes with, seriously disrupts, or destroys, an electronic system

(g) including, but not limited to:

(i) an information system; or

(ii) a telecommunications system; or

(iii) a financial system; or

(iv) a system used for the delivery of essential government services; or

(v) a system used for, or by, an essential public utility; or

(vi) *a system used for, or by, a transport system.*[92]

---

[92] *Ibid*.

Perumusan tindak pidana dalam ketentuan tersebut hampir sama dengan perumusan tindak pidana terorisme dalam Undang-undang Nomor 15 Tahun 2003, dimana cara perumusannya adalah melalui penjabaran unsur dan pengklasifikasian. Dalam *Articles* (1) pendekatan definisi yang digunakan adalah pendekatan umum, artinya menjelaskan terorisme *per se* kemudian dijabarkan apa yang dimaksud dengan terorisme, hal ini terlihat dari kalimat "*Terrorist act means an action or threat of action where*:..."[93]

(2) Amerika Serikat

Dua belas hari tepat setelah peristiwa 11 September 2002, Presiden Amerika Serikat George W. Bush mengeluarkan Keputusan Presiden (*Executive Order*) yang isinya mengatur pemblokiran harta dan transaksi keuangan terhadap orang yang terlibat, diduga terlibat atau mendukung kegiatan terorisme. Dalam *Section 3 (d) Executive Order* tersebut diberikan definisi terhadap terorisme, yaitu:

---

[93] Golder, *op. cit.,* p. 278.

Terrorism as:

an activity that –
(i) involves a violent act or an act dangerous to human life, property or infrastructure; and
(ii) appears to be intended –
(A) to intimidate or coerce a civilian population;
(B) to influence the policy of a government by intimidation or coercion; or
(C) *to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.* [94]

Kemudian, Kongres Amerika Serikat juga mengeluarkan *Legislative Definition* terkait terorisme. Salah satu anggota Kongres, Ronald Dworkin mengeluarkan definisi yang oleh Kongres diterima sehingga menjadi *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (‘*USA PATRIOT Act*’), dimana isinya tidak jauh berbeda dengan *Executive Order* yang dikeluarkan Presiden George W. Bush.[95]

Berdasarkan uraian kententuan tentang terorisme di Indonesia serta ketentuan terorisme di Australia dan

---

[94] Exec Order No 13,224, 66 Fed Reg. 49 079 (Sept 23, 2001).

[95] Uniting and Strengthening America by Providing Appropriate Tools Required intercepting and obstructing Terrorism Act of 2001, 18 USC.

Amerika Serikat, dapat disimpulkan beberapa kesamaan antara ketentuan tersebut. Pada dasarnya, ketentuan mengenai terorisme pada tiga peraturan tersebut memuat hal sebagai berikut.

1) Aksi terorisme bersifat kejahatan yang sifatnya dapat berupa kekerasan terhadap manusia, bangunan, dan fasilitas umum lainnya.
2) Ketiga ketentuan tersebut memfokuskan perlindungan terhadap masyarakat umum dan fasilitas yang bersifat pendukung hajat hidup orang banyak.
3) Adanya perlindungan terhadap masyarakat internasional melalui ketentuan nasional.

C. Terorisme dan Perkembangannya

Technology, general term for the processes by which human beings fashion tools and machines to increase their control and understanding of the material environment.[96] Definisi teknologi tersebut memberikan gambaran kepada kita, teknologi merupakan hasil karya manusia untuk

[96] Definition of Technology, Microsoft Encarta Enciclopedia.

memahami dan mengendalikan lingkungan. Dengan adanya teknologi, peradaban manusia dapat berlangsung. Perkembangan teknologi yang merupakan hasil pemikiran manusia lah yang menyebabkan manusia mampu melewati fase jaman dan beranjak dari "jaman batu" hingga saat ini yaitu jaman "Internet".[97] Perkembangan teknologi Internet sendiri tidak terlepas dari riset yang dilakukan oleh *Advance Research Projects Agency* (ARPA. Selanjutnya pada tahun 1965, ARPA mensponsori penelitian *Cooperative Network of Time-sharing Computer,* yang menghubungkan komputer di laboratorium MIT Lincoln, laboratorium Santa Monica California dan komputer yang dimiliki ARPA.

Pada 1988, ARPA digantikan oleh *National Science Foundation* (NSF) diikuti pergantian ARPAnet menjadi NSFnet sebagai *backbone*[98] jaringan Internet. Pada musim semi tahun 1995, *backbone* Internet melakukan transisi dari NSFnet ke beberapa *backbone* komersil yang memungkinkan interkoneksi

---

[97] Definisi Internet memiliki tiga pengertian, yaitu: suatu protokol yang menghubungkan jaringan-jaringan, jaringan informasi global yang menghubungkan semua sumber informasi dunia; dan jaringan global yang titik simpulnya adalah merupakan suatu jaringan. Definisi oleh Onno W Purbo, <http://www.bogor.net/idkf/~onno/library-ref-ind/ref-ind-1/application/e-commerce/KMF-E-BIS-2001.ppt>.

[98] Backbone, yaitu Lapisan teratas dari sebuah protokol yang digunakan dalam sebuah network.

antar jaringan bisa menjadi lebih jauh jaraknya. Sejak saat ini Internet mulai digunakan secara komersil dan massal.

Dengan dikenalnya Internet, disusul dengan bermunculannya *World Wide Web,*[99] maka secara tidak langsung masing-masing pengguna Internet saling berinteraksi satu sama lain menciptakan suatu hubungan sosial. Hubungan ini pada akhirnya menciptakan suatu bentuk kehidupan masyarakat di dunia maya, atau di kenal dengan *cyber community*. Internet membawa kita kepada ruang atau dunia baru yang tercipta yang dinamakan *cyberspace*.[100] Berkaitan dengan hal ini, beberapa ahli mengemukakan pendapatnya mengenai *cyberspace*.

Agus Raharjo menjelaskan istilah *cyberspace* sebagai sebuah dunia komunikasi berbasis komputer (*computer mediated communication*) yang menawarkan realitas baru, yaitu realitas virtual (*virtual reality*).[101] Sementara itu, Edmon Makarim menggunakan istilah telematika untuk

---

[99] *World Wide Web* (WWW) yaitu sistem informasi tersebar berbasis teks tingkat tinggi *(hypertext)* dengan kemampuan menampilkan beragam bentuk/gaya teks berikut gambar grafis, atau membuat, menyunting dan melihat dokumen *hypertext.*

[100] Agus Raharjo, *Cyber crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Bandung: PT. Citra Aditya Bakti, 2002), hal. 4.

[101] *Ibid*., hal 91.

menggambarkan hakekat dari *cyberspace* yakni sebagai suatu sistem elektronik yang lahir dari hasil perkembangan dan konvergensi telekomunikasi, media dan informatika itu sendiri.[102]

Seperti dua mata pisau, teknologi dapat menyelamatkan manusia dari kehancuran, tetapi teknologi juga yang dapat menyebabkan kehancuran manusia. Begitu pula dengan perkembangnya teknologi yang telah masuk keseluruh aspek kehidupan manusia, termasuk aspek lingkup hukum terutama dalam bidang kejahatan. Kejahatan telah masuk kedalam ruang baru untuk berkembang, yaitu dunia baru yang disebut *cyberspace*. Kejahatan dalam *cyberspace* ini dikenal juga dengan istilah *cybercrime (cyberspace crime)*. Dikdik M Arief Mansyur dan Elisatris Gultom menjelaskan *cybercrime* sebagai sebagai berikut.

> Upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut.[103]

---

[102] Makarim, *op. cit.,* hal. 8.

[103] Dikdik M Arief Mansur dan Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi* (Bandung: PT. Refika Aditama, 2005), hal. 8.

Berdasarkan definisi tersebut, yang menjadi cakupan dari *cybercrime* menurut Dikdik M Arief Mansyur dan Elisatris Gultom hanyalah terbatas pada kejahatan terhadap perangkat komputer. Sedangkan dalam perkembangannya, *cybercrime* tidak terbatas pada kejahatan terhadap perangkat komputer, tetapi ada kejahatan yang memanfaatkan komputer untuk melakukan kejahatan lain. Seharusnya konsep ini juga termasuk kedalam *cybercrime*. Untuk itu perlu membagi *cybercrime* kedalam dua garis besar, yaitu kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas dan kejahatan yang menjadikan sistem dan fasilitas TI sebagai sasaran.[104]

Pendapat tersebut sejalan dengan *Tenth United Nations Kongress on the Prevention of Crime and the Tratment of Offender* di Vienna pada 10-17 April 2000, membagi 2 (dua) sub-kategori *cyber crime*, yaitu:

1. *Cyber crime in a narrow sense* (*computer crime*); *any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.*

---

[104] Arif Pitoyo, "Perlunya Penyempurnaan Hukum Pidana Tangani Cybercrime,"<http://gerbang.jabar.go.id/gerbang/index.php?index=16&idberita680>, diakses 23 Desember 2006.

2. *Cyber crime in a broader sense* (*computer related crime*); *any illegal behaviour commited by means of, or in reltion to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.* [105]

Dengan pembagian kategori *cybercrime* tersebut, terdapat beberapa jenis *cybercrime* yang dikenal saat ini. Dikdik M. Areif Mansur dan Elisatris Gultom menjelaskan jenis kejahatan yang termasuk dalam kategory *cybercime*, diantaranya sebagai berikut.

1. *Cyber-terorisme.*
2. *Cyber-pornography.* Penyebaran *obscene* materials termasuk *pornography, indencent exposure*, dan *child pornograpy*.
3. *Cyber-harassment.* Pelecehan seksual melalui *e-mail*, *websites*, atau *chat programs*
4. *Cyber-stalking. Crimes of stalking* melalui penggunaan komputer dan Internet
5. *Hacking.* Penggunaan *programming abilities* dengan maksud yang bertentangan dengan hukum.
6. *Carding* (*credit-card fraud*). Melibatkan berbagai macam aktivitas yang melibatkan kartu kredit. *Carding* muncul ketika seseorang yang bukan pemilik kartu kredit menggunakan kartu kredit tersebut secara melawan hukum. [106]

---

[105] *Tenth United Nations Kongress on the Prevention of Crime and the Tratment of Offender,* sebagaimana dikutip dalam Raharjo, *op. cit.*, hal. 229.

[106] Mansur, *op. cit.*, hal. 26.

Berdasarkan berbagai jenis *cybercrime* tersebut, terlihat variasi dari cybercrime, dimana beberapa kejahatan bertujuan untuk menyerang sistem komputer (*hacking*) dan kejahatan lain hanya memanfaatkan infrastruktur dan sistem komputer (*cyber pornography)*. Dari ragam jenis *cybercrime* tersebut, yang menjadi fokus penelitian ini adalah *cyberterrorism.*

1. *Cyberterrorism*: Suatu Perkembangan dari Terorisme

Dalam beberapa kasus, penguasaan terhadap teknologi sering kali disalahgunakan untuk melakukan suatu kejahatan. Diantara ragam kejahatan menggunakan teknologi, terdapat didalamnya suatu bentuk kejahatan terorisme baru, yaitu *cyberterrorism*.

Akar perkembangan dari *cyberterrorism* dapat ditelusuri sejak awal 1990, ketika pertumbuhan Internet semakin pesat dan kemunculan komunitas informasi. Di Amerika serikat sejak saat itu diadakan kajian mengenai potensi resiko yang akan dihadapi Amerika Serikat atas ketergantungannya yang begitu erat dengan jaringan (*networks*) dan teknologi

tinggi.[107] Dikhawatirkan, karena ketergantungan Amerika Serikat yang begitu tinggi terhadap jaringan dan teknologi suatu saat nanti Amerika akan menghadapi apa yang disebut "Electronic Pearl Harbor".[108]

Faktor psikologis, politik, dan ekonomi merupakan kombinasi yang menjadikan peningkatan ketakutan Amerika terhadap isu terkait *cyberterrorism*. Sehingga pada tahun 1999, Presiden Clinton sampai mengajukan proposal anggaran dana untuk menangani aksi *cyber terrorisme* sebesar $2.8 miliar. Dana tersebut juga diperuntukan bagi penanganan keamanan nasional dari ancaman bahaya internet.[109]

Ketakutan tersebut cukup beralasan, karena telah terjadi beberapa insiden yang dikategorikan sebagai *cyberterrorisme*, antara lain pada April dan Maret 2002, di Amerika Serikat, tepatnya negara bagian California, terjadi kehilangan pasokan listrik secara total yang disebabkan

---

[107] Gabriel Weimann (a), "Cyberterrorism: How Real Is the Threat?," *USIP Special Report No. 119* (December 2004), *file* dapat diakses di <http://www.usip.org/pubs/specialreports/sr119.html>.

[108] *Ibid*.

[109] Electronic Civil Defence, <http://ntrg.cs.tcd.ie/undergrad/4ba2.02/infowar/ecd.html>, diakses 10 Februari 2007.

oleh ulah *cracker* dari Cina yang menyusup kedalam jaringan *power generator* di wilayah tersebut.[110]

Contoh lainnya adalah aksi 40 *cracker* dari 23 negara bergabung dalam perang *cyber* konflik Israel-Palestina sepanjang bulan Oktober 2000 sampai Januari 2001. Kelompok yang menamakan dirinya UNITY dan memiliki hubungan dengan organisasi Hezbollah merencanakan akan menyerang situs resmi pemerintah Israel, sistem keuangan dan perbankan, ISPs Israel dan menyerang situs *e-commerce* kaum zionis Israel.[111]

Motif dilakukannya *cyberterrorism* menurut Zhang ada lima sebab, yaitu:[112]

(1) *Psychological Warfare*. Menurut Zhang, "*The study of the modern terrorism also reveals one of the most important characteristics of the terrorism is to raise fear.*" Motif ini tidak berbeda dengan motif terorisme konvensional, dimana sasaran

---

[110] Wikipedia, <http://en.wikipedia.org/wiki/Cyber-terrorism>, diakses 10 Februari 2007.

[111] Mansur, *op. cit.*, hal. 54.

[112] Zhang, <http://www.slais.ubc.ca/courses/libr500/04-05-wt1/www/X_Zhang/5ways.htm>, diakses 15 Februari 2007.

utama terorisme adalah menimbulkan rasa ketakutan dalam masyarakt.

(2) *Propaganda*. Melalui *cyberterrorism*, kelompok teroris dapat melakukan propaganda tanpa banyak hambatan seperti sensor informasi, karena sifat Internet yang terbuka, upaya ini jauh lebih efektif

(3) *Fundraising*. Melalui *cyberterrorism*, khususnya tindakan penyadapan dan pengambilalihan harta pihak lain untuk kepentingan organisasi teroris telah menjadi motif utama dari *cyberterrorism*. Kelompok teroris juga dapat menambah keuangannya melalui penjualan CD dan buku tentang "perjuangan" mereka.

(4) *Communication*. Motif selanjutanya dari *cyberterrorism* adalah komunikasi. Kelompok teroris telah secara aktif memanfaatkan Internet sebagai media komunikasi yang efektif dan jauh lebih aman dibandingkan komunikasi konvensional.

(5) *Information Gathering*. Kelompok teroris memiliki kepentingan terhadap pengumpulan informasi untuk keperluan teror, seperti informasi mengenai

sasaran teror, informasi kekuatan pihak musuh, dan informasi lain yang dapat menunjang kinerja kelompok teroris tersebut seperti informasi rahasia (*intelegent information*) terkait persenjataan, dan lainnya. Atas dasar motif *information gathering* lah *cyberterrorism* dilakukan.

Pergeseran wilayah terorisme konvensional ke *cyberterrorism*e disebabkan beberapa faktor. Weimann dalam tulisannya *www.terror.net: How Modern Terrorism Uses the Internet* menuturkan delapan alasan mengapa terjadi pergeseran wilayah aktifitas terorisme dari konvensional ke *cyberterrorism*e yaitu sebagai berikut. [113]

a. Kemudahan untuk mengakses. *Cyberterrorism* dapat dilakukan secara *remote*. Artinya tindakan *cyberterrorism* dapat dilakukan dimana saja melalui pengontrolan jarak jauh.
b. Sedikitnya peraturan, penyensoran, dan segala bentuk kontrol dari pemerintah.

[113] Gabriel Weimann (b), "www.terror.net: How Modern Terrorism Uses the Internet," <http://www.usip.org/pubs/specialreports/sr116.pdf>

c. Potensi penyebaran informasi yang mengglobal.

d. Anonimitas dalam berkomunikasi. Hal ini merupakan hal yang biasa dalam dunia Internet. Kebanyakan orang berinteraksi di Internet menggunakan nama palsu atau biasa disebut *nickname*.[114]

e. Arus informasi yang cepat.

f. Biaya yang rendah untuk mengembangkan dan merawat website, selain itu dalam melaksanakan cyberterrorism yang diperlukan umumnya hanya perangkat komputer yang tersambung ke jaringan Internet.[115]

g. Lingkungan multimedia yang mempermudah penyampaian maksud dan tujuan teror.

h. Kemampuan yang lebih baik dari media massa yang tradisional dalam menyajikan informasi.

2. Definisi dan Karakteristik *Cyberterrorisme*

Untuk mendalami apa dan bagaimana *cyberterrorism*, perlu terlebih dahulu diberikan definisi terhadap kata

---

[114] Weimann (a), *op. cit.*

[115] *Ibid.*

tersebut. Beberapa lembaga dan ahli memberikan definisi terkait *cyberterrorism*. Definisi pertama didapat dari *Black's Law Dictionary*, yang menjelaskan sebagai berikut.

> *Cyberterrorism. Terrorism committed by using a computer to make unlawful attacks and threats of attack againts computer, networks, and electronically stored information, and actually causing the target to fear or experience harm.*[116]

Secara bebas dapat diartikan, terorisme yang dilakukan dengan menggunakan komputer untuk melakukan penyerangan terhadap komputer, jaringan komputer, dan data elektronik sehingga menyebabkan rasa takut pada korban. Dari definisi ini terlihat unsur utama dari *cyberterrorism*, yaitu,

a. penggunaan komputer,
b. tujuannya untuk melakukan penyerangan, serangan tersebut ditujukan kepada sistem komputer dan data,
c. serta adanya akibat rasa takut pada korban.

Definisi selanjutnya dikeluarkan oleh Federal Bureau of Investigation (FBI) yang menyatakan sebagai berikut.

---

[116] Graner, *op. cit.*

> *cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents.*[117]

Secara bebas dapat diterjemahkan menjadi, *cyberterrorism* adalah serangan yang telah direncanakan dengan motif politk terhadap informasi, sistem komputer, dan data yang mengakibatkan kekerasan terhadap rakyat sipil dan dilakukan oleh sub-nasional grup atau kelompok rahasia. Definisi berikutnya diberikan oleh Dorothy Denning, yaitu:

> *Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.*[118]

Terjemahan bebasnya adalah, cyberterrorsim adalah konvergensi dari *cyberspace* dan terorisme. Pengertian tersebut merujuk pada perbuatan melawan hukum dengan cara menyerang dan mengancam melakukan serangan terhadap

---

[117] Federal Bureau of Investigation (FBI), *citation* Adam Savino, *CyberTerrorisme*,<http://www.cybercrimes.net/Terrorism/ct.html>, diakses 15 Februari 2006.

[118] Dorothy Denning, *citation from* Weimann, *op. cit.*

komputer, jaringan dan informasi yang tersimpan didalamnya untuk tujuan mengintimidasi atau memaksa pemerintah atau masyarakat untuk tujuan politik atau sosial.

Lebih lanjut, Denning menambahkan, agar dapat dikualifikasikan sebgai *cyberterrorism*, tindakan tersebut juga harus menyebabkan kekerasan terhadap manusia atau kerusakan terhadap benda, atau paling tidak menimbulkan ancaman ketakutan.

Selanjutnya, James A. Lewis memberikan definisi *cyberterrorism* sebagai berikut.

> *The use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.*[119]

Definisi yang diberikan James A. Lewis ini hampir sama dengan dua definisi sebelumnya, yaitu penekanan terhadap penggunaan komputer untuk melakukan terorisme dimana target serangannya umumnya adalah sistem komputer juga. Dalam

---

[119] James A. Lewis (a), "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," *Center of Strategic & International Studies* (December 2002): 1.

tulisannya yang lain, *The Internet and Terrorism*, Lewis menyatakan sebagai berikut.

> *The Internet enables global terrorism in several ways. It is an organizational tool, and provides a basis for planning, command, control, communication among diffuse groups with little hierarchy or infrastructure. It is a tool for intelligence gathering, providing access to a broad range of material on potential targets, from simple maps to aerial photographs. One of its most valuable uses is for propaganda, to relay the messages, images and ideas that motivate the terrorist groups.*
>
> *Terrorist groups can use websites, email and chatrooms for fundraising by soliciting donations from supporters and by engaging in cybercrime (chiefly fraud or the theft of financial data, such as credit card numbers).*[120]

Berdasarkan pernyataan tersebut, kita ketahui kemungkinan atau bentuk lain dari *cyberterrorism*, yaitu pemanfaatan teknologi informasi yang dalam hal ini Internet sebagai perangkat organisasi yang berfungsi sebagai alat untuk menyusun rencana, memberikan komando, berkomunikasi antara anggota kelompok. Selain itu, basis teknologi informasi menjadi bagian penting dari terorisme yaitu sebagai media propaganda kegiatan terorisme.

---

[120] James A. Lewis (b), "Internet and Terrorism," *Center of Strategic & International Studies* (April 2005): 1.

Penggunan basis teknologi informasi sebagai media terorisme telah menunjukan bentuk dan karakter lain dari *cyberterrorisme*. Dengan demikian secara garis besar, *Cyberterrorisme* dapat dibagi menjadi dua bentuk atau karakteristik, yaitu sebagai berikut.

1. *Cyberterrorisme* yang memiliki karkateristik sebagai tindakan teror terhadap sistem komputer, jaringan, dan/atau basis data dan informasi yang tersimpan didalam komputer.
2. *Cyberterrorisme* berkarakter untuk pemanfaatan Internet untuk keperluan organisasi dan juga berfungsi sebagai media teror kepada pemerintah dan masyarakat.

3. Bentuk dan Macam *Cyberterrorism*

Berdasarkan karakteristik dari *cyberterrorism* yang telah dijelaskan sebelumnya, kita dapat melihat bentuk dan macam dari *cyberterrorism*. Bentuk atau karakter pertama *cyberterrorism* adalah sebagai tindakan teror terhadap sistem komputer, jaringan, dan/atau basis data dan

informasi yang tersimpan didalam komputer, dan beberapa contoh dari bentuk ini adalah.

(1) *Unauthorized Access to Computer System dan Service*. Merupakan kajahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer.[121]

(2) *Denial of Service Attacks (DOS)*. Penyerangan terhadap salah satu servis yang dijalankan oleh jaringan dengan cara membanjiri server dengan jutanan permintaan layanan data dalam hitungan detik yang menyebabkan server bekerja terlalu keras dan berakibat dari matinya jaringan atau melambatnya kinerja server.[122]

(3) *Cyber Sabotage and Extortion*. Kejahatan ini dilakukan dengan membuat gangguan, pengrusakan atau penghancuran terhadap suatu data, program

---

[121] Mansur, *op. cit.*, hal. 67.

[122] Michael Gregg, *Certified Ethical Hacker Exam Prep* (United States of America: Que Publishing, 2006), Ch. 7.

komputer atau sistem jaringan komputer yang terhubung dengan internet.[123]

(4) *Viruses*. Virus adalah perangkat lunak yang telah berupa program, script, atau macro yang telah didesain untuk menginfeksi, menghancurkan, memodifikasi dan menimbulkan masalah pada komputer atau program komputer lainnya.[124]

(5) *Physical Attacks*. Penyerangan secara fisik terhadap sistem komputer atau jaringan. Cara ini dilakukan dengan merusak secara fisik, seperti pembakaran, pencabutan salah satu *devices* komputer atau jaringan menyebabkan lumpuhnya sistem komputer.[125]

Selanjutnya, beberapa contoh implementasi *cyberterrorism*e berkarakter untuk pemanfaatan Internet untuk keperluan organisasi dan juga berfungsi sebagai media

---

[123] *Ibid.*

[124] Hacker High School, "Lesson 6. Malware," <http://www.hackerhighschool.com>, p. 5.

[125] Gregg, *op. cit.*, ch. 13.

teror kepada pemerintah dan masyarakat, adalah sebagai berikut.

(1) *Propaganda*. *"The lack of censorship and regulations of the internet gives terrorists perfect opportunities to shape their image through the websites."*[126] Propaganda dilakukan melalui website yang dibuat oleh kelompok teroris. Biasanya website tersebut berisi struktur organisasi dan sejarah perjuangan, informasi detail mengenai aktifitas perjuangan dan aktifitas sosial, profil panutan dan orang yang menjadi pahlwan bagi kelompok tersebut, informasi terkait ideologi dan kritik terhadap musuh mereka, dan berita terbaru terkait aktifitas mereka.[127]

(2) *Carding* atau yang disebut *credit card fraud*. *Carding* atau *credit card fraud* dalam *cyber terrorisme* lebih banyak dilakukan dalam bentuk pencarian dana. Selain itu *carding* juga dilakukan untuk mengancam perusahaan yang bergerak di bidang penyedian jasa *e-commerce* untuk menyediakan dana

---

[126] Zhang, *op. cit.*

[127] Weimann (a), *op. cit*.

agar para *carder* tidak melepaskan data kartu kredit ke internet.[128]

(3) *E-mail.* Teroris dapat menggunakan *e-mail* untuk menteror, mengancam dan menipu, *spamming* dan menyebarkan virus ganas yang fatal, menyampaikan pesan diantara sesama anggota kelompok dan antara kelompok.

Dengan demikian, pembahasan dalam sub bab ini dapat disimpulkan. Dimasa mendatang dimana kehidupan manusia sangat bergantung pada teknologi telah menimbulkan suatu potensi kejahatan model baru yang disebut *cyberterrorism*e. Untuk itu diperlukan sebuah perangkat hukum yang dapat mengakomodir upaya hukum terhadap tindak pidana *cyberterrorism*.

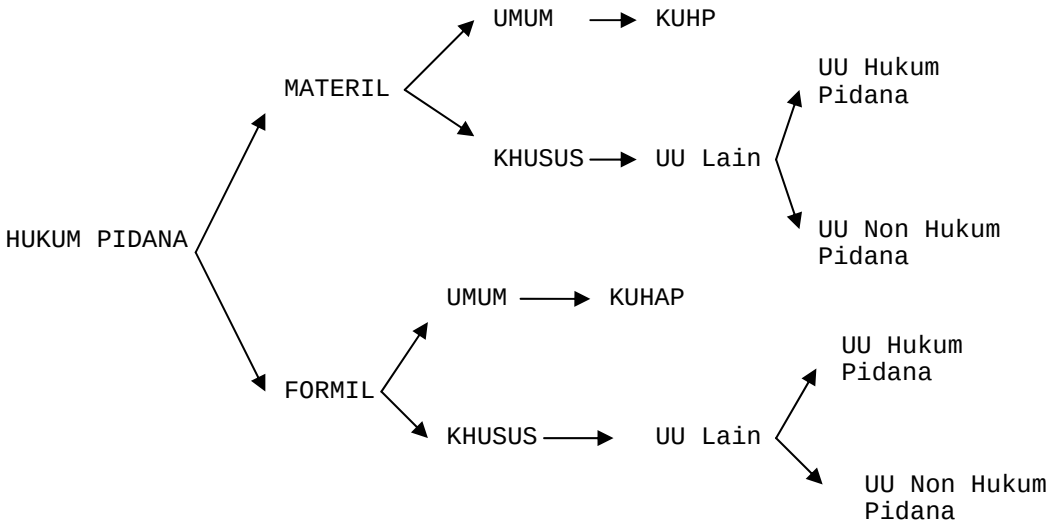
[128] Mansur, *op. cit*.

D. Proses Penyelidikan, Penyidikan, dan Upaya Paksa Penangkapan, Penahanan, Penggeledahan dan Penyitaan dalam Tindak Pidana Terorisme

Rangkaian proses beracara dalam hukum pidana telah dimulai ketika ada suatu peristiwa hukum yang terjadi. Adapun rangkaian proses acara pidana setelah diketahui adanya peristiwa pidana adalah dimulainya proses penyelidikan sebagai suatu cara atau metode yang mendahului tindakan lain. Penyelidikan dapat dikatakan sebagai langkah awal dari proses lebih lanjut, yaitu proses penyidikan, dan proses berupa upaya paksa lainnya seperti penangkapan, penahanan, dan penggeledahan.

Proses beracara dalam hukum pidana, pengaturannya secara umum diatur dalam Kitab Undang-undang Hukum Pidana (KUHAP). Namun beberapa undang-undang ternyata juga mengatur mengenai hukum acara yang terkait dengan udang-undang tersebut. Contohnya dalam undang-undang tentang tindak pidana terorisme. Dengan demikian, kedudukan dari Undang-undang Nomor 15 Tahun 2003 adalah merupakan undang-undang khusus dari KUHAP. Hal ini disebabkan terdapat pengaturan hukum acara yang menyimpang dari KUHAP. Untuk

memperjelas letak Undang-undang Nomor 15 Tahun 2003 dalam hukum pidana di Indonesia, dapat dilihat dalam skema berikut.



Berdasarkan skema tersebut, terlihat Undang-undang Nomor 15 Tahun 2003 terletak dalam dua posisi, yaitu sebagai undang-undang khusus pidana materil dan juga dapat sebagai undang-undang khusus pidana formil. Untuk itu perlu dikaji lebih lanjut mengenai hukum acara pidana dalam Undang-undang Nomor 15 Tahun 2003 dalam kaitannya dengan KUHAP.

1. Penyelidikan

Dalam Pasal 1 butir 5 KUHAP, dinyatakan penyelidikan berarti serangkaian tindakan mencari dan menemukan suatu keadaan atau peristiwa yang berhubungan dengan kejahatan dan pelangaran tindak pidana atau yang diduga sebagai perbuatan tidak pidana. Terlihat penyelidikan merupakan tindakan atau tahap permulaan dari proses selanjutnya, yaitu penyidikan. Meskipun penyelidikan merupakan proses yang berdiri sendiri, penyelidikan tidak bisa dipisahkan dari proses penyidikan.[129]

Penyelidikan merupakan bagian yang tidak terpisahkan dari fungsi penyidikan. Berdasarkan Pedoman Pelaksanaan KUHAP yang dikeluarkan oleh Departemen Kehakiman (sekarang Departemen Hukum dan Hak Asasi Manusia), dijelaskan penyelidikan adalah:

> merupakan salah satu cara atau metode atau sub daripada fungsi penyidikan yang mendahului tindakan lain, yaitu penindakan yang berupa penangkapan, penahanan, penggeledahan, penyitaan, pemeriksaan

[129] Harahap, *op. cit.*, hal. 101.

surat, pemanggilan, tindakan pemeriksaan, dan penyerahan berkas kepada penuntut umum.[130]

Fungsi dan wewenang dari penyelidik tidak diatur dalam Undang-undang Nomor 15 Tahun 2003, sehingga baik fungsi maupun wewenangnya tunduk terhadap pengaturan yang diatur dalam KUHAP. Adapun fungsi dan wewenang dari penyelidik diatur dalam Pasal 5 KUHAP, yaitu sebagai berikut.

a. Menerima laporan atau pengaduan. Penyelidik memiliki wewenang untuk menindaklanjuti adanya suatu laporan atau pengaduan dari masyarakat. Laporan atau pengaduan dari masyarakat ini dapat berupa atau sesuatu yang bisa diduga sebagai indikasi dari tindak pidana. Berdasarkan ketentuan dalam Pasal 1 butir 24, penyelidik wajib dan berwenang untuk menerima pemberitahuan laporan.[131] Adapun laporan yang diterima penyelidik harus memenuhi ketentuan yaitu, laporan tersebut harus tertulis dan harus ditandatangani oleh pelapor atau pengadu. Jika laporan tersebut dilakukan secara

---

[130] Departemen Kehakiman Republik Indonesia, *Pedoman Pelaksanaan KUHAP*, hal. 27.

[131] Indonesia (b), *op. cit.*, ps. 1 butir 24.

lisan, makan harus dicatat oleh penyelidik dan ditandatangani oleh pelapor dan penyelidik. Apabila pelapor tidak bisa menulis, maka harus diberikan keterangan oleh penyelidik.[132]

b. Mencari keterangan dan barang bukti. Telah dijelaskan sebelumnya kalau proses penyelidikan ini merupakan tahapan awal dari penyidikan dengan demikian agar proses penyidikan dapat berjalan lancar, pada tahap penyelidikan, segala keterangan maupun barang bukti harus memadai, karena segala fakta, keterangan, dan bukti tersebut akan digunakan sebagai landasan penyidikan.
c. Menyuruh berhenti orang yang dicurigai. Dasar dari kewenangan ini adalah Pasal 5 KUHAP. Penyelidik memiliki wewenang untuk menyuruh berhenti orang yang dicurigai dan menanyakan serta memeriksa tanda pengenal diri.
d. Tindakan lain menurut hukum. Ketentuan tersebut diatur dalam Pasal 5 ayat (1) KUHAP. Pada fungsi dan wewenang ini, terdapat ketidak jelasan sejauh

[132] *Ibid.*, ps. 103.

mana penyelidik dapat bertindak? Adapun penjelasan KUHAP menjelaskan, yang dimaksud dengan tindakan lain adalah tindakan dari penyelidik untuk kepentingan penyelidikan dengan syarat: Tidak bertentangan dengan suatu aturan hukum, selaras dengan kewajiban hukum yang mengharuskan dilakukanya tindakan jabatan, atas pertimbangan yang layak berdasarkan keadaan memaksa, menghormati hak asasi manusia.

Selain kewenangan yang diatur dalam KUHAP, penyelidik juga memiliki kewenangan yang bersumber dari perintah penyidik yang dilimpahkan kepada penyelidik. Tindakan dan kewenangan undang-undang melalui penyelidik dalam hal ini lebih tepat merupakan tindakan "melaksanakan perintah".[133] penyidik. Kewenagan tersebut berupa: Penangkapn, larangan meninggalkan tempat, penggeledahan, dan penyitaan; pemeriksaan dan penyitaan surat; mengambil sidik jari dan memotret seseorang; membawa dan menghadapkan seseorang pada penyidik.

[133] Harahap, *op. cit.*, hal. 107.

Dalam Undang-undang Nomor 15 Tahun 2003, ketentuan yang terkait dengan penyelidik atau penyelidikan adalah mengenai perlindungan terhadap kekerasan atau ancaman kekerasan atau dengan mengintimidasi penyelidik yang diatur dalam Pasal 20 Undang-undang Nomor 15 Tahun 2003. Dalam penjelasan umum Undang-undang Nomor 15 Tahun 2003 juga dijelaskan mengenai Undang-undang ini memuat ketentuan khusus tentang perlindungan terhadap hak asasi tersangka/terdakwa yang disebut *safe guarding rules*.

Ketentuan tersebut antara lain memperkenalkan lembaga hukum baru dalam hukum acara pidana yang disebut dengan *hearing* dan berfungsi sebagai lembaga yang melakukan *legal audit* terhadap seluruh dokumen atau laporan intelijen yang disampaikan oleh penyelidik untuk menetapkan diteruskan atau tidaknya suatu penyidikan atas dugaan adanya tindakan terorisme.

2. Penyidikan

Tahapan selanjutnya setelah penyelidikan adalah tahapan penyidikan. Pasal 1 butir 1 dan 2 KUHAP menjelaskan, penyidikan adalah serangkaian tindakan yang

dilakukan pejabat penyidik sesuai dengan cara yang diatur dalam undang-undang untuk mencari serta mengumpulkan bukti dan dengan bukti itu membuat atau menjadi terang tindak pidana yang terjadi serta sekaligus menemukan tersangkanya atau pelaku tindak pidananya.[134]

Terjadinya suatu peristiwa yang patut diduga merupakan suatu tindak pidana, dapat diketahui oleh penyeidik dengan berbagai cara, mengetahui sendiri, atau menerima laporan atau pengaduan dari seseorang. Dalam hal demikian, penyidik perlu segera melakukan tindakan penyidikan yang diperlukan seperti ditentukan dalam Pasal 106 KUHAP.[135]

Pada tahap penyidikan titik berat tekanannya diletakkan pada tindakan mencari serta mengumpulkan bukti supaya tindak pidana atau peristiwa pidana yang ditemukan menjadi terang, serta agar dapat menemukan dan menentukan pelakunya. Dalam Pasal 7 KUHAP lebih lanjut dijelaskan mengenai wewenang dari penyidik yang antara lain adalah melakukan serangkaian upaya paksa yang berupa penangkapan,

---

[134] Indonesia (b), *op. cit.*, ps. 1 butir 1 dan 2.

[135] A. Soetomo, Hukum *Acara Pidana Indonesia dalam Praktek* (Jakarta: Pustaka Kartini, 1990), hal. 20.

penahanan, penggeledahan dan penyitaan serta melakukan pemeriksaan dan penyitaan surat.[136]

Selanjutnya dalam Undang-undang Nomor 15 Tahun 2003 terdapat ketentuan dengan pengaturan secara khusus terkait penyidikan jika dibandingkan dengan yang terdapat dalam KUHAP. Hal ini terlihat dalam Pasal 25 ayat (1) Undang-undang Nomor 15 Tahun 2003, sebagai berikut.

> Penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan dalam perkara tindak pidana terorisme, dilakukan berdasarkan hukum acara yang berlaku, kecuali ditentukan lain dalam Peraturan Pemerintah Pengganti Undang-undang ini.

Berdasarkan ketentuan tersebut dapat disimpulkan, segala sesuatu terkait penyidikan yang diatur dalam Undang-undang Nomor 15 Tahun 2003 jika terdapat pengaturan yang sama dalam KUHAP, maka pengaturan yang digunakan adalah yang sesuai Undang-undang Nomor 15 Tahun 2003. Adapun yang membedakan pengaturan dalam KUHAP dengan Undang-undang Nomor 15 Tahun 2003 adalah terkait dengan upaya paksa berupa penangkapan, penahanan, dan penggeledahan.

---

[136] *Ibid.*, ps. 7 huruf c dan d.

Dalam hal siapakah pihak yang menjadi berwenang melakukan penyidikan tidak diatur dalam Undang-undang Nomor 15 Tahun 2003 tersebut, sehingga ketentuan mengenai penyidik mengikuti ketentuan yang diatur dalam KUHAP. Pihak yang berhak menjadi penyidik dalam KUHAP dapat diketahui dari Pasal 6 jo. Pasal 10 KUHAP. Dalam Pasal 6 ayat (1) huruf a KUHAP dinyatakan yang berhak menjadi penyidik adalah sebagai berikut.

1. Pejabat penyidik Polri. KUHAP telah memberikan tanggung jawab fungsi penyidikan kepada instansi Kepolisian. Akan tetapi tidak semua anggota kepolisian dapat menjadi penyidik, melainkan harus memenuhi persyaratan tertentu yang diatur dalam Peraturan Pemerintah Nomor 27 Tahun 1983. Dalam Peraturan Pemerintah tersebut, terdapat dua penyidik dari Polri. Pertama, pejabat penyidik penuh yang sekurangnya berpangkat Letnan Dua Polisi atau apabila dalam jajaran kepolisan disuatu daerah tidak ada Letnan Dua Polisi, maka Polisi berpangkat Bintara dapat menjadi penyidik. Kedua adalah penyidik pembantu dengan syarat pangkat minimum Sersan Dua Polisi atau Pegawai Negeri Sipil (PNS)

dalam lingkungan Kepolisian Negara dengan syarat sekurangnya berpangkat Pengatur Muda.

2. Penyidik Pegawai Negeri Sipil (PNS). Selain penyidik yang berasal dari Polri, KUHAP juga mengatur mengenai penyidik yang berasal dari PNS. Pengaturan tersebut terdapat dalam Pasal 6 ayat (1) huruf b, yaitu tentang PNS yang mempunyai fungsi dan wewenang sebagai penyidik. Pada umumnya, pengaturan kewenangan PNS menjadi penyidik diatur dalam undang-undang khusus, contohnya dalam Undang-undang Nomor 8 Tahun 1995 Tentang Pasar Modal, Badan Pengawas Pasar Modal (BAPEPAM) diberikan kewenangan untuk menjadi penyidik kasus terkait Pasar Modal. Kedudukan penyidik PNS sendiri ada dalam koordinasi dan di bawah pengawasan penyidik Polri. Penyidik Polri juga memberikan petunjuk kepada penyidik PNS serta memberikan bantuan terhadap penyidik PNS. Hasil penyidikan yang dilakukan penyidik PNS dilaporkan kepada penyidik Polri. Apabila penyidik PNS telah selesai melakukan penyidikan dan hasilnya akan disampaikan kepada Penuntut Umum, maka hasil tersebut diberikan

> melalui penyidik Polri. Selain itu, apabila penyidik PNS menghentikan penyidikan yang telah dilaporkan pada penyidik Polri, penyidikan tersebut harus diberitahukan kepada penyidik Polri dan penuntut umum.[137]

Telah dijelaskan sebelumnya, yang menjadi penyidik dalam Undang-undang Nomor 15 Tahun 2003 mengikuti ketentuan dalam KUHAP, dengan demikian dalam penyidik kasus tindak pidana terorisme yang dapat menjadi penyidik adalah Pejabat Penyidik dari Kepolisian Republik Indonesia dan juga Penyidik Pegawai Negeri Sipil.

3. Upaya Paksa: Penangkapan, Penahanan, Penggeledahan dan Penyitaan

Upaya paksa adalah bentuk upaya dalam mencari dan mengumpulkan bukti untuk membuat terang suatu tindak pidana yang terjadi sekaligus menemukan siapa tersangkanya dan

[137] Indonesia (b), *op. cit.*, ps. 109 ayat 3.

terkadang mengurangi kemerdekaan seseorang serta mengganggu kebebasan seseorang.[138]

(1) Penangkapan.

Berdasarkan Pasal 1 butir 20 KUHAP, dijelaskan:

> Penangkapan adalah suatu tindakan penyidik berupa pengekangan sementara waktu kebebasan tersangka atau terdakwa apabila terdapat cukup bukti guna kepentingan penyidikan atau penuntutan atau peradilan dalam hal serta cara yang diatur dalam undang-undang ini.

Karakter utama dari penangkapan adalah pengekangan sementara waktu, guna kepentingan penyidikan atau penuntutan, hal ini yang membedakan penangkapan dengan pemidanaan meskipun keduanya memiliki sifat yang sama yaitu adanya pengekangan kebebasan seseorang.

Selanjutnya, berdasarkan uraian dalam Pasal 1 butir 20 KUHAP tersebut dapat ditemukan alasan tersirat seseorang ditangkap. Seseorang ditangkap apabila seseorang tersangka diduga keras melakukan tindakan pidana, kemudian ada dugaan kuat didasarkan pada permulaan bukti yang cukup.

---

[138] Soetomo, *op. cit.*, hal. 22.

Mengenai apa yang dimaksud dengan bukti permulaan yang cukup, KUHAP tidak mengaturnya, melainkan diserahkan kepada penyidik untuk menentukannya. Hal tersebut menyebabkan terjadinya perbedaan pendapat diantara penegak hukum. Menurut Kapolri dalam SKEP/04/I/1982 tanggal 18 Februari 1982 ditentukan bukti permulaan yang cukup itu adalah bukti yang merupakan keterangan dan data yang terkandung di dalam dua di antara:

(1) Laporan polisi;

(2) Berkas Acara Pemeriksaan di Tempat Kejadian Perkara (TKP);

(3) Laporan Hasil Penyelidikan;

(4) Keterangan Saksi/Ahli; dan

(5) Barang Bukti.

Sedangkan menurut Rapat Kerja Makehjapol tanggal 21 Maret 1984 menyimpulkan bukti permulaan yang cukup seyogyanya minimal Laporan Polisi ditambah salah satu alat bukti lainnya.[139] Selanjutnya, karena sesungguhnya penangkapan ini adalah bentuk pelanggaran hak bebas seseorang yang belum terbukti bersalah, berdasarkan

---

[139] Darwan Prints, *Hukum Acara Pidana dalam Praktik* (Jakarta: Penerbit Djambatan, 1998), hal. 51.

ketentuan Pasal 19 ayat (1) KUHAP waktu penangkapan dapat dilakukan untuk paling lama satu hari. Apabila penangkapan dilakukan lewat dari satu hari, berarti telah terjadi pelanggaran hukum, dan dengan sendirinya penangkapan dianggap tidak sah.[140]

Lalu bagaimana ketentuan mengenai penangkapan yang diatur dalam Undang-undang Nomor 15 Tahun 2003? Ketentuan penangkapan dalam undang-undang tersebut mengatur ketentuan yang berbeda dengan KUHAP. Pertama, dalam hal bukti permulaan yang cukup. Dalam Pasal 26 Undang-undang Nomor 15 Tahun 2003 dijelaskan sebagai berikut.

> Pasal 26
> (1) Untuk memperoleh bukti permulaan yang cukup, penyidik dapat menggunakan setiap laporan intelijen.
> (2) Penetapan bahwa sudah dapat atau diperoleh bukti permulaan yang cukup sebagaimana dimaksud dalam ayat (1) harus dilakukan proses pemeriksaan oleh Ketua atau Wakil Ketua Pengadilan Negeri.
> (3) Proses pemeriksaan sebagaimana dimaksud dalam ayat (2) dilaksanakan secara tertutup dalam waktu paling lama 3 (tiga) hari.
> (4) Jika dalam pemeriksaan sebagaimana dimaksud dalam ayat (2) ditetapkan adanya bukti permulaan yang cukup, maka Ketua Pengadilan Negeri segera memerintahkan dilaksanakan penyidikan.

---

[140] Harahap, *op. cit.*, hal. 160.

Berdasarkan pasal tersebut, terdapat pengaturan baru yaitu penggunaan laporan intelijen sebagai bukti permulaan yang cukup. Terdapat permasalahan dalam penggunaan laporan intelijen sebagai bukti permulaan, yaitu karena laporan intelijen bersifat preventif, maka jika semua laporan intelijen layak dijadikan bukti permulaan yang cukup sebagai dasar penyidikan tindak pidana terorisme, hal tersebut adalah suatu langkah yang berlebihan dan dapat membelengu kebebasan individu.[141]

Selain itu, sebagaimana dijelaskan dalam ayat (3), pemeriksaan oleh Ketua atau Wakil Ketua Pengadilan Negeri dilaksanakan secara tertutup, hakim tidak akan memiliki opini pembanding dari laporan intelijen tersebut meskipun laporan intelijen tersebut termasuk klasifikasi AI atau AZ.[142] Pemeriksaan secara tertutup ini juga mengakibatkan seseorang tidak pernah mengetahui dirinya diduga sedang melakukan tindak pidana terorisme.

---

[141] Nasrullah, *op. cit.*, hal. 9.

[142] *Ibid*., Dalam laporan intelijen, terdapat lima klasifikasi laporan atas dasar seberapa jauh laporan tersebut dapat diandalkan dalam arti dipastikan kebenarannya. Hasil wawancara dengan Mulyo Wibisono, seorang Ahli BIN, Desember 2003.

Kedua, pengaturan terkait dengan batas waktu penangkapan. Dalam 19 ayat (1) KUHAP batas waktu penangkapan adalah satu hari, sedangkan dalam Pasal 28 dijelaskan:

> Penyidik dapat melakukan penangkapan terhadap setiap orang yang diduga keras melakukan tindak pidana terorisme berdasarkan bukti permulaan yang cukup sebagaimana dimaksud dalam Pasal 26 ayat (2) untuk paling lama 7 x 24 (tujuh kali dua puluh empat) jam.[143]

Dengan demikian, apabila seseorang ditangkap karena dugaan melakukan tindak pidana terorisme berdasarkan bukti permulaan yang cukup, sebagaimana diatur dalam Pasal 26 ayat (2) yaitu penggunaan laporan intelijen sebagai bukti permulaan yang cukup, seseorang tersebut dapat ditangkap dalam batas waktu tujuh kali dua puluh empat jam.

(b) Penahanan

Pasal 1 butir 21 KUHAP menjelaskan:

> Penahanan adalah penempatan tersangka atau terdakwa di tempat tertentu oleh penyidik atau penuntut umum atau hakim dengan penetapannya, dalam hal serta menurut cara yang diatur dalam undang-undang ini.

---

[143] Indonesia (a), *op. cit.*, ps. 28.

Berdasarkan definisi tersebut terlihat semua instansi penegak hukum memiliki wewenang dalam hal penahanan, tergantung dari tujuan penahanannya. Sebagai contoh, untuk kepentingan penyidikan, penyidik atau penyidik pembantu atas perintah penyidik berwenang melakukan penahanan.

Tidak semua pelaku kejahatan dapat dikenakan penahanan. Ditahannya seorang pelaku kejahatan atau tidak harus memenuhi dua syarat, yaitu syarat subjektif dan syarat objektif.[144] Syarat subjektif adalah alasan terkait dengan pribadi tersangka, sebagaimana dijelaskan dalam Pasal 21 ayat (1) KUHAP yang menjelaskan penahanan dilakukan terhadap seseorang tersangka atau terdakwa yang diduga keras melakukan tindak pidana berdasarkan bukti yang cukup, dalam hal adanya keadaan yang menimbulkan kekhawatiran tersangka atau terdakwa akan melakukan:

a. melarikan diri;

b. merusak atau menghilangkan barang bukti; dan/atau

c. mengulangi tindak pidana.

---

[144] T. Nasrullah (b), *Catatan Perkuliahan Hukum Acara Pidana*, Semester Gasal, Tahun Ajaran 2004 – 2005, Fakultas Hukum Universitas Indonesia.

Adapun syarat materil seorang tersangka atau terdakwa ditahan adalah apabila memenuhi ketentuan dalam Pasal 21 ayat (4) KUHAP, yaitu melakukan tindak pidana yang diancam pidana penjara lima tahun atau lebih atau melakukan tindak pidana sebagaimana diatur dalam Pasal 21 ayat (4) huruf b KUHAP. Walaupun syarat objektif sudah dipenuhi namun kalau syarat subjektif belum terpenuhi, maka tidak bisa dilakukan penahanan.[145]

Ketentuan mengenai batas waktu penahanan dalam KUHAP dibagi berdasarkan instansi mana yang melakukan penahanan. Jika penahanan tersebut diberikan oleh penyidik, maka batas waktu penahanannya paling lama dua puluh hari, dan dapat diperpanjang paling lama empat puluh hari. Sehingga, maksimal penahanan atas perintah penyidikan adalah selama enam puluh hari atau sekitar dua bulan.[146]

Penahanan atas perintah penuntut umum hanya berlaku paling lama dua puluh hari, dan guna kepentingan pemeriksaan yang belum selesai dapat diperpanjang oleh ketua pengadilan negeri yang berwenang paling lama tiga

---

[145] *Ibid.*

[146] Indonesia (b), *op. cit.*, ps 24 ayat (1) dan (2).

puluh hari. Sehingga, seorang tersangka paling lama ditahan atas perintah penuntut umum adalah lima puluh hari.[147]

Selanjutnya, jika penahanan dilakukan atas dasar perintah hakim pengadilan negeri, penahanan tersebut dilakukan untuk paling lama tiga puluh hari dan guna kepentingan pemeriksaan yang belum selesai, dapat diperpanjang oleh ketua pengadilan negeri untuk paling lama enam puluh hari, sehingga lama penahanan adalah sembilan puluh hari.

Dalam Undang-undang Nomor 15 Tahun 2003, pengaturan tentang penahanan hanya terdapat dalam satu pasal, yaitu Pasal 25 ayat (2) yang menjelaskan sebagai berikut “Untuk kepentingan penyidikan dan penuntutan, penyidik diberi wewenang untuk melakukan penahanan terhadap tersangka paling lama 6 (enam) bulan.”

Jika dibandingkan dengan KUHAP yang memberikan jangka waktu penahanan untuk kepentingan penyidikan dan penuntutan paling lama seratus sepuluh hari atau sekitar tiga setengah bulan, maka jangka waktu dalam Undang-undang Nomor 15 Tahun 2003 jauh lebih lama yaitu enam bulan. Mengenai ketentuan

---

[147] *Ibid.*, ps. 25 ayat (1) dan (2).

penahanan atas perintah hakim pengadilan negeri sebagaimana yang diatur dalam Pasal 26 ayat (1) KUHAP tidak terdapat dalam Undang-undang Nomor 15 Tahun 2003, dengan demikian ketentuan penahanan atas perintah hakim pengadilan negeri dalam Undang-undang Nomor 15 Tahun 2003 mengikuti ketentuan dalam KUHAP.

(d) Penggeledahan

Penggeledahan merupakan bagian dari wewenang dari penyidik. Terdapat perbedaan antara penahanan dengan penggeledahan dalam hal instansi yang melakukannya. Pada penahanan, masing-masing instansi penegak hukum dalam semua tingkat pemeriksaan berwenang melakukan penahanan, sedangkan dalam penggeledahan yang berwenang adalah penyidik. Meskipun demikian, dalam penggeledahan penyidik tidak bertindak sendiri melainkan ada campur tangan dari Ketua Pengadilan Negeri dalam bentuk surat izin untuk dapat melakukan penggeledahan.[148]

Penggeledahan dibagi menjadi dua, yaitu penggeledahan rumah dan penggeledahan badan. Penggeledahan rumah adalah

[148] Nasurllah (b), *op. cit.*

tindakan penyidik untuk memasuki rumah tempat tinggal dan tempat tertutup lainnya untuk melakukan tindakan pemeriksaan dan atau penyitaan, dan atau penangkapan. Sedangkan yang dimaksud dengan penggeledahan badan adalah tindakan penyidik untuk mengadakan pemeriksaan badan dan atau pakaian tersangka untuk mencari benda yang diduga keras ada pada badannya atau dibawanya serta untuk disita.

(e) Penyitaan

Penyitaan ada serangkaian tindakan penyidik untuk mengambil alih dan atau menyimpan di bawah penguasaannya benda bergerak atau tidak bergerak, berwujud atau tidak berwujud, untuk kepentingan pembuktian dalam penyidikan, penuntutan, dan peradilan.[149] Pada pokoknya, dapat disimpulkan, penyitaan adalah salah satu wewenang dari penyidik untuk mengambil alih suatu barang atau benda dari pihak tertentu.[150]

Selain penyidik, dalam penyitaan juga terlibat pihak lain yaitu pengadilan. Hal ini sejalan dengan ketentuan dalam Pasal 38 ayat (1) KUHAP yang pada pokoknya

---

[149] Indonesia (b), *op. cit.*, ps. 1 angka 16.

[150] Nasrullah (b), *op. cit.*

menjelaskan penyitaan atas benda tak bergerak harus mendapat izin dari Ketua Pengadilan Negeri. Ketentuan dalam Pasal 38 ayat (1) KUHAP tersebut dapat disimpangi apabila terjadi keadaan yang mendesak. Dalam keadaan yang mendesak, penyidik dapat melakukan penyitaan tanpa seizin Ketua Pengadilan Negeri. Akan tetapi, setelah penyidik melakukan penyitaan atas benda bergerak tersebut, penyidik wajib segera melaporkannya kepada Ketua Pengadilan Negeri.[151]

Dalam hal tertangkap tangan, penyidik juga dapat langsung melakukan penyitaan tanpa seizin Ketua Pengadilan Negeri. Penyitaan tersebut dapat dilakukan terhadap benda dan alat yang ternyata digunakan untuk melakukan tindak pidana, benda dan alat yang patut diduga telah dipergunakan dalam tindak pidana atau benda lain yang dapat digunakan sebagai alat bukti[152]

Adapun benda yang dapat disita merujuk pada ketentuan Pasal 39 ayat (1) KUHAP, yaitu:

a. benda atau tagihan tersangka atau terdakwa yang seluruh atau sebagian diduga diperoleh dan tindak pidana atau sebagai hasil dan tindak pidana;

---

[151] Indonesia (b), *op. cit.*, ps. 38 ayat (2).

[152] *Ibid.*, op. 40.

b. benda yang telah dipergunakan secara Iangsung untuk melakukan tindak pidana atau untuk mempersiapkannya;
c. benda yang dipergunakan untuk menghalang-halangi penyidikan tindak pidana;
d. benda yang khusus dibuat atau diperuntukkan melakukan tindak pidana;
e. benda lain yang mempunyai hubungan langsung dengan tindak pidana yang dilakukan.

Selain kelima benda tersebut, berdasarkan ketentuan dalam Pasal 39 ayat (2) KUHAP, benda yang berada dalam sitaan karena perkara perdata atau karena pailit juga dapat disita untuk keperluan penyidikan, penuntutan, dan pengadilan perkara pidana.

Undang-undang Nomor 15 Tahun 2003 tidak secara rinci mengatur hal mengenai penyitaan. Hanya terdapat satu pasal terkait penyitaan, yaitu Pasal 35 ayat (5) Undang-undang Nomor 15 Tahun 2003. Pada pokoknya mengatur perampasan harta kekayaan pelaku tindak pidana terorisme yang telah disita seandainya pelaku tindak pidana tersebut meninggal dunia sebelum putusan dijatuhkan dan terdapat bukti kuat yang bersangkutan adalah benar terlibat dalam tindak pidana terorisme. Dengan demikian, selain ketentuan dalam Pasal 35 ayat (5) Undang-undang Nomor 15 Tahun 2003 tersebut,

ketentuan mengenai penyitaan dalam tindak pidana terorisme mengikuti ketentuan dalam KUHAP.

E. Sistem Pembuktian, Beban Pembuktian, Alat Bukti Dalam Undang-undang Nomor 15 Tahun 2003 Tentang Tindak Pidana Terorisme

Pembuktian merupakan proses acara pidana yang memegang peranan penting dalam pemeriksaan sidang di pengadilan. Melalui pembuktian inilah ditentukan nasib terdakwa, apakah ia bersalah atau tidak. Darwan Prinst mendefinisikan pembuktian sebagai "pembuktian suatu peristiwa pidana telah terjadi dan terdakwalah yang bersalah melakukannya, sehingga harus mempertanggungjawabkannya."[153] Sesungguhnya, tujuan dari pembuktian adalah berusaha untuk melindungi orang yang tidak bersalah.

Dalam hal pembuktian, hakim perlu memperhatikan kepentingan masyarakat dan kepentingan terdakwa. Kepentingan masyarakat berarti, apabila seseorang telah melanggar ketentuan perundang-undangan, ia harus mendapat

---

[153] Prints, *op. cit.*, hal. 106.

hukuman yang setimpal dengan kesalahannya. Sementara yang dimaksud dengan kepentingan terdakwa adalah, terdakwa harus tetap diperlakukan adil sehingga tidak ada seorang pun yang tidak bersalah akan mendapat hukuman, (asas *persumtion of innocent*) atau sekalipun ia bersalah ia tidak mendapat hukuman yang terlalu berat (dalam hal ini terkandung asas *equality before the law)*.[154]

Sekalipun secara konteks yuridis teoritis, proses pembuktian dilakukan di pengadilan pada tahap pembuktian, sesungguhnya proses pembuktian sendiri telah dimulai pada tahap penyidikan. Pada tahap ini, penyidik mengolah apakah peristiwa yang terjadi merupakan peristiwa pidana atau hanya merupakan peristiwa biasa. Penyidik juga mencari dan mengumpulkan serta menganalisis bukti yang ia temukan.[155]

Dalam proses pembuktian terdapat tiga hal paling utama, yaitu sistem pembuktian, beban pembuktian, dan alat bukti. Pada proses penyelesaian terhadap tindak pidana terorisme, pembuktian sangat terkait erat dengan Hak Asasi

---

[154] Asas equality before the law berarti adanya perlakuan yang sama atas diri setiap oran di muka hukum dengan tidak mengadakan perbedaan perlakuan. Lihat Luhut MP Pangaribuan, *Hukum Acra Pidana: Surat-surat Resmi di Pengadilan oleh Advocat* (Jakarta: Djambatan, 2005), hal. 3-4.

[155] Indonesia (b), *op. cit.*, ps. 5 ayat (1) KUHAP.

Manusia (HAM). Untuk membuktian seseorang terlibat atau tidak dalam tindak pidana terorisme, proses pembuktian memegang peranan sangat penting, mengingat banyak pemidanaan dalam Undang-undang Nomor 15 Tahun 2003 berupa hukuman seumur hidup atau hukuman mati yang sesungguhnya bertentangan dengan HAM. Untuk itu perlu dikaji mengenai sistem pembuktian, beban pembuktian, dan alat bukti terkait tindak pidana terorisme sebagaimana diatur dalam Undang-undang Nomor 15 Tahun 2003.

1. Sistem Pembuktian

Menurut doktrin, terdapat empat sistem pembuktian, yaitu sebagai berikut.

a. Sistem pembuktian semata-mata berdasarkan keyakinan hakim (*conviction intime*). Dalam sistem ini, penentuan seorang terdakwa bersalah atau tidak hanya didasari oleh penilaian hakim. Hakim dalam melakukan penilaian memiliki subjektifitas yang absolut karena hanya keyakinan dan penilaian subjektif hakim lah yang menentukan keterbuktian kesalahan terdakwa. Mengenai dari mana hakim

mendapat keyakinannya, bukanlah suatu permasalahan dalam sisitem ini. Hakim dapat memperoleh keyakinannya dari mana saja.[156]

b. Sistem pembuktian berdasarkan keyakinan hakim atas alasan logis (*La Conviction Raisonee/Conviction Raisonee*). Dalam hal sistem pembuktian ini, faktor keyakinan hakim telah dibatasi. Keyakian hakim dalam sistem pembuktian ini tidak seluas pada sistem pembuktian *conviction intime* karena keyakinan hakim harus disertai alasan logis yang dapat diterima akal sehat. Sistem yang disebut sebagai sistem pembuktian jalan tengah ini disebut juga pembuktian bebas karena hakim diberi kebebasan untuk menyebut alasan keyakinannya (*vrije bewijstheorie*).[157]

c. Sistem pembuktian berdasarkan undang-undang secara positif (*positief wettelijk bewijstheorie*). Sistem pembuktian ini merupakan kebalikan dari sistem pembuktian *conviction in time*. Dalam sistem ini,

---

[156] Andi Hamzah, *Pengantar Hukum Acara Pidana di Indonesia* (Jakarta: Ghalia Indonesia, 1985), hal. 230.

[157] *Ibid*., hal. 231.

keyakinan hakim tidak diperlukan, karena apabila terbukti suatu tindak pidana telah memenuhi ketentuan alat bukti yang disebutkan dalam undang-undang, seorang terdakwa akan langsung mendapatkan vonis. Pada teori pembuktian formal/positif (*positief bewijstheorie*) ini, penekanannya terletak pada penghukuman harus berdasarkan hukum. Artinya, seorang terdakwa yang dijatuhi hukuman tidak semata-mata hanya berpegang pada keyakinan hakim saja, namun berpegang pada ketentuan alat bukti yang sah menurut undang-undang. Sistem ini berusaha menyingkirkn semua pertimbangan subjektif hakim dan mengikat hakim secara ketat menurut peraturan pembuktian yang keras.[158]

d. Sistem pembuktian undang-undang secara negatif (*negatief wettelijk bewijstheori*). Sistem pembuktian ini menggabungkan antara faktor hukum positif sesuai ketentuan perundang-undangan dan faktor keyakinan hakim. Artinya, dalam memperoleh keyakinannya, hakim juga terikat terhadap

[158] Hamzah, *op. cit.*, hal. 245.

penggunaan alat bukti yang ditentukan oleh undang-undang.

Mengenai sistem pembuktian mana yang digunakan dalam hukum acara pidana di Indonesia dapat terlihat dalam Pasal 183 KUHAP yang menyatakan hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan, suatu tindak pidana benar terjadi dan terdakwalah yang bersalah melakukannya.[159] Dengan demikian dapat disimpulkan sistem pembuktian di Indonesia menggunakan teori pembuktian undang-undang secara negatif (*negatief wettelijk bewijstheori*).

Undang-undang Nomor 15 Tahun 2003 tidak secara khusus diatur mengenai syarat minimum alat bukti, atau pun ketentuan mengenai keyakinan hakim, sehingga tidak terlihat sistem pembuktian apa yang digunakan dalam Undang-undang Nomor 15 Tahun 2003. Namun, dengan menggunakan penafsiran secara *a contrario* terhadap prinsip *lex specialis derogat legi generalis*, ketentuan mengenai sistem pembuktian dalam Undang-undang Nomor 15 Tahun 2003 menggunakan ketentuan

[159] Indonesia (b), *op. cit.*, ps. 183.

yang terdapat dalam Pasal 183 KUHAP, yaitu sistem pembuktian undang-undang secara negatif.[160] Dengan demikian, hakim dapat memutus seseorang bersalah melakukan tindak pidana terorisme apabila dari dua alat bukti yang sah ia memperoleh keyakinan kalau terdakwalah yang melakukan tindak pindana terorisme tersebut.

2. Beban Pembuktian

Beban pembuktian adalah kewajiban yang dibebankan kepada suatu pihak untuk memberikan suatu fakta di depan umum demi membuktikan fakta tersebut di depan hakim yang sedang memeriksa kasus tersebut di persidangan. Dalam hukum acara pidana dikenal tiga macam beban pembuktian, yaitu sebagai berikut.

a. Beban pembuktian biasa. Pada beban pembuktian ini, berlaku prinsip siapa yang mendalilkan maka ia

[160] Mengenai penerapan asas *lex specialis derograt legi generalis* dalam Undang-undang Nomor 15 Tahun 2003 terhadap KUHAP, secara tersirat terlihat dalam Penjelasan Umum Undang-undang Nomor 15 Tahun 2003 paragraf sembilan, yaitu sebagai berikut. “Peraturan Pemerintah Pengganti Undang-undang tentang Pemberantasan Tindak Pidana Terorisme merupakan ketentuan khusus dan spesifik karena memuat ketentuan-ketentuan baru yang tidak terdapat dalam peraturan perundang-undangan yang ada, dan menyimpang dari ketentuan umum sebagaimana dimuat dalam Kitab Undang-undang Hukum Pidana dan Kitab Undang-undang Hukum Acara Pidana.”

harus membuktikan. Beban pembuktian semacam ini biasa digunakan pada tindak pidana umum, dimana Penuntut Umum lah yang dibebani kewajiban untuk membuktikan. Seorang Jaksa Penuntut Umum harus membuktikan kebenaran dakwaan terhadap terdakwa yang ia tuliskan dalam surat dakwaan. Sedangkan, bagi terdakwa ia tidak dibebani dengan beban pembuktian.[161] Beban pembuktian seperti ini merupakan konsekuensi dari asas praduga tidak bersalah dan prinsip *non-self incrimination*, yaitu hak tersangka / terdakwa untuk tidak mempersalahkan diri sendiri.[162]

b. Beban pembuktian terbalik terbatas atau berimbang. Pada beban pembuktian seperti ini, kewajiban pembuktian terletak pada dua pihak, yaitu pada Penuntut Umum dan terdakwa sendiri. Pada dasarnya, Penuntut Umum membuktikan telah terjadi suatu peristiwa pidana yang dilakukan oleh terdakwa dan terdakwa harus mempertanggungjawabkannya. Sementara itu, terdakwa berupaya membuktikan perbuatannya

[161] Indonesia (b), *op. cit.*, ps. 66.

[162] Pangaribuan, *op. cit*.

bukan merupakan tindak pidana serta membuktikan dakwaan Penuntut Umum dalam surat dakwaan tidak benar. Dalam beban pembuktian berbalik berimbang, apabila terdakwa memiliki alibi yang kuat ia mampu membuktikan kebenarannya, maka beban pembuktian secara otomatis berpindah ke tangan Penuntut Umum untuk membuktikan dakwaan yang didakwakan adalah benar. Contoh dalam praktek, beban pembuktian semacam ini terlihat dalam tindak pidana korupsi. Dalam tindak pidana korupsi terdakwa wajib memberikan keterangan seluruh harta bendanya terkait perkara yang didakwakan, jika terdakwa tidak dapat membuktikan kekayaan yang tidak seimbang dengan penghasilannya atau sumber penambah kekayaannya, maka hal tersebut akan memperkuat alat bukti yang telah ada. Namun, penuntut umum juga tetap berkewajiban untuk membuktikan dakwaannya.[163]

c. Beban pembuktian terbalik atau pembalikan beban pembuktian. Dalam beban pembuktian terbalik, hanya terdakwalah yang dibebani kewajiban untuk

---

[163] Indonesia, *Undang-undang tentang Komisi Pemberantasan Tindak Pidana Korupsi*, UU No. 30, LN No. 137 Tahun 2002, TLN. No. 4250, ps. 37A.

membuktikan dakwaan Penuntut Umum tidak benar dan dirinya tidak bersalah. Penuntut Umum hanya bersikap pasif yaitu mengajukan dakwaan tanpa membuktikanya.[164] Contoh beban pembuktian semacam ini dapat terlihat dalam Pasal 35 Undang-undang Nomor 25 Tahun 2003 Tentang Tindak Pidana Pencucian Uang yang menjelaskan "Untuk kepentingan pemeriksaan di sidang pengadilan, terdakwa wajib membuktikan bahwa kekayaannya bukan merupakan hasil tindak pidana."[165] Berdasarkan pasal tersebut terlihat karakteristik pembuktian terbalik, yaitu dimana terdakwalah yang membuktikan ia tidak bersalah.

Baik tindak pidana korupsi maupun tindak pidana terorisme, kedua tindak pidana tersebut termasuk dalam jenis *extraordinary crime*. Akan tetapi, dalam hal pembuktian, khususnya mengenai beban pembuktian terdapat perbedaan. Dalam tindak pidana korupsi, beban pembuktiannya

---

[164] Angga Bastian dkk., *Makalah Sistem Pembuktian dan Beban Pembuktian Pada Matakuliah Hukum Pembuktian*, Fakultas Hukum Universitas Indonesia, Depok, 2006, hal. 9.

[165] Indonesia, *Undang-undang Tentang Tindak Pidana Pencucian Uang*, UU No. 15, LN. No. 30 Tahun 2002, TLN No., ps. 35.

adalah pembuktian terbalik terbatas, sedangkan dalam Undang-undang Nomor 15 Tahun 2003, beban pembuktiannya adalah beban pembuktian biasa.

Dengan demikian dalam tindak pidana terorisme, Penuntut Umum yang dibebani oleh undang-undang kewajiban untuk membuktikan seorang terdakwa terlibat atau tidak dalam tindak pidana terorisme sesuai dengan yang ia tuliskan dalam surat dakwaan.

3. Alat Bukti Dalam Tindak Pidana Terorisme dan Undang-undang Lain yang Mengatur Penggunaan Bukti Digital

Tidak ditemukan suatu definisi khusus mengenai apa itu alat bukti, namun secara umum yang dimaksud dengan alat bukti adalah alat bukti yang tercantum dalam pasal 184 ayat (1) KUHAP.[166] Fungsi dari alat bukti itu sendiri adalah untuk membuktikan adalah benar terdakwa yang melakukan tindak pidana dan untuk itu terdakwa harus mempertanggungjawabkan perbuatannya.[167] Pengaturan alat

---

[166] Djoko Prakoso, *Alat Bukti dan Kekuatan Pembuktian di dalam Proses Pidana* (Yogyakarta: Liberty, 1988), hal. 37.

[167] Harahap, *op. cit.*, hal. 285.

bukti secara umum diatur dalam Pasal 184 ayat (1) KUHAP yaitu:

a. keterangan saksi;
b. keterangan ahli;
c. surat;
d. petunjuk;
e. keterangan terdakwa.

Apabila berdasarkan KUHAP, maka yang dinilai sebagai alat bukti dan yang dibenarkan mempunyai “kekuatan pembuktian” hanya terbatas kepada alat bukti yang tercantum dalam Pasal 184 (1) KUHAP.[168] Dengan kata lain, sifat dari alat bukti menurut KUHAP adalah limitatif atau terbatas pada yang ditentukan saja. Akan tetapi, seperti yang telah diuraikan sebelumnya, KUHAP bukanlah satu-satunya undang-undang pidana formil yang mengatur mengenai ketentuan pembuktian.

Beberapa undang-undang pidana yang memiliki aspek formil juga mengatur menggenai alat bukti tersendiri. Meskipun demikian, secara umum alat bukti yang diatur dalam

[168] *Ibid.*

undang-undang pidana formil tersebut tetap merujuk pada alat bukti yang diatur dalam KUHAP. Undang-undang No. 15 Tahun 2003 tentang Tindak Pidana Terorisme selain mengatur tentang pidana material yaitu tentang macam pidana yang diklasifikasikan sebagai terorisme atau unsur tindak pidana terorisme juga mengatur aspek formil atau acara dari pidana terorisme tersebut. Dalam sub bab ini yang akan dibahas secara khusus adalah terkait dengan alat bukti yang diatur dalam Undang-undang No. 15 Tahun 2003.

Pengaturan mengenai alat bukti dalam Undang-undang No. 15 Tahun 2003 diatur dalam Pasal 27, sebagaimana berikut.

> Alat bukti pemeriksaan tindak pidana terorisme meliputi:
> 1. alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana;
> 2. alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan
> 3. data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada :
>   1) tulisan, suara, atau gambar;
>   2) peta, rancangan, foto, atau sejenisnya;
>   3) huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.

Penggunaan bukti digital dalam Undang-undang Nomor 15 Tahun 2003, terlihat pada Pasal 27 tersebut. Dalam Pasal 27 Undang-undang Nomor 15 Tahun 2003 dinyatakan yang dapat menjadi alat bukti pemeriksaan tindak pidana terorisme adalah alat bukti sebagaimana dalam Hukum Acara Pidana (merujuk pada KUHAP) dan terdapat dua alat bukti lainnya yang merupakan alat bukti digital.

Selain Undang-undang No. 15 Tahun 2003, Undang-undang No. 15 Tahun 2002 Tentang Tindak Pidana Pencucian Uang (Undang-undang No. 15 Tahun 2002) mengatur pula aspek formil atau acara dari pidana pencucian uang tersebut. Pasal 38 Undang-undang No. 15 Tahun 2002, menggunakan informasi elektronik sebagai alat bukti dalam penyidikan, penuntutan, dan pemeriksaan. Bunyi Pasal 38 Undang-undang No. 15 Tahun 2002 sebagaimana berikut.

> Pasal 38
> Alat bukti pemeriksaan tindak pidana pencucian uang berupa:
> 1. alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana;
> 2. alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara

elektronik dengan alat optik atau yang serupa dengan itu; dan
3. dokumen sebagaimana dimaksud dalam Pasal 1 angka 7.

Pasal 38 Undang-undang No. 15 Tahun 2002, khususnya huruf b membuktikan bahwa Undang-undang tersebut menggunakan alat bukti yang terkait dengan elektronik seperti informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik. Contohnya adalah informasi yang didapat dari *email* atau bukti transfer uang melalui *e-banking*.

Undang-undang Nomor 20 Tahun 2001 Tentang Perubahan Atas Undang-undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi, mengatur pula khusus tindak pidana korupsi, alat bukti dapat diperoleh berupa informasi dan dokumen elektronik. Alat bukti tersebut diatur dalam Pasal 26 A sebagai berikut.

> Alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (2) Undang-undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana, khusus untuk tindak pidana korupsi juga dapat diperoleh dari:
> a. alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan

b. dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca, dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna.

Dalam penjelasan pasal diuraikan bahwa yang dimaksud dengan “disimpan secara elektronik” misalnya data yang disimpan dalam mikro film, *Compact Disk Read Only Memory* (CD-ROM) atau *Write Once Read Many* (WORM). Sedangkan yang dimaksud dengan “alat optic atau yang serupa dengan itu” dalam ayat ini tidak terbatas pada data penghubung elektronik (*electronic data interchange*), surat elektronik (*email*), telegram, teleks, dan faksimili.

Sebagai catatan, dalam Undang-undang Nomor 20 Tahun 2001 Tentang Perubahan Atas Undang-undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi alat bukti digital digunakan sebagai perluasan alat bukti pentujuk sebagaimana dimaksud dalam Pasal 188 ayat (2) KUHAP, jadi dalam hal ini bukti digital pada tindak pidana korupsi tidak seperti bukti digital pada Tindak Pidana Pencucian Uang dan Tindak Pidana Teroris, yang penggunaannya telah berdiri sebagai satu alat bukti tersendiri.

Ketiga undang-undang yang memuat alat bukti elektronik menandakan adanya perkembangan penggunaan alat bukti konvensional menjadi alat bukti berteknologi modern sesuai perkembangan zaman. Hal tersebut berbeda dengan alat bukti yang diatur dalam KUHAP. Beberapa alat bukti yang diatur dalam KUHAP adalah surat dan petunjuk. Akan tetapi, KUHAP tidak mengakomodir kemungkinan bahwa surat atupun petunjuk tersebut ditemukan dalam format, misal, *email* atau website di Internet. Namun demikian, ketiga undang-undang tersebut mengatur lebih lanjut alat bukti yang mengandung unsur elektronik. Sehingga, dengan adanya ketiga undang-undang tersebut memungkinkan penggunaan informasi dan dokumen elektronik sebagai alat bukti.

Dikaitkan dengan tindak pidana terorisme, pengaturan alat bukti berupa informasi dan dokumen elektronik sangat diperlukan. Alasannya, aksi terorisme semakin gencar dan menghalalkan segala cara untuk dapat beraksi. Aksi terorisme yang dilakukan pun lebih pintar yaitu dengan digunakannya teknologi modern. Contohnya saja dengan adanya website www.anshar.net. Website tersebut seakan ingin lebih menunjukkan saat ini dunia menghadapi terorisme.

BAB III

KODE SUMBER *WEBSITE* SEBAGAI ALAT BUKTI BERUPA INFORMASI ELEKTRONIK

A. Aspek Pengembangan Teknologi *World Wide Web*

Teknologi *World Wide Web* (WWW) atau Web mulai berkembang sejak tahu 1990 ketika seorang peneliti bernama Tim Berners-Lee mengimplementasikan sistem manajemen untuk mencegah terjadinya kehilangan informasi dari seluruh struktur penelitian yang dilakukan oleh *European Organization for Nuclear Investigation*.[169] Perkembangan teknologi Web terkait secara langsung dengan perkembangan Internet. Internet telah menjadi tulang punggung utama dari perkembangan teknologi Web.

Pertumbuhan penggunaan Internet berbanding lurus dengan pertambahan penggunaan Web sebagai salah satu

---

[169] Tim Berners-Lee, "Information Management: A Proposal," World Wide Web Consortium (W3C).

aplikasi dari Internet. Kenaikan tersebut bahkan telah mencapai angka enam puluh dua persen pertahun.[170]

Teknologi Web pada dasarnya adalah sebuah sistem informasi yang berfungsi sebagai perantara. Perantara disini diartikan sebagai suatu program yang bertindak untuk pihak lain atau merupakan suatu proses perubahan atau merupakan proses pertukaran informasi.

Dalam hal bertindak sebagai perantara, teknologi Web umumnya dibedakan menjadi dua jenis layanan perantara, yaitu perantara dari sisi penyedia layanan (*server*) maupun perantara dari sisi pengguna layanan (*user*).[171] Perantara dari sisi *server* memiliki tugas untuk melayanani pengiriman atau penerimaan data dan informasi dari dan kesisi *user.* Sedangkan Web dipandang dari sisi *user* dapat diartikan sebagai pemberi layanan terhadap permintaan yang diajukan oleh *user*.

---

[170] Web Growth Summary, <http://www.mit.edu/people/mkgray/net/>, di akses 14 Juni 2007.

[171] *Server* adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. *Server* didukung dengan prosesor yang bersifat *scalable* dan RAM yang besar, juga dilengkapi dengan sistem operasi khusus, yang disebut sebagai sistem operasi jaringan atau *network operating system*. *Server* juga menjalankan perangkat lunak administratif yang mengontrol akses terhadap jaringan dan sumber daya yang terdapat di dalamnya, seperti halnya berkas atau alat pencetak (printer), dan memberikan akses kepada workstation anggota jaringan. Sumber: http://id.wikipedia.org/wiki/*Server*

Karateristik utama dari sebuah Web adalah adanya keterkaitan (*interlink*) antara satu Web dengan Web lain. Dengan adanya karakteristik tersebut, maka tujuan utama dari "dibuatnya" Web oleh Tim Berners-Lee telah tercapai yaitu mencegah terjadinya kehilangan secara menyeluruh seluruh data karena tidak adanya sistem distribusi data sebagaimana jika dilakukan menggunakan teknologi Web.[172] Selain memiliki karakteristik keterkaitan, teknologi Web juga memiliki ciri khas lain yaitu *evolution* dan *decentralization* yang masing-masing berarti teknologi Web akan selalu berevolusi (*evolution*) dan teknologi Web merupakan teknologi yang tersebar (*decentralization*).[173]

Agar teknologi Web selalu berkarakteristik keterkaitan, berevolusi dan terdesentralisasi, pengembangan teknologi *Website* dibagi menjadi tiga aspek bagian.[174] Bagian pertama adalah aspek repesentasi atau perwakilan

---

[172] Design space tree of the World Wide Web technology, <http://newdevices.com/publicaciones/www/ch01.html>, diakses 14 Juni 2007.

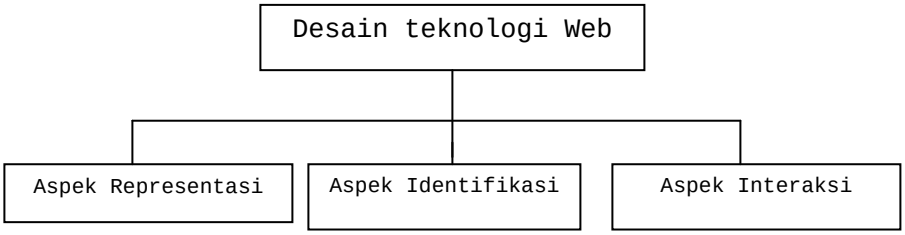
[173] World Wide Web Consortium (W3C), "About the World Wide Web Consortium (W3C)," <http://www.w3.org/Consortium/>, diakses 14 Juni 2007.

[174] Loc. cit

(*representation aspect*) yang memiliki fungsi strukturisasi dan menampilkan kembali (*represent*) segala informasi yang tersimpan dalam Web dalam kapasitasnya sebagai perantara dari sisi *server*. Desain dalam pengembangan teknologi Web yang kedua adalah aspek identifikasi (*identification aspect*) yang menggambarkan teknologi Web berfungsi sebagai media identifikasi dan melokalisasikan informasi diseluruh jaringan.

Selanjutnya, apabila sebuah informasi dalam jaringan telah distrukturisasikan, ditampilkan kembali (*representing*) kemudian telah diidentifikasi serta telah disimpan dalam suatu media penyimpanan (*storage*) atau yang lazim disebut sebagai *Web Hosting*, diperlukan suatu aspek teknologi Web terakhir yaitu aspek interaksi (*interaction*) yang berfungsi untuk mengakses, memperbarui, mengganti, memeroses atau saling menukar informasi (*information exchange*) antara jaringan yang satu dengan jaringan lainnya yang saling terinterkoneksi. Interaksi ini merupakan bentuk komunikasi antara *user* dengan *server* atau *server* dengan *server* yang terjadi melalui jalur transmisi elektronik atau

biasa disebut sebagai suatu protokol (*protocol*).[175] Dengan demikian terlihat masing-masing aspek desain tersebut akan menggambarkan seperangkat konsep independensi yang keberadaannya dapat dikombinasikan. Oleh karena itu, aspek representasi, identifikasi, dan interaksi dalam desain teknologi Web merupakan sebuah garis tegak lurus, yang saling terkait. Secara mudah, desain teknologi Web tersebut dapat digambarkan dalam diagram pohon sebagai berikut.

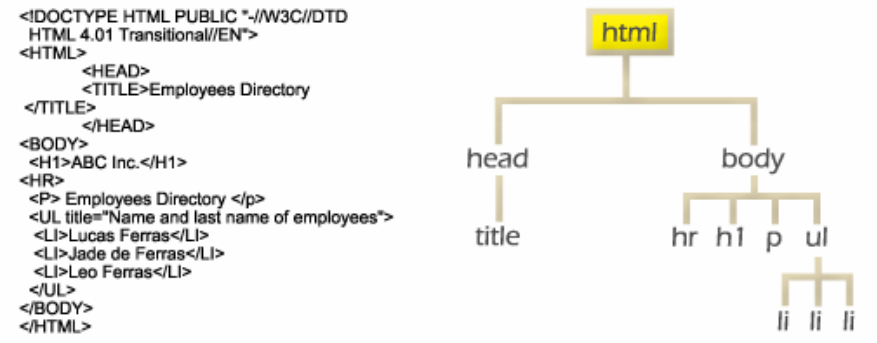


Bagan 3.1. Desain Teknologi Web

Lebih lanjut aspek tersebut dapat dijelaskan sebagai berikut. Aspek desain representasi harus diimplementasikan

[175] Berdasarkan definisi Request for Comment (RFC) yang dikeluarkan Internet Engineering Task Force (IETF) kata Protokol dapat dijelaskan sebagai berikut. “Protocol can be defined as the rules governing the syntax, semantics, and synchronization of communication. Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behavior of a hardware connection.” Secara bebas dapat diartikan, protokol adalah seperangkat aturan yang diatur berdasarkan sintaks yang disusun secara semantik dan tersinkronisasi pada sebuah jaringan komunikasi. Protokol dapat digunakan dalam tataran perangkat keras, perangkat lunak maupun kombinasi dari keduanya

dalam sebuah cara khusus. Artinya, cara tersebut merupakan cara yang melindungi prinsip interoperabilitas, evolusi, dan desentralisasi desain diantara fungsi para perantara *server – user*.[176] Gambaran tersebut menjelaskan mengapa pendesain teknologi Web mengadopsi standard internasional yaitu *Standard Generalized Markup Language* (SGML) untuk mengimplementasikan spesifikasi atau rincian yang menampilkan kembali informasi dokumen Web. Tujuan akhir dari usaha standardisasi ini adalah menjamin representasi Web yang sama jika ditampilkan dimana saja dan kapan saja. Struktur umum dari SGML dapat dilihat dari tabel berikut.



Gambar 3.1. Struktur Reperesentasi Web berdasarkan SGML

[176] Berdasarkan *The Institute of Electrical and Electronics Engineers* (IEEE) interoperabilitas adalah kemampuan dua atau lebih system atau komponen untuk pertukaran informasi dan untuk penggunaan informasi yang telah dipertukarkan.

SGML memungkinkan implementasi metode yang tepat dalam mengembangkan dan menyebarkan spesifikasi formal yang digunakan untuk menampilkan kembali sebuah informasi dalam suatu cara yang terstruktur. Hal tersebut bertujuan agar *hardware* dan *software* (perangkat keras dan perangkat lunak) yang digunakan untuk mengakses informasi yang terdapat di tempat penyimpanan perantara dapat bekerja bersama.

SGML tidak menyediakan format presentasi dalam suatu informasi. Format presentasi dari suatu informasi dalam dokumen Web merupakan fungsi dari sebuah *style sheet*. *Style sheet* memungkinkan informasi dipresentasikan kepada *user* dalam format yang mudah terbaca. Dengan demkian desain *space-tree* dari sebuah perwakilan aspek desain dua aspek desain, yaitu representasi dan presentasi.

Penampilan informasi awal diperlukan untuk menciptakan dokumen Web. Selanjutnya, mempresentasikanya kepada *user* dalam format yang mudah terbaca. Readable format adalah tampilan akhir Web yang akan dilihat oleh *user*. Fungsi aspek desain representasi adalah untuk mewakili dan memberi struktur pada informasi dokumen Web dan menjaga agat struktur Web tersebut tidak berubah. Fungsi dari aspek

desain presentasi adalah untuk menyediakan format presentasi pada informasi seperti format *text* (txt), *portable document format* (PDF), *hypertext markup language* (HTML), dan sebagainya.[177]

SGML sendiri adalah standar internasional yang digunakan untuk mendefinisikan bahasa program tingkat tinggi) untuk sebuah deskripsi dan definisi dari sebuah *mark up language* dokumen elektronik. *Mark up language* digunakan untuk menampilkan kembali informasi. SGML adalah standard internasional utama untuk menampilkan kembali informasi dari dokumen elektronik.

Untuk menyederhanakan kompleksitas standard SGML, pendesain Web menciptakan bahasa SGML yang disebut *Extensible Markup Language* (XML). Dokumen XML merupakan dokumen SGML yang sah karena XML adalah sebagai pengganti SGML di hadapan *end-user*. Teknologi Web menetapkan XML sebagai *mark-up language* utama untuk sebuah deskripsi dan

---

[177] Istilah *markup language* sendiri digunakan untuk menjelaskan adanya kombinasi teks dan tambahan informasi terkait teks tersebut. Dengan kata lain *markup laguage* adalah tambahan atau pelengkap dari substansi teks. Contoh: teks standar “hallo” jika ditambahkan *markup language* ber-*tag* hallo akan menjadi **hallo.** Teks dalam sintak tersebut adalah “hallo” sedangkan adalah pelengkap yang dalam hal ini disebut *markup language*.

definisi dokumen elektronik dan bahasa yang ditambahkan. Metode formal dalam menjelaskan sintaks SGML adalah *Extended Backus-Naur Form* (EBNF), sebuah sintaks yang digunakan untuk mendefinisikan elemen dan atribut yang digunakan dalam bahasa program tingkat tinggi.

Dengan demikian dapat disimpulkan, aspek identifikasi, representasi dan interaksi merupakan basis dasar dari teknologi Web. Ketiga aspek tersebut diimplementasikan dalam sebuah program perantara, bahasa pemerograman, sistem operasi dan spesifikasi dari *World Wide Web* atau idiom www.

1. *Hypertext Markup Language* (HTML): Standardisasi Penulisan Bahasa Web

Hypertext Markup Language (HTML) adalah sebuah *markup language* yang digunakan untuk membuat sebuah dokumen *hypertext* agar dapat berdiri secara independen. HTML sendiri adalah dokumen berbasiskan SGML yang dilengkapi seperangkat bahasa generik yang dapat disesuaikan untuk dapat merepresentasikan dokumen disebuah *Website*.

Dokumen HTML tersebut dapat berupa representasi dari dokumen berita *online*, surat elektronik (*e-mail*), perangkat

database atau tempat belanja *online* (*e-shopping*) yang dipresentasikan oleh Web melalui *Web browser*.[178] Meskipun demikian perlu diketahui, HTML bukanlah bagian dari dokumen itu sendiri melainkan atribut mandiri sebagai faktor representasi dari Web. Secara sederhana dapat dikatakan dokumen HTML adalah sebuah dokumen yang SGML. Hal tersebut disebabkan karena dokumen HTML memiliki sebuah entitas, sturktur dan logika program yang telah sesuai dengan SGML.

a. Elemen HTML Berdasarkan fungsi

Untuk mempermudah memahami kode sumber dari sebuah halaman Web caranya adalah memisahkan antara elemen dalam suatu dokumen HTML dengan isi dokumen HTML tersebut. Berikut adalah tabel yang berisi elemen HTML yang sering digunakan dalam suatu dokumen HTML.

BAGIAN HTML	NAMA TAG	TAG	FUNGSI
Head Element	Title	<title>	Memberikan judul pada tiap halaman Web
	Link	<link>	Tag yang digunakan untuk saling

[178] Web browser adalah perangkat lunak (*software*) yang digunakan oleh end-user untuk melihat tampilan sebuah Web. Dengan menggunakan web browser, end-user tidak lagi melihat struktur dasar dari sebuah Web yang terdiri dari sintaks HTML.

			menghubungkan dokumen
	Meta	<meta>	Digunakan sebagai identifikasi dari dokumen Web. Isinya dapat berupa informasi pembuat Web, aplikasi yang digunakan dalam membuat Web dan lainnya.
	Inline	 	Untuk membuat cetak miring. Membuat cetak tebal
	Image	<img>	Untuk membuat *link* terhadap suatu objek gambar
Block	Break Line	 	Memisahkan satu paragraf dengan paragraf lainnya.
	Paragraf	<p>	Memulai dan mengakhiri suatu paragraf
	Headings	<h1>,<h2>	Menentukan ukuran huruf
	Tables	<table>	Membuat suatu tabel
	Form	<form action=”..”>	Membuat formulir untuk pengisian
	Frame	<iframe>	Memasukkan objek dalam kerangka yang telah dibuat tetapi tidak terpisah dari halaman tempat tag tersebut berada.
Presentational Markup	Bold	<b>	Membuat cetak tebal (hampir sama dengan tag hanya penggunaan <b> lebih lazim digunakan suatu kata dalam kalimat tertentu)
	Font	<font [color=*color*]	Menentukan jenis huruf

		[size=*size*] [face=*face*]>…	dan besar huruf yang akan digunakan dalam suatu dokumen Web

Tabel 3.1. Tabel Elemen HTML

b. HTML Sebagai Kode Sumber Sebuah *Website*

Setelah memahami berbagai tag dari HTML yang lazim digunakan dalam sebuah dokumen Web, berikutnya akan diberikan contoh implementasi dari tag tersebut. Apabila kita menggunakan sebuah *Web browser* kemudian menuju sebuah alamat Web dengan mengetikan alamat Web tersebut pada kolom *search*, misalnya http://www.law.ui.ac.id, maka akan tampil sebuah Web sebagai berikut.

Gambar 3.2. Tampilan Web FHUI dalam Representasi dan presentasi Web Browser

Sesungguhnya tampilan Web tersebut merupakan hasil representasi dari HTML yang dilakukan oleh Web browser yang kita gunakan. Tampilan asli dari Web tersebut biasa disebut *Web source code* atau kode sumber *Website* yang tidak ditampilkan karena tidak bersifat *readable* dan tidak *user friendly*. Untuk melihat kode sumber dari sebuah Web dapat dilakukan dengan memanfaatkan fitur dari *Web browser* yang digunakan. Berikut adalah tampilan dari kode sumber *Website* http://www.law.ui.ac.id

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
        <head>
                <title>| FHUI |</title>
                <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
                <link href="images/master2.css" rel="stylesheet" type="text/css">
        </head>
        <body background="images/makarabg.gif" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0"
                <table align="center" cellpadding="0" cellspacing="0" style="border:1px solid #FFCC33">
                        <tr>
                                <td>
                                        <table width="760" border="0" align="center" cellpadding="0" cellspa
                                        <tr align="right" valign="bottom">
                                                <td height="115" colspan="4" background="images/header.gif">
                                <tr>
                                        <td width="49%"> </td>
                                        <td width="51%" align="center" valign="middle">|
                                        <a href="index.php" class="top_link">halaman depan</a> |
                                        <a href="temporary/law_ui_eng.htm" class="top_link"> english </a> |<
                                </tr>
                                <tr>
                                        <td colspan="2"> </td>
                                </tr>
                        </table>
                </td>
                </tr>
                <tr>
                        <td width="25" bgcolor="#FFFFFF"> </td>
                        <td width="550" align="left" valign="top" bgcolor="#FFFFFF">
                        <table width="100%" border="0" cellspacing="0" cellpadding="0">
                                <tr align="center" valign="middle" bgcolor="#FFFFFF">
                                        <td height="5" colspan="4"> </td>
```

Gambar 3.3. Kode Sumber Web FHUI

Jika melihat kode sumber tersebut terlihatlah sesungguhnya proses representasi dari sintaks HTML yang

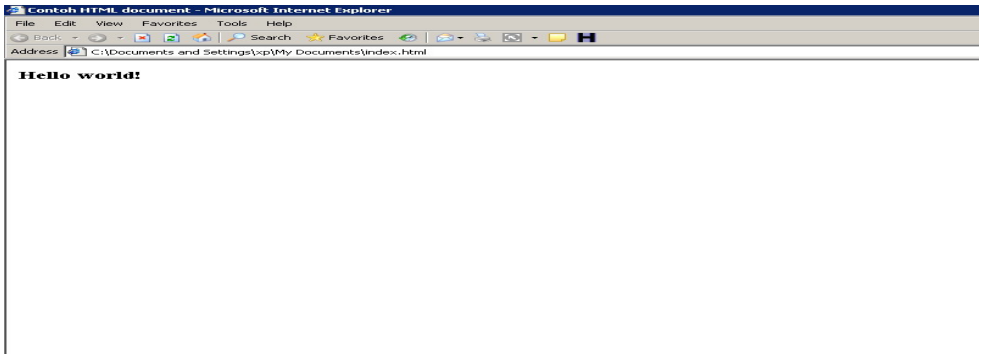
dilakukan oleh *Web browser*. Agar dapat menganalisis kode sumber dari sebuah *Website*, diperlukan pemahaman terkait dengan struktur bahasa program dari HTML itu sendiri.

Struktur dasar dari HTML selalu berawal dari *opening tag* dan berakhir pada *closing tag*. *Opening tag* dalam HTML secara umum dibuka dengan *tag* <html> dan diakhiri dengan *tag* </html>, sedangkan sintaks yang berada diantara <html> sampai dengan </html> merupakan sintaks *BODY*. Secara sederhana berikut adalah contoh struktur dari tag HTML.

```
<HTML>
   <HEAD>
        <TITLE>Contoh HTML document</TITLE>
   </HEAD>
        <BODY>
                <P><B>Hello world!</B>
        </BODY>
</HTML>
```

Skrip 3.1. Struktur Sederhana HTML

Jika struktur HTML tersebut disimpan dengan file berformat *.html lalu menggunakan Web Browser dibuka, maka file tersebut akan tampak sebagai berikut.



Gambar 3.4. Tampilan Representasi dari Sintask HTML

Dapat dijelaskan dalam tabel 4, struktur dari HTML merupakan dokumen yang tidak *user friendly* serta *unreadable*, sedangkan dalam tabel 5, sintak HTML telah direpresentasi dan dipresentasikan oleh *Web Browser* menjadi *human readable document*.

Suatu dokumen HTML memiliki unsur terpenting, unsur tersebut adalah sintak *HEAD* dan sintask *BODY*, sedangkan sintask lainnya merupakan sintak asesoris atau sintak pelengkap. Dalam sintask *HEAD* terdapat beberapa elemen pelengkap, yaitu elemen informasi mengenai dokumen HTML tersebut seperti judul dokumen atau biasa disebut dengan *TITLE* yang menggunakan tag <title></title>, kata kunci yang akan digunakan oleh mesin pencari (*search engine*) atau *META DATA* dengan *tag* <meta> dan data lain yang tidak terkait

secara langsung dengan substansi. Elemen ini tidak akan dilihat oleh pengguna Web, selama tidak melihat dari kode sumber dari dokumen HTML tersebut dan tidak akan berpengaruh secara langsung terhadap substansi dokumen. Unsur ini yang disebut unsur representasi dari Web tetapi tidak mempresentasikan isi dari HTML secara keseluruhan. Pembahasan lebih lanjut mengenai Web Forensic akan dibahas dalam sub-bab selanjutnya.

Untuk mempelajari kode sumber dari sebuah Web yang ditulis dalam bahasa HTML fokus utamanya adalah pada *BODY*, karena segala yang terdapat di dalam sintak *BODY* akan mempengaruhi substansi dari Web itu sendiri. Elemen dari *BODY* sendiri antara lain sebagai berikut. Pertama adalah elemen paragraf yang ditandai dengan *tag* <p>. Elemen paragraf ini digunakan untuk memulai suatu kalimat dalam suatu paragraf. Sebagaimana HTML pada umumnya, elemen dari *BODY* juga terdiri dari tiga bagian, yaitu *start tag* atau *opening tag* yang pada umumnya terdiri dari *attribut tag* dan *value* dari *tag* tersebut kemudian *content* atau substansi dan diakhiri oleh *end tag* atau *closing tag*. Untuk mudahnya

dapat dilihat pada contoh berikut yang diambil dari *Website* www.ansar.net pada halaman tc-1.htm

```
1  <p class="MsoNormal" align="justify">Apabila kondisi trafik sudah pas, maka
2  speda motor akan mendekati mobil dan pembonceng akan menempelkan granad ke
3  mobil. Setelah tempelan speda motor kabur. Diharapakan ledakan granad akan
4  mematikan target.</p>
```

Script 3.2. Potongan sintak BODY *Website* http://www. ansar.net dokumen tc-1.htm

Penjelasan dari script tersebut adalah, baris pertama (1) dimulai dari <p class="MsoNormal" align="justify"> adalah bagian *start tag* dengan atribut *tag*-nya adalah *class=* dan *align*, sedangkan *value*-nya adalah *MsoNormal* dan *justify*. Kemudian baris pertama hingga keempat (1-4) yang dimulai dari kata “Apabila...” hingga kata “...target” adalah content atau isi dari sintak tersebut yang akan ditampilkan di Web. Terakhir, baris keempat (4) yaitu <p>, adalah *end tag* atau *closing tag*.

Dengan demikian dapat disimpulkan yang dimaksud dengan informasi elektronik dari sebuah Web adalah keseluruhan Web tersebut, termasuk tag HTML dan substansi dari Web tersebut. Artinya, sebuah informasi elektronik Web tidak hanya meliputi substansi informasi apa yang disampaikan oleh Web, tetapi juga meliputi unsur pendukung sehingga

informasi tersebut dapat terpresentasikan melalui *Web Browser*, yang dimaksud dalam hal ini adalah atribut dari *tag* HTML. Lebih lanjut pembedahan kode sumber *Website* yang akan digunakan sebagai alat bukti akan dibahas dalam sub-bab selanjutnya.

2. *HyperText Transfer Protocol* (HTTP): Protokol Primer Sebuah *Website*.

a. HTTP: Protokol Primer Sebuah *Website*

Seperti yang telah diketahui, Web adalah aplikasi internet yang paling populer. Web memberikan penggunanya kemampuan untuk mengakses banyak informasi dan layanan ketika terhubung dengan Internet. Pengguna Web juga dapat mempublikasikan sebuah informasi atau menawarkan suatu jasa di Web melalui Internet sehingga dapat diakses seluruh orang di mana saja mereka berada sepanjang terkoneksi dengan Internet.[179]

[179] Request for Comment (RFC) 1945, "Hypertext Transfer Protocol -- HTTP/1.0," <http://tools.ietf.org/rfc/rfc1945.txt>, diakses 10 Juni 2007.

Hal demikian dapat berjalan dengan baik karena adanya sebuah protokol yang membuat seorang pengguna Web dapat menjalin keterkaitan antara satu Web dengan Web lainnya. Protokol tersebut bernama *HyperText Transfer Protocol* atau disingkat menjadi HTTP. Protokol HTTP ini telah digunakan untuk keperluan Web sejak 1990 ketika versi pengembangan dari HTTP ini masih diberi kode HTTP/1.0.[180]

HTTP adalah protokol pada lapisan aplikasi (*application layer*) dalam suatu jaringan komunikasi berbasis TCP/IP.[181] Fungsi utama dari HTTP pada awalnya adalah mengantarkan dan mendistribusikan informasi dalam format HTML pada sebuah jaringan informasi berbasiskan teknologi Internet, sehingga HTTP bukan lah layanan utama dari Internet, melainkan hanya bagian kecil dari jaringan

---

[180] Ibid.

[181] HTTP merupakan bagian dari lima lapisan protokol yang berfungsi agar tiap protokol dapat berkomunikasi. Protokol yang paling banyak digunakan dalam komunikasi antar jaringan adalah *Transmission Control Protocol* (TCP) dan *Internet Protocol* (IP). TCP/IP sendiri terdiri dari lima lapisan. Lapisan pertama (*first layer*) adalah *physical layer* yang berisi Ethernet, WiMAX, ISDN, Modem dan lainnya yang umumnya merupakan perangkat keras (*hardware*). Lapisan kedua merupakan lapisan *data link* yang berisi protokol wireless (802.11), GPRS, EVDO, PPP dan lainnya. Lapisan ketiga merupakan lapisan yang disebut *Internet layer* yang isinya adalah koneksi IP, IGMP, ICMP, ARP dan lainnya. Lapisan keempat berisi *transport layer* atau lapisan yang digunakan untuk mengantarkan data yaitu TCP, UDP, GTP dan lainnya. Sedangkan lapisan terakhir atau lapisan kelima berisi aplikasi untuk koneksi TCP/IP yaitu HTTP, FTP, DNS, SMTP, SSH dan lainnya. Lebih lanjut lihat http://tools.ietf.org/html/rfc1180.

Internet secara menyeluruh.[182] Teknologi HTTP terus berkembang, perkembangan teknologi ini ditandai dengan macam versi dari HTTP. HTTP yang pertama dinamakan HTTP/1.0 sebagaimana telah dijelaskan sebelumnya, HTTP/1.0 ini yang menjadi awal penggunaan teknologi protokol HTTP dalam mempublikasikan dokumen HTML. Sedangkan saat ini HTTP yang digunakan dalam Internet adalah versi HTTP/1.1. Dalam perkembangannya, HTTP tidak hanya mengantarkan dan mendistribusikan informasi, melainkan juga melakukan kolaborasi informasi serta melakukan manajemen terhadap sistem. Meskipun teknologi dari HTTP terus berkembang seiring bertambahnya fungsi dari HTTP, akan tetapi cara kerja dari HTTP adalah tetap, yaitu melayani transaksi komunikasi berupa *request/respone protocol* yang berasal dari pengguna (*user or client*) kepada penyedia jasa (*server*). [183]

Berdasarkan letak dalam suatu jaringan komunikasi, HTTP dapat dikatakan berada di tengah antara pengguna Internet dan penyedian jasa atau layanan Internet berupa

---

[182] Request For Comment (RFC) 2616, “Hypertext Transfer Protocol -- HTTP/1.1,” <http://tools.ietf.org/rfc/rfc2616.txt>, diakses 10 Juni 2007.

[183] *Ibid*.

Web (*server*). Protokol komunikasi memiliki dua sifat, yaitu sifat aktif dan pasif. Sifat ini ditentukan dari apakah *server* tersebut yang aktif memberikan informasi kepada jaringan atau perangkat komunikasi lain seperti protokol IP, atau protokol tersebut hanya menunggu permintaan (*request*) dari perangkat komunikasi lainnya. HTTP adalah protokol komunikasi yang sifatnya pasif.[184] Artinya, HTTP baru bekerja dalam *server* apabila ada respon (dalam istilah *computer networking* disebut kondisi *listening*). HTTP akan bekerja apabila dari sisi pengguna terdapat koneksi yang berjalan pada protokol TCP melalui port 80 menghubungi atau mengkoneksikan dirinya dengan HTTP *server*. Dalam memberikan respon terhadap komunikasi protokol TCP tersebut, HTTP *server* memiliki delapan metode dalam mengindikasikan sebuah permintaan (*request*) yang datang untuk kemudian diberikan tanggapan (*respone*). Adapun kedelapan metode respon tersebut sebagai berikut.[185]

---

[184] HTTP Performance Overview, <http://www.w3.org/Protocols/HTTP/Performance/>, diakses 11 Juni 2007.

[185] HTTP Authentication: Basic and Digest Access Authentication, <ftp://ftp.isi.edu/in-notes/rfc2617.txt>.

METODE RESPON	FUNGSI
HEAD	Berfungsi sebagai tahap identifikasi awal terhadap permintaan informasi yang datang dari pengguna. Metode respon ini hanya memberikan informasi terkait identitas data atau dalam bahasa sederhana, hanya mengidentifikasi “kepala surat” tidak mengindentifikasi “isi surat” yang dimintakan oleh pengguna.
GET	Metode respon yang diberikan oleh *server* ketika pengguna meminta suatu dokumen yang berada pada *server*.
POST	Metode ini merupakan metode respon yang diberikan oleh *server* seandainya dalam struktur sintak HTML ada form yang diisi dan dikirim melalui koneksi protokol HTTP (lihat kembali fungsi tag <form> dalam sintak HTML yang telah dijelaskan sebelumnya)
PUT	Metode respon apabila memasukkan sebuah sintak HTML (metode PUT berbeda dengan metode POST, dalam PUT dokumen tidak dikirimkan, melainkan hanya diletakkan dalam *server*)
DELETE	Untuk menghapus sebuah sintak atau dokumen dalam *server*
TRACE	Untuk melacak jalur data yang telah dilalui oleh sebuah dokumen HTML
OPTIONS	Metode yang digunakan untuk merespon permintaan yang datang apabila menggunakan berbagai layanan *server* yang berbeda sistem agar data yang diberikan sesuai dengan karakteristik sistem yang digunakan oleh pengguna
CONNECT	Metode respon dengan mengalihkan koneksi yang masuk kekoneksi lainnya. Sebagai contoh, apabila koneksi yang masuk meminta respon yang berasal dari model “secure http” maka, HTTP akan mengalihkannya dengan respon CONNECT ini ke layanan HTTPS (*hypertext transfer protocol secure*)

Tabel 3.2. Metode Respon dari HTTP

Prinsip kerja ini terkait dengan bagaimana sebuah informasi dari sebuah Web dapat terbaca melalui Web Browser. Selain itu, melalui prinsip kerja dari HTTP yang hanya melayani permintaan dan respon terhadap permintaan, terlihat HTTP tidak berfungsi sebagai media penyimpanan dari sebuah Web (*Web storage*). Untuk mempermudah, akan diperlihatkan sebuah ilustrasi bagaimana sebuah data HTML dapat terpresentasikan melalui Web Browser. Ketika kita mengetikkan alamat URL http://www.anshar.net/ di Web Browser kemudian kita menekan tombol *search*, maka Web Browser akan melakukan koneksi melalui Port 80 sebagai berikut.

```
GET /index.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /blog/wp-login.php
  User-Agent: Opera/9.20 (Windows NT 5.1; U; en)\r\n
  Host: www.anshar.net\r\n
```

Skrip 3.3. Proses permintaan dokumen terhadap suatu website

Perintah “GET /index.html HTTP/1.1\r\n” adalah perintah yang diberikan oleh *Web Browser* yang digunakan oleh pengguna (*user*) untuk mengambil “GET” dokumen HTML bernama “index.html” yang teridentifikasi menggunakan protokol versi HTTP/1.1 berada pada direktori “/” pada sebuah *server* (*Host*) “Host: www.anshar.net\r\n”. Setelah

mendapatkan request seperti itu, maka dari sisi *server* akan memberikan respon sebagai berikut.

```
HTTP/1.1 200 OK
Date: Fri, 22 June 2007 22:38:34 GMT
Server: Apache/1.3.27 (Unix)  (Red-Hat/Linux)
Last-Modified: Wed, 08 Jan 2007 23:11:55 GMT
Etag: "3f80f-1b6-3e1cb03b"
Accept-Ranges: bytes
Content-Length: 438
```

Skrip 3.4. Respon dari website

Respon dari *server* tersebut pada pokoknya menjelaskan koneksi dari pengguna pada Jumat, 22 Juni 2007 Pukul 22:38:34 Waktu GMT telah diterima dengan baik (Status “OK”) melalui protokol HTTP/1.1 dengan kode keberhasilan “200”. Informasi lainnya dalam respon tersebut terkait dengan sistem operasi yang dijalankan oleh program HTTP tersebut.

Berdasarkan gambaran koneksi terhadap suatu *Website* yang telah dijelaskan sebelumnya, terbukti peran dari protokol HTTP adalah sebagai protokol primer dalam proses representasi dan presentasi dari HTML. Tanpa adanya HTTP, tidak akan ada substansi HTML yang akan terlihat oleh pengguna. Begitu pula dari sisi *server*, tanpa adanya

permintaan dan respon yang diberikan *user* terhadap *server* HTTP maka *daemon server* HTTP tidak akan bekerja pula.[186]

b. Penelusuran Transaksi TCP/IP Berbasiskan HTTP Terhadap Pembuatan *Website* Al-Anshar.net

Dalam studi kasus pada penulisan ini, M. Agung Prabowo mendesain situs http://www.anshar.net dan mendaftarkan hosting lewat alamat situs www.joker.com dan www.openhosting.co.uk. Pendaftaran itu ia lakukan dengan *carding* atau menggunakan nomor kartu kredit orang lain.[187] Pada kondisi semacam ini akan terlihat adanya tiga jenis transaksi TCP/IP yang saling berkaitan. Pertama, adanya transaksi antara M. Agung Prabowo dengan *server* penyedian layanan pendaftaran *domain name* yaitu *server* Web www.joker.com.[188] Dengan menggunakan *Operation System* Debian

---

[186] Terminologi *daemon server* merujuk pada sebuah proses yang berjalan pada sisi *server* dan mempunyai tujuan serta fungsi tertentu. Lebih lanjut lihat http://en.wikipedia.org/wiki/Web_*server*.

[187] "Bertemu di Dunia Maya, Berakhir di Penjara," *Sinar Harapan*, <http://www.sinarharapan.co.id/berita/0706/21/nas04.html>. diakses 21 Juni 2007.

[188] *Domain name* adalah nama yang digunakan di Internet untuk mempermudah penyebutan terhadap alamat suatu *server*. Lebih lanjut lihat http://www.icann.org/.

GNU/Linux 4.0, dapat dilakukan penelusuran terhadap Web tersebut sebagai berikut.

```
zka@ahmadzakaria:~$ whois joker.com

domain:       joker.com
owner:        n/a
organization: CSL Computer Service Langenbach GmbH
email:        admin@joker.com
address:      Hansaallee 191-193
city:         Duesseldorf
postal-code:  40549
country:      DE
```

Skrip 3.5. Perintah untuk melihat identitas website

Berdasarkan hasil penelusuran tersebut diketahui M. Agung Prabowo telah melakukan transaksi TCP/IP dari Indonesia menuju *server* yang berada di Jerman (DE).[189] Maka berdasarkan penjelasan sebelumnya yaitu setiap transaksi TCP/IP yang terjadi terhadap *server* akan diberikan respon. Disamping memberikan respon, *server* juga mencatat sumber transaksi tersebut yang dalam hal ini alamat IP yang digunakan oleh M. Agung Prabowo.[190]

---

[189] Kode block IP Jerman dapat dilihat di http://www.ipdeny.com/ipblocks/data/countries/de.zone

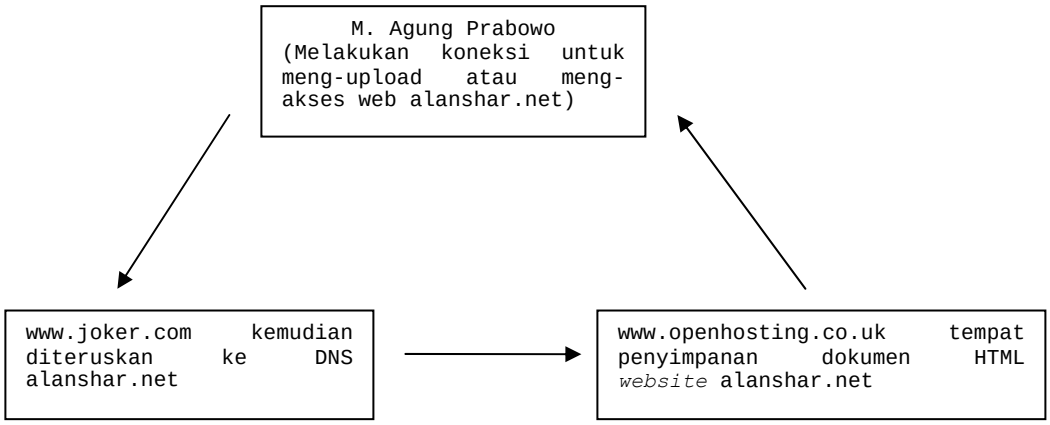
[190] Berdasarkan definisi yang diberikan oleh Wikipedia Alamat IP dijelaskan sebagai berikut. Alamat IP adalah alamat unik pada tiap perangkat elektronik yang digunakan untuk mengidentifikasi dan berkomunikasi dengan perangkat lain pada jaringan Internet.Lebih lanjut lihat http://en.wikipedia.org/wiki/IP_address.

Transaksi TCP/IP kedua yang dilakukan oleh M. Agung Prabowo adalah transaksi TCP/IP dengan *server* www.openhosting.co.uk, yang bertindak sebagai *server* tempat M. Agung Prabowo meletakan dokumen HTML (*Web hosting*). Di *server* www.openhosting.co.uk ini seluruh dokumen HTML oleh M. Agung Prabowo disimpan (*storage*) untuk kemudian apabila ada *request* HTTP, *server* akan merespon dengan merepresentasikan serta mempresentasikan dokumen HTML tersebut.

Transaksi terakhir adalah transaksi yang terjadi antara tiga pihak, yaitu antara M. Agung Prabowo, *server* www.joker.com sebagai penyedia domain name dan dengan *server* www.openhosting.co.uk. Kondisi ini terjadi pada saat M. Agung Prabowo melakukan *upload* dokumen HTML ke *Website* www.anshar.net, maka sesungguhnya pertama kali komputer M. Agung Prabowo akan melakukan koneksi ke *Domain Name Server* (DNS) untuk mencari *domain name* alanshar.net, setelah domain tersebut ditemukan, maka koneksi tersebut akan dilanjutkan ke *Web Hosting*-nya yaitu www.openhosting.co.uk.

Setelah terjadi koneksi, M. Agung Prabowo dapat melakukan upload atau mengakses *Website* tersebut. Pada tahap tersebut, *Website* Al-Anshar sudah dapat diakses oleh

setiap orang yang terhubung ke Internet. Jika digambarkan, maka koneksi ketiga pihak tersebut akan tampak sebagai berikut.



Bagan 3.2. Proses transaksi HTTP

Dengan pemahaman terhadap konsep HTML dan transaksi TCP/IP melalui protokol HTTP, langkah untuk memperoleh bukti keterlibatan M. Agung Prabowo dalam pembuatan al-anshar.net dapat dilakukan dengan lebih mudah. Artinya, dalam melakukan pencarian bukti tersebut lingkup pencariannya telah diperkecil yaitu melihat pada tiga bentuk koneksi TCP/IP yang terjadi. Selanjutnya yang perlu dipahami adalah, bukti seperti apa yang diperoleh dari penelusuran transaksi koneksi TCP/IP tersebut, apakah bukti tersebut berupa bukti yang selama ini dikenal dalam Hukum

Acara Pidana Indoensia ataukah bukti digital, yaitu suatu terminologi baru dalam Hukum Acara Pidana di Indonesia. Untuk itu lebih lanjut mengenai bukti digital akan dibahas dalam sub-bab berikut.

B. Bukti Digital (*Digital Evidence*)

Perkembangan teknologi menyebabkan tergesernya bentuk media cetak menjadi bentuk media digital (*paper less*). Beberapa contoh dari perkembangan ini dengan adanya media pemberitaan online seperti Detikcom (www.detik.com) yang telah mengubah paradigma pemberitaan lama, yaitu secara konvensional melalui media cetak untuk kemudian dikembangkan menjadi berbasis Internet. Contoh lain, mulai maraknya *Internet Banking* atau kegiatan perbankan berbasiskan Internet yang dilakukan oleh usaha perbankan di Indonesia.

Perkembangan tersebut juga diikuti oleh berkembangnya jenis kejahatan baru menggunakan komputer. Pada umumnya kejahatan berbasis komputer merupakan kejahatan biasa, hanya saja karena berbasis komputer maka terdapat karakteristik khusus yang membedakan dengan kejahatan

biasa. Salah satu karakter khususnya ada pada bukti kejahatan berbasis komputer berbeda dengan bukti pada kejahatan konvensional. Bukti pada kejahatan berbasiskan komputer akan mengarahkan suatu peristiwa pidana pada bukti berupa data elektronik, baik yang berada di dalam komputer itu sendiri (*hardisk/floppy disc*) atau yang merupakan hasil *print out*, atau dalam bentuk lain berupa jejak (*path*) dari suatu aktivitas pengguna komputer.[191]

Hal ini sejalan dengan pendapat dari Susan W. Brenner dalam tulisanya berjudul "*Cybercrime Metrics: Old Wine, New Bottles?*" yang menyatakan sebagai berikut.

> *The differentiating effects of these factors are exacerbated by another aspect of online crime. Because online criminals commit their crimes in a virtual environment, the evidence that law enforcement needs to apprehend and convict them is, for the most part, intangible, digital evidence.*[192]

Pendapat tersebut pada pokoknya menjelaskan kejahatan online dilakukan pada lingkungan online pula, sehingga

---

[191] Makarim, *op. cit.*, hal. 455.

[192] Susan W. Brenner, "Cybercrime Metrics: Old Wine, New Bottles?," *Virginia Journal of Law & Technology* (Fall 2004): 14.

bukti yang dibutuhkan untuk penegakan hukum dari kejahatan tersebut umumnya bersifat tidak berwujud.

1. Pengertian Bukti Digital (*Digital Evidence*)

Tidak banyak ditemukan dalam literatur berbahasa Indonesia termasuk peraturan perundang-undangan yang di dalamnya mengatur penggunaan bukti digital pada acara pembuktian menjelaskan definisi dari bukti digital. Untuk itu perlu mencari literatur beserta doktrin dari negara lain yang telah lama menerapkan bukti digital dalam proses hukum. Kelompok kerja yang bernama "*The Scientific Working Group on Digital Evidence*" (SWGDE) yang berdiri sejak Pebruari 1998 bekerjasama dengan Laboratorium Kriminal Federal di Amerika Serikat (*US Federal Crime Laboratory*) dan supervisi dari *International Organization on Computer Evidence* (IOEC) dalam kajian multidisipliner memberikan pedoman dan standardisasi terhadap upaya perolehan kembali, penyajian kembali dan pengujian terhadap bukti digital,

termasuk peralatan audio, pencitraan dan gambar yang menggunakan elektronik.[193]

Hasil dari kelompok kerja tersebut salah satunya adalah definisi dari bukti digital (*digital evidence*). Definisinya yang diberikan kelompok kerja tersebut adalah "*Information of probative value stored or transmitted in digital form*."[194] Definisi tersebut jika diterjemahkan secara bebas sebagai berikut. Bukti digital adalah segala informasi yang bersifat membuktikan terhadap nilai yang tersimpan atau ditransmisikan dalam bentuk digital.[195] Berdasarkan definisi tersebut, bukti digital tidak hanya meliputi bukti yang dihasilkan atau ditransmisikan melalui jaringan komputer saja, akan tetapi juga termasuk perangkat audio, video bahkan telepon selular.[196]

---

[193] Albert J. Marcella and Robert Greenfield, *Cyber Forensics — A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes* (New York: A CRC Press Company, 2001), p. 131.

[194] Carrie Morgan Whitcomb, "An Historical Perspective of Digital Evidence: A Forensic Scientist's View," *International Journal of Digital Evidence* (Spring 2002, Vol. 1, Issue 1): 4.

[195] Digital merupakan kata yang digunakan dalam menggambarkan transmisi data berbasiskan bilangan biner 1 dan 0. Lebih lanjut lihat http://en.wikipedia.org/wiki/Digital.

[196] Brenner, *op. cit.*, p. 3.

Debra Littlejohn Shinder mengklasifikasikan digital menjadi dua bagian, yaitu:

> *Digital evidence can be classified as original digital evidence (that is, the physical items and data objects associated with those items at the time the evidence was seized) and duplicate digital evidence (referring to an accurate digital reproduction of all the data objects contained on an original physical item).*[197]

Klasifikasi yang diberikan oleh Debra Littlejohn Shinder terkait dengan bentuk dan sifat dari bukti digital itu sendiri. Klasifikasi pertama menjelaskan bukti digital yang orisinal, yaitu bukti digital secara fisik dan data yang terasosiasi dengan perangkat fisik tersebut ketika bukti digital disita oleh kepolisian.[198] Sedangkan klasifikasi kedua merujuk pada bukti digital yang merupakan hasil duplikasi atau hasil reproduksi dari bukti digital orisinal, di dalamnya terkadung data sebagaimana yang terdapat pada bukti digital orisinal.

---

[197] Debra Littlejohn Shinder, *Scene of The Cybercrime, Computer Forensics Handbook* (United State of America: Syngress Publishing Inc., 2002), p. 550.

[198] Pengertian data disini merujuk pada istilah "*data object*", yaitu: "*Objects or information of potential probative value that are associated with physical items.*" Marcella, *op. cit.*, p. 132.

Lebih lanjut Debra Littlejohn juga menejelaskan, bukti digital secara prinsip memang berbeda dengan bukti konvensional, tetapi secara sifat memiliki beberapa persamaan. Contohnya adalah proses pengambilan sidik jari (*fingerprints*) pada kejahatan konvensional yang pada satu saat dapat terlihat (*visible*) dengan mudah, begitu pula bukti digital yang secara fisik terlihat (contohnya: *computer hard disk*). Tetapi disisi lain, sidik jari tidak terlihat begitu saja, melainkan harus melalui suatu proses tertentu hingga sidik jari tersebut dapat terlihat, demikian halnya pada bukti digital yang dalam proses untuk mendapatkannya membutuhkan perangkat keras maupun perangkat lunak tertentu.[199]

2. *Standard Operating Procedures* (SOPs) Terkait Bukti Digital

Aspek terpenting yang harus dimiliki bukti digital agar memiliki kekuatan pembuktian adalah aspek orisinalitas, akurasi, terpercaya dan teruji. Untuk

[199] Shinder, *op. cit.*, p. 546.

mencapai standar tersebut, dalam bekerja penyidik memerlukan adanya standar operasional prosedur (SOP) baku yang menjamin proses perolehan, penyajian, pengujian dan transmisi terhadap bukti digital tetap terjaga akurasi dan orisinalitasnya.

Kepolisian Republik Indonesia (Polri) khususnya Unit Kejahatan Maya (*Cybercrime*) telah memiliki SOP dalam menangani kasus terkait *cybercrime*. Standar yang digunakan oleh Polri mengacu pada standar Internasional yang telah banyak digunakan lembaga kepolisian diberbagai negara, termasuk digunakan oleh FBI di Amerika Serikat.[200]

Terkait dengan tujuan dibuatnya SOP, FBI dalam *Website*-nya mengutip hasil "*G8 Proposed Principles For The Procedures Relating To Digital Evidence*" menjelaskan sebagai berikut.

> *In order to ensure that digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system. Standard Operating Procedures (SOPs) are documented quality-control guidelines that must be*

[200] Hasil wawancara dengan Kepala Unit V *Information* dan *Cyber Crime* Badan Reserse Kriminal Mabes Polri Komisaris Besar Petrus Reinhard Golose tanggal 16 April 2007.

supported by proper case records and use broadly accepted procedures, equipment, and materials.[201]

Adapun karaktreistik standar dari dibentuknya SOP terhadap penanganan bukti digital yang telah dikembangkan oleh International Organization of Computer Evidence (IOCE) yang merupakan standar Internasional adalah:

1. *Consistency with all legal systems;*
2. *Allowance for the use of a common language;*
3. *Durability;*
4. *Ability to cross international boundaries;*
5. *Ability to instill confidence in the integrity of evidence;*
6. *Applicability to all forensic evidence; and*
7. *Applicability at every level, including that of individual, agency, and country.*[202]

Dapat dijelaskan berdasarkan kutipan tersebut, SOP terhadap bukti digital dikembangan untuk konsisten terhadap berbagai sistem hukum yang ada di dunia saat ini, menggunakan bahasa yang mudah dipahami, dapat digunakan untuk jangka waktu yang lama, kemampuan untuk digunakan lintas batas negara, meningkatkan kepercayaan terhadap integritas penggunaan bukti digital, dapat diterapkan dalam

---

[201] "Digital Evidence: Standards and Principle," <http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm#Definition>, diakses 25 Juni 2007.

[202] http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm#International

berbagai teknik forensik digital, dapat digunakan dalam berbagai tingkat baik individu, biro serta negara.

Terkait dengan SOP, terdapat beberapa prinsip SOP terkait penanganan bukti digital. Prinsip ini diakui sebagaian besar organisasi ahli forensik computer dan ahli teknis lainnya, adapun prinsip tersebut sebagai berikut.

1. Bukti digital orisinal secepatnya harus mendapat perlindungan dari negara terdekat dimana bukti digital tersebut ditemukan.[203] Dalam kasus *Website* Al-Anshar, bukti digitalnya terdapat di dua negara, yaitu Jerman sebagai tempat *domain name* Al-Anshar terdaftar dan negara Inggris tempat dimana dokumen HTML *Website* tersebut tersimpan. Dengan demikian, atas permintaan pemerintah Indonesia kedua negara tersebut dapat bertindak untuk menyimpan bukti digital terkait *Website* Al-Anshar tersebut.

   Mengenai bukti lintas negara (*transnational evidence*) semacam ini, Perserikatan Bangsa Bangsa pada 1995, yaitu pada kongres kedelapan mengeluarkan resolusi berjudul "*United Nations Manual on the Prevention and*

[203] Shinder, *op. cit.*, p. 552.

Control of Computer-Related Crime" yang antara lain isinya mengatur mengenai kerjasama internasional dalam penanganan kejahatan berbasis computer termasuk di dalamnya terkait dengan *transnational evidence*.[204]

2. Apabila berdasarkan bentuk dan sifatnya dimungkinkan untuk mengambil salinan (*copy*) terhadap citra bukti digital yang orisinal agar dalam pemeriksaan lebih lanjut yang digunakan adalah hasil salinan tersebut dan bukti digital yang orisinal tetap terjaga integritasnya.[205] Sebagai contoh, dalam kasus Al-Anshar perlu dilakukan penyalinan terhadap hard disk pada *Webhosting*. Penyalinan disini tidak hanya menyalin data atau dokumen, tetapi juga termasuk menyalin secara *bitstream* yang artinya menyalin satu per satu *bit* data dan *boot record* yang ada pada *hard drive*. Hasilnya, salinan tersebut akan berupa *clone* yang merupakan *copy digital evidece* dari *hard drive* yang berupa *original evidence*. Proses penyalinan *bit*

---

[204] International Review of Criminal Policy, *United Nations Manual on the Prevention and Control of Computer-Related Crime*, <http://www.uncjin.org/Documents/EighthCongress.html>, diakses 20 Juni 2007.

[205] Bruce Middleton, *Cyber crime investigator's field guide* (Florida: CRC Press LCC, 2002), p. 16.

per *bit* memungkinkan ikut tersalinnya juga informasi pada *hard drive* yang telah dihapus dan juga informasi lain yang disembunyikan (*hidden file*).[206] Keahlian teknik komputer diperlukan dalam upaya penyalinan, terutama dalam mencari *computer file* yang telah terhapus.[207]

3. Salinan dari data yang digunakan untuk pemeriksaan harus steril. Artinya media *back up* tersebut tidak pernah digunakan sebelumnya dan media tersebut juga harus bebas dari kemungkinan adanya virus dan *bad sector*.[208]
4. Segala tindakan terkait dengan bukti digital harus selalu terdokumentasi secara detail dan terdapat kejelasan rantai pemeriksaannya pada tiap-tiap acara pemeriksaan.[209] Artinya, setiap akan dilakukan maupun telah dilakukannya pemeriksaan pada bukti digital, segala proses tersebut harus terdokumentasi atau dibuatkan Berita Acaranya. Hal ini sejalan dengan

---

[206] *Ibid.*, p. 22.

[207] Brenner, *op. cit.*, p. 14

[208] Shinder, *op. cit.*

[209] Ibid.

"*Standard and Criteria 1.6*" yang dikeluarkan oleh SWGDE dan IOCE yaitu "*All activity relating to the seizure, storage, examination, or transfer of digital evidence must be recorded in writing and be available for review and testimony*."[210]

Dengan demikian, SOP ini harus digunakan oleh setiap pihak (penyidik) dalam hal melakukan penyitaan atau pengujian terhadap bukti digital. Setiap tindakan tersebut harus tercantum pada SOP dan diikuti bersama.[211]

3. Perolehan Informasi Terkait Bukti Digital Pada *Website* Al-Anshar.net Menggunakan Teknik *Internet Forensic*

Pada sub-bab ini akan diberkan ilustrasi teknik pengumpulan bukti digital pada *Website* Al-Anshar.net berdasarkan SOP yang dikeluarkan oleh IOCE. Penjabaran teknik ini terbatas pada tahapan *Website based forensic*. Artinya, informasi yang diperoleh adalah informasi terkait

---

[210] "FBI Standards and Principles Digital Evidence," < http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm#IOCEIntroduction>, diakses 20 Juni 2007

[211] <http://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf>

secara langsung terhadap website Al-Anshar.net. Apabila dalam teknik forensic yang dilakukan oleh Polri menggunakan perangkat lunak *nCase* 2.08 yang merupakan *proprietary software*, maka pada penulisan ini digunakan adalah *Operation System HELIX V. 3* berbasiskan *free software*.[212] Terdapat beberapa langkah dalam melakukan pengumpulan informasi, adapun langkahnya sebagai berikut.

1. Capturing Web Pages

Langkah pertama dalam melakukan pengumpulan informasi dalam sebuah *Website* adalah "*Capturing Web Pages*". Seperti yang telah dijelaskan dalam sub-bab sebelumnya, kode sumber sebuah *Website* yang ditulis dalam sintak HTML mengandung banyak informasi terkait siapa pembuat *Website*, asal dari si pembuat *Website* dan adanya sintak *link* yang dapat digunakan untuk melakukan pemetaan terhadap keseluruhan *Website* yang saling berkaitan. Dengan melakukan teknik

[212] Perangkat lunak nCase 2.08 dapat diunduh dari *website* http://www.guidancesoftware. Sedangkan, Sistem Operasi (SO) HELIX diperoleh di *website* http://www.e-fense.com/helix/. Informasi terkait perangkat lunak yang digunakan oleh Polri diperoleh berdasarkan wawancara dengan anggota Detasemen Khusus Antiteror 88, bertempat di Pengadilan Negeri Semarang pada tanggal 18 Juni 2007.

"*capturing Web pages*" kita akan memperoleh seluruh dokumen HTML yang disimpan pada sebuah *Web hosting*.[213] Banyak teknik yang dapat digunakan untuk meng-capture sebuah *Website*, salah satunya adalah memanfaatkan fitur "save as" pada Web Browser. Akan tetapi teknik ini memiliki kelemahan, yaitu hasil dokumen HTML yang ter-capture tidak identik dengan dokumen aslinya. Berikut akan berikan contoh.

```
<table width="90%" border="0" align="center" cellpadding="0"
cellspacing="0">
      <tr>
```

Skrip 3.6. Kode sumber asli sebuah *website*

Berikutnya adalah kode sumber *Website* yang telah di-*capture* oleh Web Browser Mozilla Firefox, yang secara otomatis akan mengurutkan penamaan tag <table> menjadi alfabetik dan menambahkan tag <tbody> sebagai awalan dari tag <tr>.

```
<table     align="center"     border="0"     cellpadding="0"
cellspacing="0" width="90%">
<tbody><tr>
```

Skrip 3.7. Contoh HTML Setelah di-*capture* oleh Mozilla

[213] Robert Jones, *Internet Forensics* (United State of America: O'Reilly Publishing, 2005), ch. 5, sc. 1.

Dari kode sumber tersebut terlihat perbedaan. Meskipun, berbeda, secara esensial perbedaan urutan sintak tersebut tidak akan merubah tampilan dari *Website* dan tidak akan mengubah struktur bahasa dari dokumen HTML tersebut. Namun perlu diperhatikan prinsip dasar dari bukti digital adalah adanya kesamaan antara *original digital evidence* dengan *copy digital evidence.* Untuk menghindari adanya perubahan konsistensi data selama proses *capturing Web pages*, sebaiknya menggunakan perangkat lunak bernama "wget", yang secara *default* sudah terpasang dalam sistem operasi berbasis Linux. Adapun perintah yang digunakan untuk memperoleh seluruh *Website* termasuk *link* yang digunakan sebagai berikut.

```
$ wget –mn http://www.anshar.net/

--04:41:53--  http://alanshar.net/
          => `alanshar.net/'
Reusing existing connection to alanshar.net:80.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://alanshar.net/ [following]
--04:41:55--  http://alanshar.net/
          => `alanshar.net/index.html'
Reusing existing connection to alanshar.net:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
```

Skrip 3.8. Perintah untuk meng-*capture Web Pages* secara menyeluruh

2. Melihat Kode Sumber HTML

Dalam pengetikan kode sumber HTML, terkadang beberapa programer menulisnya tidak secara sistematik. Hal tersebut menyebabkan kode sumber dari HTML tersebut tidak mudah untuk dipahami struktur sintaknya. Selain itu format *markup language* dalam HTML terkadang menyebabkan kesulitan dalam membaca konten dari dokumen HTML, karena banyaknya *tag* dan sintak yang digunakan dalam HMTL. Untuk mempermudah membaca konten dari dokumen HTML, sebagian besar produk HTML editor menerapkan perbedaan warna dalam membedakan antara tag HTML dengan konten.[214]

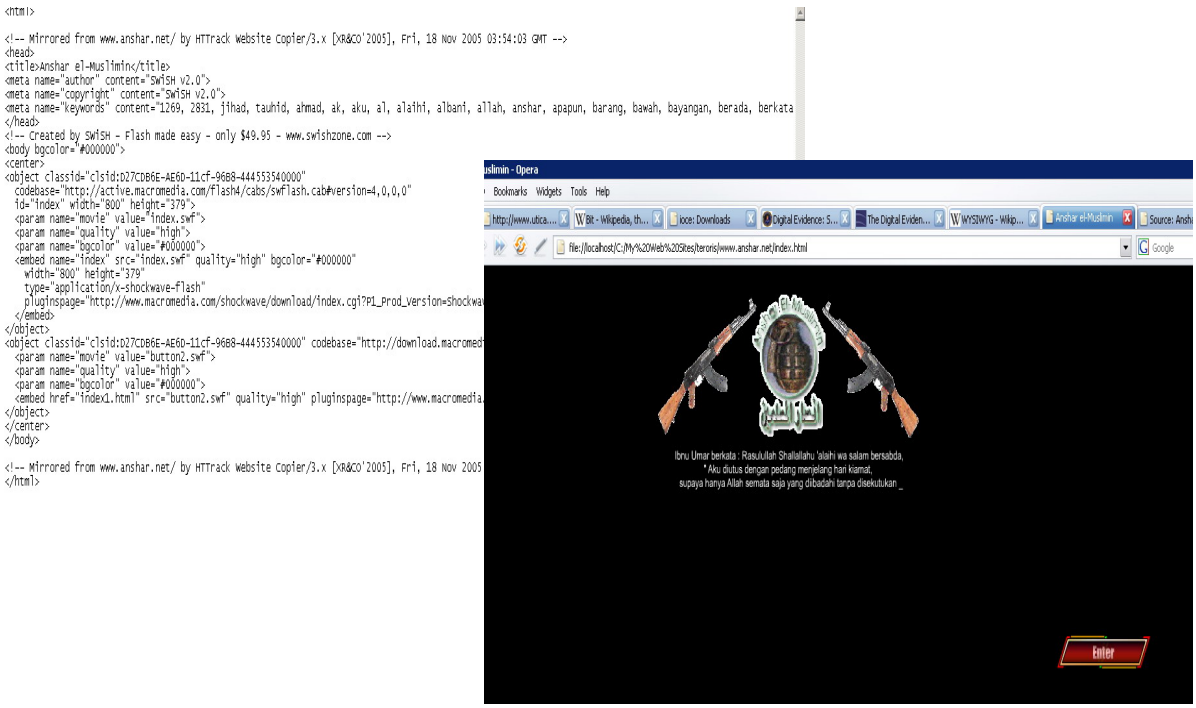
Salah satu perangkat HTML editor yang disarankan dalam melakukan pemeriksaan kode sumber HTML adalah *emacs*.[215] Emacs adalah teks editor berbasis "*What You See Is What You Need*" (WYSIWYN), artinya segala yang tersaji dalam tampilan *emacs* adalah apa yang ingin dibuat oleh si programer. HTML editor lainya yang cukup baik adalah *Macromedia MX*. Program editor ini tidak berbasis WYSIWYN, tetapi berbasis "*What*

---

[214] *Ibid.*, ch. 5, sc. 2.

[215] http://www.gnu.org/software/emacs/

You See Is What You Get" (WYSIWYG), artinya proses pembuatan tampilan HTML langsung secara visual tidak lagi berbasis kode sumber. Berikut akan diperlihatkan perbandingan antara kode sumber berbasis HTML dengan kode sumber yang telah diedit menggunakan editor berbasis WYSIWYG dan dipresentasikan oleh Web Browser.



Gambar 3.3. Tampilan Kode sumber (belakang) dan tampilan presentasi HTML (depan).

Nilai penting dari penelusuran terhadap kode sumber adalah dapat diperoleh informasi yang valid mengenai keseluruhan *Website*, karena apa yang terlihat melalui *Web*

browser belum tentu merupakan informasi yang esensial. Tampilan di Web browser sangat tergantung pada kelengkapan yang dimiliki oleh Web browser tersebut. Tidak semua Web browser memiliki standardisasi fitur.

Sangat dimungkinkan tampilan pada suatu web browser akan berbeda dengan web browser lainnya. Dengan demikian, apabila ingin memperoleh bukti digital dari tindak pidana terorisme pada *Website* Al-Anshar.net sumber perolehannya berada pada kode sumber dokumen HTML pada *Website* tersebut.

3. Melakukan Perbandingan Dokumen HTML

Setelah mendapatkan seluruh dokumen web menggunakan teknik yang telah dibahas pada poin ke-2 yaitu "*capturing web pages*" dan telah dilakukan upaya membaca kode sumber dari *website*, maka langkah selanjutnya adalah mencegah terjadinya perubahan data, nilai, sintak atau *tag* pada dokumen HTML yang akan dilakukan eksaminasi atau pengujian. Langkah ini memiliki tujuan untuk menjaga akuntabilitas dari kode sumber *website* yang akan dijadikan bukti digital. Meskipun, bukti digital yang akan diteliti atau diuji merupakan salinan (*copy digital evidence*), pencegahan

terjadinya perubahaan terhadap bukti digital tersebut tetap perlu dilakukan.

Salah satu cara yang digunakan dalam menguji apakah telah terjadi perubahan data, nilai, sintak atau tag pada dokumen HTML adalah menggunakan perintah “diff” pada Sistem Operasi HELIX. Berikut akan diberikan ilustrasi mengenai perbandingan dokumen HTML. Pada saat pemeriksaan terhadap bukti digital berupa kode sumber *website* yang pertama dengan nama “hello.html” yang memiliki kode sumber sebagai berikut.

```
<HTML>
   <HEAD>
        <TITLE>Canto HTML document</TITLE>
   </HEAD>
        <BODY>
                <P><B>Hello world!</B>
        </BODY>
</HTML>
```

Skrip 3.9. Contoh Kode sumber

Kemudian ketika diperiksa oleh penyidik, perangkat lunak yang digunakan untuk menguji kode sumber menyebabkan terjadinya perubahan tag dan menyebabkan tag <B> dan </B> hilang tanpa diketahui oleh penyidik tersebut. Selanjutnya, penyidik tersebut akhirnya menyadari kalau dokumen dengan nama “hello.html” tersebut mengalami perubahan, akan tetapi ia tidak mengetahui bagian mana dari dokumen tersebut yang

berubah. Solusi dari permasalahan ini adalah menggunakan perintah “diff” sebagai berikut.

```
$ diff hello.html hello2.html
6c6
<            <P><b>Hello world!</b>
---
>            <P>Hello world!
9c9
<
---
>
```

Skrip 3.10. Contoh Perintah diff

Berdasarkan hasil dari perintah “diff” tersebut terlihat jelas data, nilai, sintak atau tag mana yang mengalami perubahan. Hasil perbandingan dua dokumen pada ilustrasi yang diberikan mungkin tidak terlalu memperlihatkan kesulitan dalam mencari data, nilai, sintak atau tag yang berubah dalam suatu dokumen HTML. Hal tersebut disebabkan, baris program HTML yang digunakan sebagai contoh hanya terdiri dari delapan baris. Namun, sebagai contoh yang komplek dapat digunakan dokumen HTML yang berasal dari *website* Al-Anshar.net dengan nama dokumen “tc-1.htm” yang memiliki jumlah program HTML sebanyak 326 baris. Dengan jumlah baris program sebanyak itu, tentu akan menghabiskan waktu apabila dilakukan pemeriksaan baris per baris. Untuk itu, dalam pemeriksaan, penggunaan program

untuk membandingkan perubahan data, nilai, sintak atau tag pada suatu dokumen HTML adalah diperlukan.

4. Analisis Terhadap Server Log Website Al-Anshar.net[216]

Server log adalah sebuah catatan pada *server* yang secara otomatis merekam segala transmisi yang terjadi dari dan menuju *server*.[217] *Server log* pada dasarnya mencatat informasi sebagai berikut.

1. Informasi mengenai *Internet Protocol address* yang melakukan akses terhadap *server*.
2. Informasi waktu berupa tanggal, bulan dan tahun serta jam yang menunjukan kapan akses terhadap *server* dilakukan.
3. Permintaan (*request*) tertentu yang diterima *server* dari pengguna. Permintaan ini dapat berupa dokumen HTML.

---

[216] Analisis ini hanya merupakan ilustrasi belaka untuk menggambarkan proses analisis terhadap *file log* untuk mencari bukti pada website alanshar.net. Penulis tidak memiliki akses secara langsung kedalam *server* alanshar.net yang di-hosting pada *server* openhosting.co.uk. Pihak yang dapat mengakses *file log* website alanshar.net adalah *root* (*system administrator*) pada *web hosting* openhosting.co.uk.

[217] http://en.wikipedia.org/wiki/Server_log

4. Informasi berisi *fingerprints* dari perangkat lunak yang digunakan *user* untuk mengakses *website*.

Untuk mempermudah pemahaman terhadap *server log* akan diilustrasikan sebagai berikut. M. Agung Prabowo melakukan akses terhadap website www.openhosting.co.uk untuk keperluan pendaftaran *hosting*. Ketika ia melakukan akses tersebut, secara otomatis aktifitas tersebut akan tercatat di *log* pada *server* website www.openhosting.co.uk.[218] Contoh dari *server log*-nya, yaitu:

```
202.*.*.* - - [25/Jun/2007:23:02:47 -0400] "GET / HTTP/1.1" 200
44 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4"
```

Skrip 3.11. Contoh *log server*

Server log tersebut dapat dijelaskan sebagai berikut.

1. IP Adress yang digunakan untuk mengakses website adalah 202.*.*.*.
2. Akses kedalam website dilakukan pada tanggal 25 Juni 2007, pada pukul 23:02:47 UTC -0400.

[218] Pada saat M. Agung Prabowo mengentahui website yang dibelinya merupakan website teroris, ia memindahkan *name server* dari ns.open*hosting*.co.uk ke ns.israel-web*hosting*.com. Meskipun demikian, yang dialihkan hanyalah *name server*, sementara seluruh dokumen tetap berada pada server openhosting.co.uk.

3. Perintah permintaan yang dilakukan kepada server adalah “GET / HTTP/1.1”, yang berarti meminta segala berkas HTML yang terdapat para direktori utama aplikasi web. Secara *default* berkas yang akan ditampilkan bernama “index.html”.
4. Perangkat lunak yang digunakan oleh *user* adalah Mozilla yang berjalan pada Sistem Operasi Windows dengan nomor seri Firefox/2.0.0.4.

Apabila telah dapat dipastikan *IP Adress* 202.*.*.* adalah milik M. Agung Prabowo, maka untuk mengetahui lebih lanjut aktifitas yang ia lakukan selama terkoneksi dengan server www.openhosting.co.uk dapat digunakan perintah sebagai berikut.

```
# grep -i 202.*.*.* access_log |grep 'GET /' | more > log.txt
```

Skrip 3.12. Perintah grep

Dengan perintah tersebut, maka akan terbentuk suatu berkas baru bernama “log.txt” yang berisi log aktifitas yang dilakukan oleh pengguna *IP Adress* 202.*.*.*. Catatan tersebut akan mejelaskan aktifitas apa saja yang dilakukan,

berapa lama aktifitas tersebut dilakukan dan apa hasil dari aktifitas yang dilakukan.

Server log pada suatu sistem dapat digunakan untuk membuktikan suatu peristiwa hukum, karena keberadaan suatu arsip (yang dalam hal ini adalah *server log*) adalah dimaksudkan sebagai suatu alat pembuktian yang merekam atau menerangkan suatu informasi tertentu.[219] Dalam kasus Al-Anshar.net ini keberadaan *server log* digunakan untuk membuktikan apakah benar M. Agung Prabowo yang membeli dan meregistrasi web hosting al-anshar.net di website www.openhosting.co.uk.

Berdasarkan uraian mengenai perolehan informasi terkait bukti digital pada website www.anshar.net menggunakan teknik *Internet Forensic* dapat disimpulkan sebagai berikut.

1. Keberadaan dokumen HTML yang diperoleh menggunakan teknik "*capturing web pages*",
2. Usaha untuk meneliti kode sumber HTML dengan mempelajari baris per baris bahasa progra HTML dan *server log* pada website www.openhosting.co.uk

[219] Makarim, *op. cit.*, hal. 237.

terkait dengan akses dan aktifitas yang dilakukan oleh M. Agung Prabowo.

Merupakan suatu informasi yang dihasilkan oleh suatu sistem informasi elektronik yang bersifat netral, sepanjang sistem tersebut berjalan baik tanpa gangguan, sehingga *input* dan *output* yang dihasilkan oleh mesin server website www.openhosting.co.uk berjalan sebagaimana mestinya.[220] Dengan demikian, seharusnya kode sumber HTML dan *server log* yang diperoleh dan dihasilkan sistem website www.openhosting.co.uk selama telah terjamin berjalan sebagaimana mestinya, maka sepanjang tidak dibuktikan lain, semestinya dapat diterima dan memiliki nilai pembuktian.[221]

4. Otentifikasi Bukti Digital Melalui Teknik Enkripsi

Kata kriptografi berhasal dari bahasa Yunani, *kryptos* yang berarti tersembunyi dan *graphein* yang berarti tulisan. Sehingga secara etimologi kriptografi adalah tulisan tersembunyi. Enkripsi merupakan bagian dari kriptografi merupakan proses pengaburan informasi berupa teks yang

[220] *Ibid.*, hal. 241.

[221] Ibid.

semula dapat terbaca (*plaintext*) kemudian membuat informasi tersebut tidak dapat dibaca tanpa kemampuan khusus atau alat tertentu (*chipertext*).[222]

Teknologi enkripsi bukan merupakan sebuah teknologi baru pada peradaban manusia. Terbukti teknologi enkripsi ini telah banyak digunakan pada masa lalu. Salah satu yang telah ditemukan antara lain penggunaan metode enkripsi tertua pada jaman Julius Caesar yang digunakan untuk berkomunikasi dengan panglima perang kerajaan dikenal sebagai *caesar cipher*.[223]

Selain itu, penggunaan enkripsi sejak lama tersebut didukung dengan ditemukannya dokumen yang tersandi berjudul *Einige Originalschriften des Illuminaten Ordens* oleh polisi Bavaria yang ditulis oleh Baron Xavier von Zwack kepada Robespierre pada tahun 1784.[224] Bukti terakhir dan yang paling terkenal adalah digunakannya mesin *Enigma* oleh tentara Nazi pada perang dunia ke-II. Mesin ini merupakan

---

[222] Jeff Tyson, "How Encryption Works," <http://computer.howstuffworks.com/encryption1.htm>, di akses 20 Juni 2007

[223] http://library.thinkquest.org/C0126342/ceaser.htm

[224] http://freemasonry.bcy.ca/anti-masonry/illuminatitexts.html

salah satu mesin pertama yang memanfaatkan mekanisme *rotor* dalam melakukan enkripis serta dekripsi.[225]

Seiring berjalannya waktu, perkembangan teknologi enkripsi juga semakin pesat. Pada saat awal digunakannya teknologi ini, proses enkripsi data cukup menggunakan kertas dan pena (*paper-based encryption*) dan sekarang proses pengenkripsian data telah menggunakan komputer (*computer-based encryption*). Karena proses enkripsi tidak lagi merupakan upaya memeroses karakter tetapi sudah memeroses aliran *bit* (*bit stream*) yang merupakan bagian esensial dalam proses komputasi. Selain itu, implementasi atau penerapan enkripsi di dunia komputer juga telah menyentuh banyak protokol jaringan seperti *secure http* (https), *secure ftp* (sftp), *secure shell* (SSH) dan lainnya.

Prinsip dasar dari bekerjanya enkripsi dapat dijelaskan sebagai berikut. Operasi enkripsi berjalan pada sebuah plaintext (P) dengan fungsi enkripsi (E) yang menggunakan sebuah *key*/kunci (k) dan menghasilkan sebuah ciphertext (C) yang dinyatakan dengan persamaan :

$$C = E_k(P)$$

---

[225] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (New York: John Wiley & Sons, 1996), p. 15.

Fungsi tersebut tentu dilakukan oleh pengirim pesan. Sedangkan di sisi penerima pesan, ia harus bisa membaca informasi tersebut dengan cara melakukan operasi dekripsi yang menggunakan fungsi (D) yang bekerja pada ciphertext (C) serta menggunakan kunci (k) sehingga dihasilkan sebuah plaintext (P) dan dinyatakan dalam persamaan:

$$P = D_k(C)$$

dua persamaan di atas hanyalah penjabaran proses enkripsi dan dekripsi secara global karena nanti akan muncul bermacam metode enkripsi.

a. Kegunaan Enkripsi dalam Otentifikasi Data

Tujuan digunakannya enkripsi selain menyembunyikan informasi yang terkandung di dalamnya juga digunakan untuk menjaga integritas sebuah informasi pada saat ditransmisikan. Hal ini dimungkinkan karena dengan adanya teknik enkripsi, seluruh informasi akan “digembok” menjadi satu kesatuan. Sehingga apabila ada bagian informasi yang rusak (*file corrupt*), maka “kunci” yang digunakan untuk

mendekripsi akan memberitahu kerusakan informasi tersebut.[226]

Selain itu, dengan metode enkripsi hanya pihak yang berwenang terhadap informasi terenkripsi saja yang dapat membuka serta membaca informasi tersebut. Sehingga, isi dari informasi yang dienkripsi tidak akan bisa disangkal (*non-repudiation*) oleh pihak yang mendekripsi informasi tersebut. Hal ini terkait dengan konsep tanda tangan digital (*digital signature*) pada teknologi enkripsi. Mark Taylor dalam tulisannya yang berjudul *Uses of Encryption: Digital Signatures* mengatakan:

> *digital signatures designed in such a way that the authenticity and integrity of the data to which they are attached can be assured. In essence, the key issues for data which have been signed digitaly are:*
> - *whether those data have been altered between their being signed and being read or received by the intended recipient; and*
> - *whether those data were actually signed by the person by whom the data purport to have been signed or whether the signature attached to them is forged in some way.*[227]

---

[226] Tyson, *op. cit.*

[227] Mark Taylor, *Uses of Encryption: Digital Signatures,* (USA: Sweet & Maxwell Limited and Contributors, 1999), p. 2.

Perlindungan keotentikan suatu dokumen yang menggunakan tanda tangan digital jauh lebih kuat, karena sebuah tanda tangan digital memiliki karakter yang sangat unik dan telah tersandikan (*encrypted*) sehingga kemungkinan ditiru sangat kecil. Hasilnya, dokumen yang ditandatangani (*sign*) menggunakan *digital signature*, akan menjadi dokumen yang identik dengan si pemilik tanda tangan.

Selain perlindungan informasi dan data menggunakan *digital signature*, teknologi enkripsi juga memanfaatkan fungsi *fingerprints* yang dihasilkan oleh *Message-Digest algorithm* 5 (MD5).

b. *Message-Digest algorithm* 5 (MD5) sebagai standardisasi enkripsi dan otentifikasi pada bukti digital

Message Digest 5 (MD5) merupakan salah satu jenis fungsi *hash* satu arah (*one-way hash function*) yang dikembangkan oleh Ron Rivest.[228] *Hash function* diartikan sebagai "*reproducible method of turning some kind of data into a (relatively) small number that may serve as a*

[228] http://tools.ietf.org/html/rfc1321

digital "fingerprint" of the data."[229] Artinya, *hash* function mereproduksi sebagian kecil dari data untuk digunakan sebagai "sidik jari" atau identitas suatu data. Fungsi *hash* satu arah merupakan suatu fungsi yang digunakan untuk mengecek integritas atau keaslian sebuah data.[230]

Keunikan fungsi ini dari algoritma enkripsi yang lain adalah fungsi ini hanya membutuhkan *input* sebuah pesan tanpa perlu menggunakan sebuah kunci (*key*) untuk mendapatkan nilai *hash* yang nantinya akan dicocokkan dengan nilai *hash* yang asli.

MD5 sendiri merupakan kelanjutan proyek *Message Digest* 4 yang telah dikembangkan sejak Oktober 1990. Tujuan dikembangkannya MD4 menjadi MD5 antara lain sebagai berikut.

1. Keamanan. Secara perhitungan matematis tidak dimungkinkan untuk mendapatkan dua pesan berbeda yang memiliki nilai *hash* yang sama.
2. Keamanan Langsung. Keamanan MD5 tidak didasarkan pada suatu asumsi, seperti kesulitan pemfaktoran.

---

[229] "General purpose *hash* function algorithms (C/C++/Pascal/Java/Python/Ruby)," http://www.partow.net/programming/*hash* functions/index.html.

[230] http://www.cryptography.com/cnews/*hash*.html

3. Kecepatan. MD5 sesuai untuk diimplementasikan dengan perangkat lunak berkecepatan tinggi, karena berdasar pada sekumpulan manipulasi operasi data 32-bit.
4. Kesederhanaan dan keringkasan. MD5 Sederhana tanpa struktur atau program yang kompleks.[231]

Fungsi *hash* satu arah (H) beroperasi pada sebuah pesan (M) dengan panjang sembarang, dikarenakan ketaktentuan panjang sebuah pesan. Fungsi ini harus menghasilkan sebuah output (h) yang harus sama panjanganya (length(h_1) = length(h_2) = ... = length(h_n)) agar bisa dilakukan proses pengecekan keaslian pesan tersebut.Sifat fungsi *hash* harus memenuhi syarat sebagai berikut:

1. Diberikan pesan/file (M), dan harus mudah menghitung H(M) = h
2. Diberikan output (h), sehingga sangat sulit atau mendekati ketidakmungkinan mendapatkan M sedemikian hingga H(M) = h
3. Diberikan pesan/file (M), sehingga sangat sulit

[231] http://www.cryptodox.com/MD5

atau mendekati ketidakmungkinan mendapatkan M’ yang memiliki nilai *hash* yang sama dengan M sedemikian hingga H(M) <> H(M’).Jika terjadi H(M) = H(M’) maka telah terjadi tabrakan (*collision*)

4. Sangat sulit atau mendekati ketidakmungkinan mendapatkan dua pesan M dan M’ sedemikian hingga H(M) = H(M’)

Sepintas, poin ketiga dan keempat di atas terlihat sama. Tetapi yang dimaksud poin ketiga di atas adalah sudah ada pesan tertentu yaitu M, kemudian kita mencari pesan lain M’ sedemikian hingga H(M)=H(M’). Sedangkan, pada poin keempat, kita mencari dua pesan sembarang yang memenuhi H(M)=H(M’).

c. Implementasi Penggunaan Teknik Enkripsi dan *MD5 Hases* dalam Kasus Website Anshar.net

Berikut akan diilustrasikan bagaimana teknik enkripsi dan MD5 *hash sums* dapat digunakan sebagai perlindungan nilai otentifikasi dan integritas website www.anshar.net. Pada sub-bab sebelumnya telah dijelaskan mengenai tata cara perolehan seluruh dokumen HTML pada website www.anshar.net menggunakan perintah “wget –m www.anshar.net”. Apabila

perintah tersebut telah selesai dan seluruh dokumen yang berada di dalam website www.anshar.net telah terunduh, maka dalam *hard drive* akan terbentuk direktori baru dengan nama www.anshar.net.

Untuk keperluan pemberian tanda tangan digital dan proses enkripsi serta mencari nilai *hash* dari direktori www.asnhar.net tersebut, akan dilakukan proses pemberkasan terkompresi menggunakan perangkat lunak “tar” dan “gzip”.[232] Berikut perintah melakukan pemberkasan terkompresi terhadap direktori www.anshar.net, kemudian melihat hasil dari kompresinya.

```
$ tar –cf www.anshar.net.tar www.anshar.net/

$ gzip www.anshar.net.tar

$ ls –al

drwxrwxr-x  3 zka zka   1024 Jun 26 15:06 ./
drwxr-xr-x 44 zka zka   2048 Jun 26 14:18 ../
drwxrwxr-x 14 zka zka   1024 Jun 26 14:54 www.anshar.net/
-rw-rw-r--  1 zka zka 276910 Jun 26 15:04 www.anshar.net.tar.gz
```

Skrip 3.13. Perintah kompresi

Hasil perintah tersebut memperlihatkan saat ini telah terbentuk dokumen baru bernama “www.anshar.net.tar.gz”.

[232] Perangkat lunak “tar” dan “gzip” secara otomatis sudah ter-install dalam setiap distribusi Sistem Operasi berbasis GNU/Linux. Untuk aplikasi sejenis pada Sistem Operasi Windows dapat menggunakan perangkat lunak “WinZip” atau “WinRar”.

Ekstensi *.tar.gz dibelakan www.anshar.net menandakan kalau direktori tersebut telah diberkaskan dan dikompresi. Langkah selanjutnya adalah memberikan tanda tangan digital kepada dokumen “www.anshar.net.tar.gz” tersebut. Tanda tangan digital yang digunakan dalam ilustrasi ini adalah tanda tangan digital unit *cybercrime* “Kepolisian Republik Indonesia”. Proses enkripsi pada berkas terkompresi tersebut dilakukan menggunakan perangkat lunak Gnu Privacy Guard (GPG), dengan tingkat besaran kunci 2048 bits. Adapun perintah enkripsinya sebagai berikut.

```
$ gpg –e –a www.anshar.net.tar.gz > www.anshar.net.tar.gz.asc

Enter the user ID.  End with an empty line: Kepolisian Republik
Indonesia

Current recipients:
2048g/D7DAC941 2007-06-26 "Kepolisian Republik Indonesia (Polri)
<unitcybercrime@polri.go.id>"

$ ls –al

drwxrwxr-x  3 zka zka   1024 Jun 26  ./
drwxr-xr-x 44 zka zka   2048 Jun 26  ../
drwxrwxr-x 14 zka zka   1024 Jun 26  www.anshar.net/
-rw-rw-r--  1 zka zka 276909 Jun 26  www.anshar.net.tar.gz
-rw-rw-r--  1 zka zka 375901 Jun 26  www.anshar.net.tar.gz.asc
```

Skirp 3.14. Perintah Enkripsi

Saat ini berkas terkompresi www.anshar.tar.gz telah menjadi berkas terenkripsi dan telah dilekatkan tanda tangan “penyidik” dari “Kepolisian Republik Indonesia”. Dengan demikian, pihak yang dapat melakukan pemeriksaan

terhadap berkas tersebut hanyalah pihak yang memiliki kata kunci untuk membuka dokumen terenkripsi tersebut. Berkas www.anshar.net.tar.gz.asc ini sebaiknya disimpan pada tempat yang aman untuk dijadikan penguji berkas salinannya yang digunakan untuk pemeriksaan. Selanjutnya, untuk mencegah adanya perubahan integritas dari berkas www.anshar.net.tar.gz dan www.anshar.net.tar.gz.asc, keduanya akan diperiksa *hash sums*-nya.

```
$ md5sum www.anshar.net.tar.gz
  d0108b88f99075acfc0df017364ef265  www.anshar.net.tar.gz
$ md5sum www.anshar.net.tar.gz.asc
  c20084ec65892a6389ad3d8d5d2c921b  www.anshar.net.tar.gz.asc
```

Skirp 3.15. Perintah *Check Sums*

Terlihat dalam gambar tersebut berkas www.anshar.net.tar.gz memiliki *hash sums* “d0108b88f99075acfc0df017364ef265” dan berkas www.anshar.net.tar.gz.asc memiliki *hash sums* “c20084ec65892a6389ad3d8d5d2c921b”.

Sebagai pengujian, telah dilakukan perubahan satu karakter yaitu dengan mengubah huruf “i” pada kata “link” menjadi huruf “a” sehingga kata tersebut menjadi “lank”

pada baris keenam dokumen bernama “cntnn.html” yang berada dalam direktori www.anshar.net/. Direktori tersebut dijadikan berkas terkompresi dan dienkripsi menggunakan tanda tangan digital pihak lain, kemudian dilakukan pengecekan ulang terhadap *output* dari *hash sums*-nya. Hasilnya sebagai berikut.

```
$ md5sum www.anshar.net.tar.gz

d2ba60d7deb743061322ec2786a5826d  www.anshar.net.tar.gz

$ md5sum www.anshar.net.tar.gz.asc

86bc22d0eb6b3260a8654773ca2fa82a  www.anshar.net.tar.gz.asc
```

Skirp 3.16. Perintah *Check Sums* Untuk Perbandingan

Hasil dari *md5ceksum* berkas tersebut ternyata berbeda, meskipun perubahan yang dilakukan hanya terhadap satu huruf pada satu dari ratusan dokumen yang terdapat dalam direktori www.anshar.net.[233] Dengan demikian, proses menjadikan suatu berkas terkompresi kemudian dienkripsi dapat menjaga otentifikasi serta integritas dari

[233] Jika pengujian dilakukan lebih lanjut menggunakan teknik perbandingan yang telah dijelaskan dalam sub-bab sebelumnya, yaitu menggunakan perintah “diff” pada kedua berkas www.anshar.net.tar.gz.asc, maka akan terlihat terjadi perubahan seluruh struktur berkas, tidak hanya satu baris. Hal ini disebabkan karena berkas tersebut sesungguhnya adalah berkas terenkripsi yang dilekatkan *digital signature* sehingga sifatnya sangat unik dan identik dengan pemilik digital signature tersebut. Artinya, apabila suatu berkas terenkripsi yang ditandatangani oleh dua *digital signature* yang berbeda maka akan mengasilkan dua berkas yang sama sekali akan berbeda.

keseluruhan dokumen tersebut, sehingga keabsahan dokumen tersebut tidak dapat lagi disangkal dan seharusnya dapat diterima sebagai bukti otentik.

BAB IV

ANALISIS ALAT BUKTI DALAM KASUS *CYBER TERROISM* (*WEBSITE* ANSHAR.NET)

A. Kasus Posisi

Situs www.anshar.net yang dibuat Juni-Agustus 2005 atas permintaan Noordin M Top berisi tentang penjelasan soal jihad yang diyakini oleh kelompok Noordin M Top dan Dr. Azahari.[234] Halaman depannya bergambar dua pucuk senapan dan granat. Dalam situs tersebut terdapat menu yang berisi wasiat dari Mukhlas alias Ali Ghufran.[235] Salah satu

---

[234] "Situs 'Teroris' Anshar.Net Akan Diblokir Polri,"<http://jkt.detiknews.com/index.php/detik.read/tahun/2005/bulan/11/tgl/22/time/154522/idnews/483936/idkanal/10>, diakses 22 September 2005.

[235] Terdapat lima belas halaman *Website* yang berisi wasiat dari Mukhlas, yaitu halaman "mkhls.htm" hingga "mkhls15.htm".

pernyataan dalam wasiat itu adalah mereka mengakui dirinya sebagai teroris.

Selanjutnya, situs tersebut menerangkan bagaimana cara kerja teroris mengebom. Dalam pemaparan, dijelaskan perumpamaan tempat keramaian, seperti kawasan wisata, mal, restoran dan jalan tol. Lokasi yang dicontohkan adalah beberapa tempat keramaian di Jakarta.[236] Tidak hanya cara peledakan bom, situs tersebut mengulas pula cara penembakan dan penyerangan dengan granat.[237] Berdasarkan penyelidikan kepolisian, polisi akhirnya menangkap dua tersangka *cyber terorism*, yang selama ini membantu pengelolaan jaringan terorisme melalui internet. Keduanya adalah Agung Setyadi dan Mohammad Agung Prabowo di Semarang, Jawa Tengah, yang ditangkap pada 12 Agustus dan 16 Agustus 2006.[238]

Fokus pada penulisan ini adalah pada kasus M. Agung Prabowo yang terbukti membuat *Website* www.anshar.net.[239] Mohammad Agung Prabowo alias Max Fiderman alias Ahmad alias

---

[236] Informasi terkait dengan tata cara penembakan, target lokasi dan cara melarikan diri terdapat pada dokumen HTML tc.htm, tc-1.htm dan tc-2.htm.

[237] www.metrotvnews.com/berita.asp?id=40825

[238] http://www.suaramerdeka.com/harian/0608/24/nas02.htm

[239] www.suaramerdeka.com/harian/0706/21/nas14.htm

Bebek-bebekan (Agung) merupakan mahasiswa Fakultas Teknik Elektro Universitas Semarang yang memiliki pemahaman terhadap teknik *carding,* dan *cracking.* Perkara yang menimpa Agung berawal dari hubungan Agung dengan Abdul Azis atau Qital (Terpidana Kasus Bom Bali II), Agung Setyadi (Terpidana terorisme) dan Imam Samudra (Terpidana mati Kasus Bom Bali I). Berdasarkan keterangan Kepala Unit V *Information* dan *Cyber Crime* Badan Reserse Kriminal Mabes Polri Komisaris Besar Petrus Reinhard Golose, Imam masih sempat mengendalikan jaringannya dengan seperangkat *notebook* saat masih ditahan di Lembaga Permasyarakatan Krobokan di Denpasar, Bali. Menurut Petrus, *notebook* tersebut dikirim oleh suruhan Imam, yaitu Agung Setyadi alias Pakne alias Salaful Jihad melalui jasa kurir Titipan Kilat (TIKI) ke alamat salah seorang sipir penjara. Sipir tersebut lalu menyampaikannya kepada Imam di sel penjaranya.[240]

Hubungan yang dilakukan Agung dengan Abdul Aziz tersebut dilakukan pertama kali melalui *chatting* pada Mei

---

[240] "Imam Samudra Sempat Kendalikan Jaringan Terorisme dari Penjara," <http://www.kompas.com/ver1/Nasional/0608/23/183643.htm>, diakses 25 Agustus 2006.

2005 dengan menggunakan perangkat lunak *International Relay Chat* (mIRC)di *channel* #ahlussunnah dan *channel* #cafeislam server *dal.net*.[241] Selama *chatting,* Agung memberikan penjelasan tentang *hacking, carding,* dan fa'i (harta rampasan). Selain itu, Agung membantu membuat tutorial tentang *SQL Injection* melalui IRC oleh Qital dan Imam. Pada Juni 2005, Noordin M. Top dan Abdul Hadi meminta Qital membuat *Website* www.anshar.net tentang jihad dengan tujuan untuk dipublikasikan melalui Internet.

Peran Agung dalam *Website* www.anshar.net adalah membantu Qital untuk mendaftarkan domain dan hosting www.anshar.net. Agung pula yang melakukan *carding* untuk pembayaran pendaftaran tersebut serta menyerahkan *username* dan *passwordnya* kepada Qital. Dengan demikian, dapat diduga *Website* tersebut dapat disalahgunakan untuk melakukan kejahatan.[242]

---

[241] "Bertemu di Dunia Maya, Berakhir di Penjara," <www.sinarharapan.co.id/berita/0706/21/nas04.html>, diakses 21 Juni 2007.

[242] "Max Bukan Jaringan Noordin," <http://www.suaramerdeka.com/harian/0703/27/nas17.htm>, diakses 10 Juni 2007

Website www.anshar.net merupakan *Website* terorisme pertama di Indonesia yang memuat materi sebagai berikut.

a. Kajian Manhaj. Kajian Manhaj ini merupakan wasiat Muklas (Ali Gufron) dan wasiat ulama lain dan beberapa artikel tentang jihad.
b. Askariyah. Askariyah merupakan taktik dan strategi perang meliputi gambar-gambar di jalan dengan cara memanfaatkan antrian mobil di pintu tol, kemacetan, *shopping mall,* pusat hiburan, pusat olahraga, hotel, dan sebagainya.
c. Mutafajjrot. Mutafajjrot merupakan teori tentang bahan peledak.
d. Silah. Silah merupakan teori persenjataan yang seluruhnya bersumber dari Noordin M. Top.

Jumlah keseluruhan dokumen HTML yang terdapat dalam *Website* www.anshar.net adalah tiga puluh satu dokumen. Sedangkan, total seluruh berkas dalam *Website* tersebut adalah seratus empat puluh enam berkas dan terdapat dua belas direktori (*folder*).

Agung Prabowo diduga membantu pelaksanaan terorisme di Indonesia karena Agung melakukan hal-hal sebagai berikut.

1. Sebagai Mahasiswa Fakultas Teknik Elektro Universitas Semarang, Semarang, yang mampu melakukan *carding*, *cracking*, dan *hacking*, Agung merupakan pihak yang selama ini banyak memberikan bimbingan teknologi kepada Agung Setyadi dan Abdul Aziz alias Qital (tersangka Bom Bali II).
2. Agung diduga membantu Imam yang diawali dari *chatting* di provider MiRC melalui channel #cafeislam dan #ahlussunah dengan Imam.
3. Agung berperan pula dalam penggarapan situs www.anshar.net, yang didesain Qital atas permintaan Noordin M Top.
4. Agung mendaftarkan hosting situs www.anshar.net di www.openhosting.co.uk (Inggris) dengan biaya 300 poundsterling atas permintaan Qital.
5. Agung lalu mendaftarkan domainnya di www.joker.com (Jerman) dengan biaya 60 dollar Amerika.
6. Atas kemampuan *carding*, *cracking*, dan *hacking*, Agung diduga membantu terorisme mendapatkan dana, sehingga pencarian dana untuk terorisme beralih ke cara dengan menggunakan *cyber crime.*

Atas perbuatan tersebut, dalam perkara dengan Nomor Register Perkara 84/PID/B/2007 PN SMG, Agung diancam Pasal 13 huruf c Peraturan Pemerintah Pengganti Undang-undang nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme *jo.* Pasal 1 Undang-undang Republik Indonesia Nomor 15 Tahun 2003 Tentang Penentapan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme. Bunyi Pasal 13 huruf c Undang-undang nomor 1 Tahun 2003 sebagai berikut.

> Setiap orang yang dengan sengaja memberikan bantuan atau kemudahan terhadap pelaku tindak pidana terorisme, dengan:
>
> a. ...
> b. ...
> c. menyembunyikan informasi tentang tindak pidana terorisme

Pada Rabu, 20 Juni 2007 lalu, Agung Prabowo divonis tiga tahun penjara oleh majelis hakim dalam sidang di Pengadilan Negeri Semarang. Vonis terhadap Agung lebih ringan lima tahun dari tuntutan jaksa yang menuntut delapan tahun. Dalam pembacaan vonisnya, hakim ketua Sucipto SH mengatakan, Agung secara sah dan meyakinkan bersalah

melakukan tindak pidana teroris. Terdakwa secara sah dan meyakinkan melanggar Pasal 13 huruf C Perpu Nomor 1 Tahun 2002 jo UU 15/2003 tentang Pemberantasan Tindak Pidana Terorisme. Agung dinilai pula dengan sengaja memberikan kemudahan terhadap pelaku tindak teroris. Adapun barang bukti yang digunakan dalam kasus ini berupa:

1. Digital MP3 *player* merek genesis dengan kapasitas 256 MB warna hitam;
2. *Bluetooth* USB warna hitam;
3. *Telepon seluler merek Sony Ericsson T 610 warna biru imei 35198800695471-4;*
4. SIM *card* IM3 nomor 6221114060561805 nomor +62815640555516;
5. SIM *card* matrix warna biru dengan kapasitas 64 kb nomor 89620100000095451959, nomor telepon +628157702037;
6. Satu unit *hard disk* merek Seagate tipe barracuda ATA IV, model ST 3200 11 A, kapasitas 20 GB, nomor seri 3HT4HM8;
7. Satu buah kotak CD; dan
8. Dua buku tabungan mahasiswa Bank Negara Indonesia (BNI) atas nama Mohammad Agung Prabowo nomor 33173102.

B. Analisis Alat Bukti Pada Kasus Anshar.net Berdasarkan Undang-undang Nomor 15 Tahun 2003

Pembuktian merupakan proses acara pidana yang memegang peranan penting dalam pemeriksaan sidang di pengadilan. Melalui pembuktian inilah ditentukan nasib terdakwa, apakah ia bersalah atau tidak.[243] Undang-undang No. 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme selain mengatur tentang pidana material yaitu tentang macam pidana yang diklasifikasikan sebagai terorisme atau unsur tindak pidana terorisme juga mengatur aspek formil atau acara dari pidana terorisme tersesebut.

Undang-undang Nomor 15 Tahun 2003 dalam hal acara pembuktian mengatur penggunaan alat bukti tersendiri untuk digunakan pada saat suatu kasus terkait peristiwa terorisme. Dalam kasus, M. Agung Prabowo di pidana karena melakukan tindak pidana sebagaimana diatur dalam Pasal 13 huruf C Undang-undang Nomor 15 Tahun 2003. Dengan demikian dalam kasus ini dipergunakan ketentuan yang diatur oleh

---

[243] Prints, *op. cit.*, hal. 105

Undang-undang Nomor 15 Tahun 2003, termasuk proses acara pembuktian dan penggunaan alat bukti.

Alat bukti dalam tindak pidana terorisme sebagai mana diatur dalam Undang-undang Nomor 15 Tahun 2003 terdapat pada Pasal 27, yaitu sebagai berikut.

> Alat bukti pemeriksaan tindak pidana terorisme meliputi:
> 1. alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana;
> 2. alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan
> 3. data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada :
>   1) tulisan, suara, atau gambar;
>   2) peta, rancangan, foto, atau sejenisnya;
>   3) huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.

Berdasarkan Pasal 27 Undang-undang Nomor 15 Tahun 2003 tersebut terlihat Undang-undang Nomor 15 Tahun 2003 menerapkan dua jenis alat bukti, yaitu alat bukti yang terdapat dalam Hukum Acara Pidana (merujuk pada KUHAP) dan alat bukti yang diatur secara khusus dalam Undang-undang ini. Untuk menganalisis penggunaan alat bukti dalam kasus

M. Agung Prabowo ini, perlu lebih lanjut dijabarkan mengenai alat bukti yang digunakan dalam kasus ini untuk dilihat apakah penggunaan alat bukti dalam kasus M. Agung Prabowo telah sesuai dengan pengaturan yang terdapat dalam KUHAP serta Undang-undang Nomor 15 Tahun 2003.

Pasal 27 ayat (1) Undang-undang Nomor 15 Tahun 2003 menjelaskan “Alat bukti pemeriksaan tindak pidana terorisme meliputi alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana”. Alat bukti yang diatur oleh Hukum Acara Pidana terdapat ketentuannya di dalam Pasal 184 KUHAP, yaitu:

a. keterangan saksi
b. keterangan ahli
c. surat
d. petunjuk
e. keterangan terdakwa.[244]

Dalam suatu tindak pidana, kelima alat bukti tersebut tidak selamanya harus ada, karena berdasarkan Pasal 183 KUHAP, minimal alat bukti yang diperlukan dalam menentukan seorang terdakwa bersala terhadap suatu tindak pidana adalah dua alat bukti, dan dari dua alat bukti tersebut hakim memperoleh keyakinan benar terdakwa yang melakukan

[244] Indonesia (b), *op. cit.*, ps 184.

tindak pidana tersebut. Merujuk pada Surat Tuntutan (*Requisitor*) No. Reg. Perk. PDM-376/SEMAR/Ep.2/XII/2006, alat bukti yang digunakan dalam kasus M. Agung Prabowo (No. Reg 84/PID/B/2007 PN SMG) adalah keterangan saksi, keterangan ahli, keterangan terdakwa dan petunjuk. Adapun penjelasan lebih lanjut sebagai berikut.

1. Keterangan Saksi

Pada umumnya, alat bukti keterangan saksi merupakan alat bukti yang paling utama dalam perkara pidana. Hampir semua pembuktian perkara pidana selalu bersandar kepada pemeriksaan keterangan saksi. Sekurangnya di samping dengan alat bukti lain, masih selalu diperlukan pembuktian dengan alat bukti keterangan saksi.[245]

Berdasarkan Pasal 1 angka 20 KUHAP, yang dimaksud dengan saksi adalah sebagai berikut.

> Keterangan saksi adalah salah satu alat bukti dalam perkara pidana yang berupa keterangan dari saksi mengenai suatu peristiwa pidana yang ia dengar

[245] Harahap, *op. cit.,* hal. 286.

sendiri, ia lihat sendiri, dan ia alami sendiri dengan menyebut alasan dari pengetahuannya itu.[246]

Suatu keterangan saksi dapat bernilai sebagai alat bukti apabila saksi tersebut memenuhi persyaratan sebagai mana telah dijelaskan oleh Pasal 1 angka 20 KUHAP, yaitu suatu peristiwa pidana yang saksi lihat sendiri, saksi dengar sendiri dan saksi alami sendiri serta menyebut alasan dari pengetahuannya itu. Dengan demikian setiap keterangan saksi di luar apa yang didengarnya sendiri dalam peristiwa pidana yang terjadi atau di luar yang dilihat atau dialaminya dalam peristiwa pidana yang terjadi, keterangan yag diberikan di luar pendengaran, penglihatan atau pengalaman sendiri mengenai suatu peristiwa pidana yang terjadi, tidak dapat dijadikan dan dinilai sebagai alat bukti.[247]

Lebih lanjut mengenai keterangan saksi diatur dalam Pasal 185 KUHAP, yang antara lain menjelaskan keterangan saksi sebagai alat bukti ialah apa yang saksi nyatakan di sidang pengadilan. Artinya, keterangan yang diberikan saksi sewaktu diperiksa pada tahap penyidikan belum merupakan

---

[246] *Ibid.*, ps. 1 angka 20.

[247] Harahap, *op. cit.*, hal. 287.

alat bukti yang sah. Kemudian, dalam ayat (2) dijelaskan keterangan seorang saksi saja tidak cukup untuk membuktikan bahwa terdakwa bersalah terhadap perbuatan yang didakwakan kepadanya, hal ini terkait dengan asas *unus testis nullus testis*, yaitu seorang saksi bukan lah saksi.[248] Namun, apabila dalam suatu tindak pidana ternyata saksi yang ada hanya satu, maka keterangan saksi tersebut baru akan bernilai sebagai alat bukti apabila keterangan saksi tersebut didukung satu alat bukti yang sah lainnya.

Selanjutnya dalam ayat (3) dijelaskan, keterangan beberapa saksi yang berdiri sendiri-sendiri tentang suatu kejadian atau keadaan dapat digunakan sebagai suatu alat bukti yang sah apabila keterangan saksi itu ada hubungannya satu dengan yang lain sedemikian rupa, sehingga dapat membenarkan adanya suatu kejadian atau keadaan tertentu. Syarat yang diatur dalam Pasal 185 KUHAP ini biasa disebut sebagai syarat materil keterangan saksi yang dapat dijadikan alat bukti.[249]

Selain harus memenuhi syarat materil sahnya keterangan saksi sebagimana dijelaskan tersebut, keterangan saksi agar

---

[248] Soetomo, *op. cit.*, hal. 58.

[249] Prints, *op. cit.*, hal. 108

dapat menjadi alat bukti dan memiliki nilai pembuktian harus juga memenuhi syarat formil. Syarat formil dari keterangan saksi adalah apabila keterangan saksi tersebut diberikan di bawah sumpah.[250] Hal ini merupakan penafsiran secara *a contrario* dari ketentuan dalam Pasal 185 ayat (7) yaitu: “Keterangan saksi yang tidak disumpah meskipun sesuai satu dengan yang lain, tidak merupakan alat bukti...” Keterangan saksi semacam itu hanya dapat dipergunakan sebagai tambahan alat bukti sah yang lain.

Hakim dalam melakukan penilaian terhadap keterangan saksi harus sungguh-sungguh memperhatikan nilai persesuaian keterangan saksi yang satu dengan lainnya, persesuaian keterangan saksi dengan alat bukti lainnya, alasan yang mungkin dipergunakan oleh saksi dalam memberikan keterangan, dan cara hidup serta kepribadian dari saksi tersebut. Selain itu, hakim juga perlu memperhatikan konsistensi dari jawaban saksi. Menurut DR. Wahjadi Dharmabrata, konsistensi sangat menentukan apakah seseorang mampu untuk diwawancarai atau dimintai keterangan. Yang dimaksud konsitensi di sini adalah:

---

[250] *Ibid.*

a. informasi tidak berubah pada pemeriksaan oleh satu pemeriksaan dalam waktu yang berbeda
b. informasi tetap konsisten pada pemeriksaan oleh beberapa pemeriksa pada waktu yang sama atau berbeda. [251]

Dalam kasus Anshar.net ini terdapat sebelas orang saksi, yang pada pokoknya menerangkan sebagai berikut.

3. Abdul Azis alias Jafar Alias Qital

a. Bahwa saksi mengenal Agung hanya sebatas hubungan dunia maya melalui *chatting*, dan tidak pernah bertatap muka.

b. Bahwa saksi merupakan pembuat *content Website* www.anshar.net tentang jihad atas permintaan Noordin M. Top.

c. Bahwa saksi meminta bantuan Agung untuk membelikan serta mendaftarkan domain dan hosting. Atas permintaan saksi Agung membelikan dan mendaftarkan domain dan hosting tersebut.

d. Bahwa saksi mengakui keterlibatan M. Agung Prabowo hanya pada tahap membelikan dan

---

[251] Wahjadi Dharmabrata, *Psykiatri Forensic* (Jakarta: EGC, 2003), hal. 75.

mendaftarkan domain dan hosting saja, sehingga saksi tidak mengetahui mengenai *Website* www.anshar.net karena Agung tidak termasuk dalam jaringan.

4. Andi Jati Tristiyanto
   a. Saksi merupakan teman sekampung, kos, dan kuliah Agung sehingga mengetahui bahwa Agung memang ahli dalam *Website*, situs, dan merupakan jasa konsultan.
   b. Bahwa benar Agung sering *chatting* dengan Qital, Pakne, Blandong Sapi, dan Salafuljihad.
   c. Bahwa saksi mengetahui Agung Setyadi pernah bertemu dengan Agung.
   d. Bahwa saksi pernah diajak Agung untuk mengambil upah di ATM.
   e. Bahwa saksi mengetahui sarana dalam melakukan pendaftaran domain dan hosting *Website* www.anshar.net dengan menggunakan HP Sony Ericson Tipe T-610, milik Agung.
5. Juli Pangestu
   a. Saksi mengenal Agung karena Agung adalah mahasiswa Universitas Semarang.

b. Bahwa saksi mengetahui Agung sering menggunakan warnet dan melakukan *chatting.*

4. Febby Firmansyah
   a. Bahwa saksi tidak mengenal Agung.
   b. Bahwa saksi merupakan korban bom Hotel JW Marriot.
   c. Bahwa saksi mengetahui www.anshar.net melalui stasiun Metro TV.
   d. Bahwa saksi mengetahui *content Website* tersebut karena saksi sengaja membukanya. Isi *Website* tersebut adalah peta atau tempat yang akan menjadi sasaran pengeboman atau penembakan para teroris.
   e. Bahwa dengan adanya *Website* tersebut saksi merasa takut, bahkan keluarga saksi pun turut takut dan trauma.
5. Vivi Normasari
   a. Bahwa saksi tidak mengenal Agung.
   b. Bahwa saksi mengetahui *Website* www.ansher.net dan isi *Website* tersebut.
   c. Bahwa saksi merasa takut, resah, dan trauma dengan keberadaan *Website* tersebut.
6. Zamri

a. Bahwa saksi adalah Penyidik Madya Unit V IT&CC Dit II Eksus Bareskrim Polri yang telah melakukan penangkapan terhadap Agung.
b. Penangkapan terhadap Agung dilakukan dengan menelusuri terlebih dahulu *Website* www.anshar.net yang memang benar merupakan situs teroris, yang didapat dari barang bukti *hard disk* dalam perkara Qital.
c. Bahwa domain tersebut didaftarkan di Semarang, setelah terdaftar terjadi peledakan Bom Bali II, selanjutnya nama *server*nya dialihkan oleh Agung.
d. Agung mengalihkan *Website* tersebut karena takut Agung pernah melakukan *chatting* dengan Qital yang pada waktu itu sudah tertangkap.
e. Bahwa benar Agung telah memandu Qital dalam mendaftar domain dan hosting.
f. Bahwa benar Agung adalah orang yang pandai di bidang computer dan informatika yang telah mendaftarkan domain dan hosting *Website* www.anshar.net atas permintaan Qital.

g. Bahwa karena pengetahuan tersebut pada angka 6, Agung merupakan orang yang dimanfaatkan Qital dan kelompoknya (kelompok teroris).

h. Bahwa Agung ditangkap karena pengembangan perkara Bom Bali II dimana Qital terkait dengan peristiwa tersebut dan dinyatakan bersalah oleh Hakim.

7. Eddy Hartono

a. Bahwa saksi bekerja di TIKI.

b. Bahwa benar sesuai pengakuan pengirim bahwa barang yang dikirim tersebut adalah *notebook.*

8. Ari Herawati

a. Bahwa saksi bekerja di TIKI.

b. Bahwa benar terdapat pengiriman paket berupa *notebook* dengan nama pengirim Anisa LD untuk tujuan Benny Irawan dengan alamat Perum Lapas Kelas II A Denpasar.

9. Agung Setyadi alias Pakne alias Salafuljihad

a. Bahwa saksi mengenal Agung di serambi Masjid Universitas Semarang dan yang mengenalkan adalah Al-Irhab melalui *chatting* di #cafeislam.

b. Bahwa saksi bertemu secara fisik dengan Agung sebanyak empat kali.

c. Bahwa saksi pernah *chatting* dengan Al-Irhab alias Imam Samudra akan tetapi secara langsung tidak pernah bertemu.

d. Bahwa saksi yang mengirim MP3, Qur’an Digital, dan buku Islam atas permintaan dan dana dari Kulhad yang dialamatkan untuk Ihwan, Lapas Krobokan Denpasar.

e. Bahwa pengiriman tersebut menggunakan nama Annisa L.D, yang *nota bene* adalah nama anak perempuannya.

10. AKP Trikuncoro

a. Bahwa saksi mengetahui secara kronologis peristiwa terjadinya Bom Bali II.

b. Bahwa saksi tidak mengetahui siapa pelaku pemboman tersebut.

11. Yuda Pratiyoko

a. Bahwa saksi mengenal Agung.

b. Bahwa Agung memang pintar dalam teknologi.

c. Bahwa Agung sering melakukan *chatting* dan menyediakan layanan jasa pendaftaran domain dan hosting saja.

Berdasarkan pokok keterangan saksi tersebut, terlihat adanya kesesuaian kesaksian antara para saksi terutama terkait dengan keterlibatan M. Agung Prabowo dalam pembuatan *domain name* dan *hosting Website* www.anshar.net. Antara lain kesaksian dari Qital yang menyatakan meminta bantuan M. Agung Prabowo untuk membelikan serta mendaftarkan domain dan hosting. Atas permintaan saksi, M. Agung Prabowo membelikan dan mendaftarkan domain dan hosting tersebut, dengan demikian keterlibatan M. Agung Prabowo menurut Qital hanya pada tahap membelikan dan mendaftarkan domain dan hosting saja.

Selanjutnya, kesaksian dari rekan M. Agung Prabowo yaitu Andi Jati Tristiyanto yang menyatakan saksi mengetahui sarana dalam melakukan pendaftaran *domain* dan *hosting Website* www.anshar.net dengan menggunakan HP Sony Ericson Tipe T-610, milik Agung. Dari dua kesaksian tersebut terlihat adanya persesuaian yaitu pernyataan yang menyatakan M. Agung Prabowo adalah benar merupakan orang yang melakukan pembelian *domain name* dan *Web hosting*. Jika melihat syarat minimun dari saksi, maka kesaksian kedua saksi tersebut telah memenuhinya.

2. Keterangan Ahli

Alat bukti berikutnya dalam kasus www.anshar.net ini adalah keterangan ahli. Pengertian keterangan ahli paling awal dapat ditemukan pada ketentuan umum KUHAP yang menjelaskan: “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.”[252]

Apabila hanya melihat definisi yang diberikan dalam Pasal 1 angka 28 KUHAP ini, tidak akan memberikan kejelasan mengenai keterangan ahli sesungguhnya. Oleh sebab itu, Pasal 1 angka 28 KUHAP ini harus dikaitkan dengan pasal lainnya yang menjelaskan tentang keterangan ahli, antara lain Pasal 120, Pasal 132 ayat (1), Pasal 133, Pasal 179, Pasal 180 dan Pasal 186 KUHAP.

Dalam hukum acara pidana, keterangan ahli sesungguhnya telah ada sejak tahap penyidikan. Hal ini terlihat pada Pasal 120 ayat (1) KUHAP, yang menjelaskan sebagai berikut. “Dalam hal penyidik menganggap perlu, ia dapat minta pendapat orang ahli atau orang yang memiliki keahlian

[252] Indonesia (b), *op. cit.*, ps. 1 angka 28.

khusus.” Pada tahapan ini pun ahli sudah diambil sumpah atau janjinya untuk memberikan keterangan menurut pengetahuannya.[253]

Pada dasarnya KUHAP membagi ahli menjadi dua. Hal ini terlihat dalam Pasal 133 ayat (1) jo. Pasal 179 ayat (1) yang pada pokoknya menjelaskan setiap orang yang diminta pendapatnya sebagai *ahli kedokteran kehakiman* atau dokter atau *ahli lainnya*. Ahli kedokteran kehakiman adalah ahli yang memiliki keahlian khusus dalam kedokteran kehakiman sehubungan dengan pemeriksaan korban penganiayaan, keracunan atau pembunuhan. Sedangkan yang dimaksud dengan “ahli lainnya” adalah ahli pada umumnya, yaitu orang yang memiliki “keahlian khusus” pada suatu bidang tertentu.[254]

Pasal tentang keterangan ahli yang disebutkan sebelumnya bukan merupakan keterangan ahli sebagai alat bukti, karena keterangan ahli yang bernilai sebagai alat bukti adalah keterangan ahli yang disampaikan dihadapan sidang pengadilan, sebagaimana diatur dalam Pasal 186 KUHAP. Untuk itu perlu diperhatikan KUHAP membedakan keterangan seorang ahli di persidangan sebagai alat bukti

[253] Ibid., ps. 120 ayat (2).

[254] Harahap, *op. cit.*, hal. 301.

keterangan ahli (lihat Pasal 186 KUHAP) dan keterangan seorang ahli secara tertulis di luar sidang pengadilan sebagai alat bukti surat (lihat Pasal 187 huruf c KUHAP).[255] Keadaan seperti ini yang terkadang disebut sebagai sifat dualisme keterangan ahli.[256]

Alasan disebut dualisme keterangan ahli adalah, terkadang terdapat kondisi, pada saat yang bersamaan di hadapan sidang pengadilan diajukan suatu alat bukti berupa keterangan ahli yang berbentuk laporan atau *visum et repertum* yang dijadikan alat bukti surat sebagai pada dimaksud dalam Pasal 187 huruf c KUHAP yaitu surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai sesuatu hal atau sesuatu keadaan yang diminta secara resmi dari padanya, sementara dalam persidangan itu juga, terdapat alat bukti keterangan ahli yang berbentuk keterangan langsung secara lisan, sebagaimana diatur dalam Pasal 186 KUHAP.

Penyelesaiannya menurut M. Yahya Harahap, laporan dari ahli berupa *visum et repertum* tersebut sebaiknya dijadikan "surat keterangan" bukan sebagai alat bukti surat. Selain

---

[255] Hamzah, op. cit., hal. 269.

[256] Harahap, op. cit., hal. 302.

itu penilaian terhadap alat bukti juga akan diserahkan kepada hakim, apakah hakim akan menilainya sebagai dua alat bukti yang berbeda atau tidak.[257]

Disamping itu, sering terjadi salah paham dikalangan masyarakat dengan menyebut kehadiran seorang ahli dipersidangan adalah sebagai saksi ahli. Ini adalah sesuatu yang keliru, karena terkesan menyamakan antara saksi dengan ahli, sesungguhnya keduanya sangat berbeda. Terdapat faktor yang membedakan antara keterangan saksi dengan keterangan ahli. Keterangan saksi diberikan berdasarkan apa yang saksi lihat, saksi dengar dan saksi alami sendiri serta menyebut alasan pengetahuannya itu, sedangkan keterangan ahli diberikan berdasarkan pengetahuan si ahli tersebut.[258]

Kembali pada kasus Anshar.net. Kasus Anshar.net ini merupakan kasus yang cukup kompleks karena secara langsung menyangkut beberapa aspek kehidupan bermasyarakat, yaitu aspek hukum, aspek sosial, aspek psikologis dan aspek informasi teknologi (IT). Disebabkan keterkaitan kasus Anshar.net ini dengan berbagai aspek kehidupan

---

[257] Prints, op. cit., hal.

[258] Wirjono Prodjodikoro, *Hukum Acara Pidana di Indonesia* (Jakarta: Ghalia, 1982), hal. 87

bermasyarkat, tentunya penyelesaian kasus ini tidak hanya murni menggunakan disiplin ilmu hukum belaka, tetapi harus juga melibatkan disiplin ilmu lain yang terkait dengan aspek lainnya dalam kasus ini.

Terbukti pada saat penyelesaian kasus ini terdapat tiga orang ahli dari disiplin ilmu yang berbeda. Mereka adalah Prof. Dr. Sarlito Wirawan seorang Guru Besar dari Universitas Indonesia dalam bidang Psikologi, berikutnya adalah Ir. Budi Rahardjo, Msc. Ph.D berprofesi sebagai Dosen ITB bidang Teknik Elektro dan Informatika yang dalam dunia IT di Indonesia dan luar negeri sudah diakui keahliannya, dan yang terakhir adalah Prof. Romli Atsasmita, S. H., LL.M., seorang Dosen Universitas Padjajaran yang merupakan ahli dalam bidang Ilmu Hukum. Berikut adalah pokok keterangan ahli yang mereka berikan.

1. Prof. Dr. Sarlito Wirawan
    a. Ahli merupakan Guru Besar UI bidang Psikologi.
    b. Bahwa benar seseorang melihat gambar yang terdapat dalam *Website* anshar.net tersebut dapat menimbulkan rasa takut dan memiliki arti perihal ancaman kekerasan.

c. Bahwa gambar dalam tampilan *Website* www.anshar.net tidak ada makna lain kecuali untuk menimbulkan situasi yang menakutkan yaitu mengandung suatu ancaman kekerasan atau bahaya yang tidak dapat diatasi oleh orang yang bersangkutan sehingga akan menimbulkan rasa takut.

d. Ahli menjelaskan isi *Website* anshar.net menimbulkan suatu rasa takut, yaitu suatu keadaan emosi yang timbul ketika seseorang melihat gambar tersebut.

e. Ahli menjelaskan rasa takut memiliki tiga kategori, pertama yaitu takut dengan ciri objek yang ditakuti ada, alasan jelas dan bahaya jelas. Kedua adalah fobia, dimana objek yang ditakuti ada, tetapi alasan ketakutan tersebut tidak diketahui. Ketiga adalah cemas, dimana objek yang ditakuti tidak jelas dan bahaya serta alasan tidak jelas.

2. Ir. Budi Raharjo

a. Bahwa saksi adalah dosen ITB bidang Teknik Elektro dan Informatika.

b. Untuk membuat *Website* dilakukan beberapa tahap:

1) Membuat design yang berisi tulisan dan gambar;
2) Menempatkan design tersebut di sebuah server yang terhubung ke Internet, untuk servernya dapat dilakukan dengan menempatkan server yang dimiliki sendiri di sebuah provider atau *Internet Service Provider* (ISP) atau dengan menyewa tempat yang sudah disediakan oleh Web hosting yang menyediakan layanan gratis dan layanan berbayar.

c. Dengan melihat gambar No. 2 pada *Website* tersebut, dapat disimpulkan bahwa gambar tersebut merupakan *Website* yang datanya sudah ter-*upload*. Sedangkan untuk gambar selanjutnya, dapat merupakan *content* dari *Website* yang sudah ter-*upload* tersebut. Bagi pihak yang membuat *domain name*, dapat mendaftarkan domainnya di *registar* seperti www.joker.com, www.netsol.com, dan sebagainya.

d. Pendaftaran tersebut dapat dilakukan oleh siapa saja selama pendaftar tersebut memiliki kartu kredit untuk mendaftar. Biasanya, pendaftaran tidak melakukan verifikasi terhadap pendaftar sepanjang domain yang terpilih tersedia. Akan

tetapi, nama domain tersebut kemudian diarahkan kepada server yang memberikan layanan Webhosting, seperti www.anshar.net diarahkan pada server openhosting.co.uk.

e. Dalam hal pembayaran, penyedia layanan tidak memerdulikan lokasi fisik dari user karena proses dilakukan melalui Internet. Contoh, dapat dimungkinkan *user* berasal dari Indonesia dan penyedia layanan dari Inggris atau Amerika. Penyedia layanan tersebut dapat pula mengabaikan asal dari kartu kredit, maksudnya, penyedia layanan tidak memerdulikan apakah kartu kredit itu milik yang bersangkutan atau hasil *carding.*

f. Ahli menjelaskan bahwa *Website* yang masih *up to date* maupun yang sudah di *down*-kan atau tidak dapat diakses lagi masih dapat diketahui siapa dan darimana pembuatnya tergantung kepada ketersediaan catatan atau *log file*. Contohnya, ketika *file* yang berisi design Web di upload ke *Webhosting* dengan menggunakan *ftp* atau fitur *upload* dari *Webhosting*, aktifitas tersebut dicatat oleh *server Webhosting*. *Log* tersebut dapat memberikan informasi asal nomor

IP dari pembuat situs Web serta nomor IP tersebut dapat ditelusuri ISP yang digunakan oleh pembuat situs Web. Berdasarkan ISP, dapat diketahui pengguna nomor IP pada saat *upload*. Cara lain yang dapat digunakan adalah dengan melihat data pendaftar domain, apabila pendaftar tersebut menggunakan data yang tidak palsu maka dapat diketahui pendaftar domain tersebut, yang kemungkinan berkaitan dengan pemilik situs Web.

g. Menurut Ahli, dokumen atau *file* yang tersimpan di dalam sebuah *hard disk* dapat diperoleh kembali dengan berbagai cara tergantung pada kondisi hard disk. Untuk berkas yang belum terhapus, tentunya, berkas tersebut masih tersedia, sedangkan untuk berkas yang sudah terhapus sebenarnya berkas tersebut masih tersimpan di hard disk, hanya indeks dari berkas tersebut dihapuskan dari *catalog* daftar isi sehingga seolah-olah berkas sudah tidak terdapat di *hard disk* walaupun sebenarnya berkas tersebut masih tersimpan bahkan mem-*format hard disk* pun masih meninggalkan berkas dalam *hard disk*.

h. Dapat dikatakan bahwa di dalam hard disk seringkali masih terdapat sisa log dari aktifitas *user,* seperti situs Web yang dikunjungi ataupun file yang didownload. Biasanya Web browser memiliki direktori *cache* yang berfungsi untuk menampung sementara situs yang dikunjungi. Tujuan direktori cache atau *temporary directory* adalah untuk mempercepat proses *browsing*.

3. Prof. Dr. Romli Atsasmita

a. Ahli memberi keterangan kalau M. Agung Prabowo memenuhi unsur pelaku tindak pidana dalam arti luas. Hal tersebut merujuk pada kalimat “setiap orang yang dengan sengaja memberi bantuan atau kemudahan...”

b. Saksi merupakan dosen di Universitas Padjajaran, jurusan hukum. Menurut Ahli, perbuatan Agung mendaftarkan domain dan hosting, memindahkan penghostingan *Website* www.anshar.net serta tidak melaporkan kepada pihak berwajib termasuk dalam perbuatan menyembunyikan informasi sebagaimana diatur dalam pasal 13 huruf c Perpu Nomor 1 Tahun 2002 sebagaimana telah ditetapkan sebagai Undang-

undang Nomor 15 Tahun 2003. Alasannya, pengalihan hosting internet oleh agung merupakan upaya untuk menyesatkan informasi dengan tujuan untuk menghindarkan diri dari tertangkapnya pelaku oleh petugas hukum.

c. Upaya tersebut dilakukan mengingat himbauan polisi untuk menyerahkan diri telah ditayangkan dalam media TV secara luas kepada masyarakat.

Berdasarkan keterangan ahli tersebut, khususnya keterangan ahli Ir. Budi Rahardjo, semakin menjelaskan posisi dari *website* tersebut, termasuk penjelasan ahli terkait dengan proses pembelian, pembayaran, hingga proses peng-*upload*-an konten dari *website* www.anshar.net. Ahli Ir. Budi Rahardjo juga menjelaskan kalau di dalam *hard disk* yang dijadikan barang bukti mungkin masih tersimpan *log file* terkait percakapan M. Agung Prabowo dengan terdakwa / terpidana lainnya melalui *chating* di IRC.

3. Surat

Pengertian surat menurut KUHAP adalah surat sebagaimana yang tercantum dalam Pasal 184 ayat (1) huruf c, dibuat atas sumpah jabatan atau dikuatkan dengan sumpah, sebagai berikut.

a. Berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat dihadapannya, yang memuat keterangan tentang kejadian atau keadaan yang didengar, dilihat atau yang dialaminya sendiri, disertai dengan alasan yang jelas dan tegas tentang keterangannya itu; Jadi pada dasarnya surat yang termasuk dalam alat bukti surat yang disebut disini ialah “surat resmi” yang dibuat oleh “pejabat umum” yang berwenang membuatnya tapi agar surat resmi tersebut dapat bernilai sebagai alat bukti dalam suatu perkara pidana maka surat resmi itu haruslah:

   1) memuat keterangan tentang kejadian atau keadaan yang didengar, dilihat atau dipahami oleh pejabat.

2) disertai dengan alasan yang jelas dan tegas mengenai keterangannya itu.[259]

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. Jenis surat ini dapat dikatakan hampir meliputi segala jenis surat yang dibuat oleh pengelola administrasi dan kebijakan eksekutif. Contoh: Kartu Tanda Penduduk, Akta Keluarga, Akta Tanda Lahir, dan lain sebagainya.

c. Surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahlian mengenai sesuatu hal atau sesuatu keadaan yang diminta secara resmi daripadanya.

Surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian lain (surat pada umumnya).

Dalam kasus M. Agung Prabowo dan merujuk pada Surat Tuntutan yang dibuat oleh Jaksa Penuntut Umum, pada penyelesaian perkara dipersidangan tidak tidak digunakan alat bukti surat.

---

[259] Harahap, *op. cit.*, hal. 307.

3. Petunjuk

Alat bukti selanjutnya dalam perkara ini adalah alat bukti petunjuk. 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.[260] Djoko Prakoso berpendapat bahwa alat bukti petunjuk adalah merupakan alat bukti yang penggunaannya dilakukan secara tidak langsung.[261] Sebab, hakim dalam mengambil suatu kesimpulan terhadap suatu pembuktian haruslah menghubungkan suatu alat bukti dengan alat bukti lainnya dengan memilih yang ada persesuainya satu dengan yang lain.

Karena suatu petunjuk membutuhkan alat bukti lain, maka petunjuk bukan merupakan alat bukti langsung.[262] Petunjuk hanya dapat diketahui dari keterangan saksi, surat, dan keterangan terdakwa.[263] Penilaian terhadap

---

[260] Indonesia (b), *op. cit.*, ps. 188 ayat (1).

[261] Djoko Prakoso, *op. cit.*, hal. 95.

[262] Hari Sasangka dan Lily Rosita, *Hukum Petunjuk dalam Perkara Pidana* (Semarang: Mandar MAju, 2003), hal. 75-76.

[263] H.F.A. Kuffal, *Penerapan KUHAP di Indonesia* (Malang: UMM Press, 2004), hal. 23.

kekuatan pembuktian dari suatu petunjuk dilakukan oleh hakim dengan arif lagi bijaksana setelah ia mengadakan pemeriksaan dengan penuh kecermatan dan kesaksamaan berdasarkan hati nuraninya.[264]

Jaksa Penuntut Umum dalam surat tuntutannya mengajukan petunjuk untuk dipertimbangkan oleh majelis hakim. Adapun petunjuk yang diajukan oleh Jaksa Penuntut Umum adalah sebagai berikut.

Berdasarkan keterangan saksi satu dengan yang lain, apabila dikaitkan maka terdapat persesuaian yang menandakan bahwa telah terjadi suatu tindak pidana terorisme sebagaimana didakwakan terhadap Agung dan membuktikan bahwa benar Agung yang melakukan perbuatan tersebut. Agung terbukti melakukan perbuatan sebagai berikut.

1. Agung adalah pihak yang mendaftarkan *domain* dan *hosting website* www.anshar.net, di Semarang.
2. Dengan metode teknologi pelacakan terungkap *name server website* tersebut telah dipindahkan yaitu dari ns.openhosting.co.uk dan ns2.openhosting.co.uk ke ns.israel-webhosting.com dan ns2.israel-webhosting.com

[264] Indonesia, op. cit., ps. 188 ayat (3).

yang dilakukan oleh Agung melalui warnet Universitas Negeri Semarang dengan maksud agar *website* tersebut tidak dapat diakses.

Kedua pentunjuk tersebut menggambarkan terdapat dua perbuatan M. Agung Prabowo yang terkait langsung dengan tindak pidana yang ia lakukan, yaitu melakukan pendaftaran domain dan hosting serta mengalihkan name server *website* www.anshar.net. Petunjuk tersebut diperoleh dari adanya persesuaian keterangan saksi yang satu dengan saksi lainnya.

4. Keterangan Terdakwa

Alat bukti terakhir yang disebutkan jaksa dalam surat tuntutannya adalah alat bukti keterangan terdakwa. Keterangan terdakwa ialah apa yang terdakwa nyatakan di sidang pengadilan tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri atau alami sendiri.[265] Menurut yurispridensi, keterangan dari terdakwa yang hendaknya didengar adalah berupa penyangkalan, pengakuan, ataupun

[265] R. Soesilo dan M. Karjadi, *Kitab Undang-undang Hukum Acara Pidana dengan Penjelasan Resmi dan Komentar* (Bogor: Politea, 1997), hal. 167.

sebagian perbuatan atau keadaan.[266] Pengertian keterangan Terdakwa berbeda dengan pengertian pengakuan terdakwa. Menurut Andi Hamzah, pengakuan sebagai alat bukti mempunyai syarat-syarat sebagai berikut.

1. mengakui ia yang melakukan delik yang didakwakan
2. mengaku ia bersalah. [267]

Dengan kata lain, isi dari keterangan terdakwa adalah berupa pembenaran baik seluruh atau sebagian perbuatan yang disebut dalam surat dakwaan, serta pengakuan seluruhnya atau sebagian perbuatan yang disebut dalam surat dakwaan.

Keterangan terdakwa yang menyangkal dakwaan tetapi membenarkan beberapa keadaan atau perbuatan yang menjurus pada terbuktinya perbuatan sesuai alat bukti lain adalah merupakan alat bukti. Sedangkan pengakuan terdakwa di muka hakim tidak cukup untuk menjatuhkan suatu hukuman pidana kepada terdakwa. Pengakuan terdakwa di muka hakim untuk menjadi bukti yang sempurna harus diikuti keterangan yang jelas tentang keadaan, pada saat peristiwa pidana

---

[266] Hoge Raad dengan Arrestnya 22 Juni 1994, NJ.44/45 No. 589.

dilakukan.[268] Dengan demikian, keterangan terdakwa tidak perlu sama sekali dengan pengakuan.

Kedudukan terdakwa dalam acara pidana adalah sebagai subjek yang harus mendapat penghargaan sepenuhnya, tanpa mengurangi pentingya tujuan dari acara pidana itu sendiri dalam mencari kebenaran di pemeriksaan perkara pidana. Ini berarti apabila seorang terdakwa mengakui terus terang kesalahannya, belum tentu ia pasti dihukum. Pengakuan terdakwa harus pula berdasar pada kebenaran. Sebab kebenaranlah yang menjadi dasar dari suatu putusan pidana.[269]

Keterangan terdakwa yang diberikan pada tahap penyidikan untuk yang pertama kali banyak manfaatnya, karena hal yang disampaikannya masih murni, belum tercampur dengan cerita yang dibuat-buat atau telah dipikirkan terlebih dahulu. Hal ini berakibat logis bagi seorang

---

[268] Mien Rukmini, *Perlindungan HAM Melalui Asas Praduga Tidak Bersalah dan Asas Persamaan Kedudukan dalam Hukum Pada Sistem Peradilan Pidana Indonesia* (Bandung: PT Alumni, 2003), hal. 139.

[269] Djoko Prakoso, *Alat bukti dan Kekuatan Pembuktian di dalam Proses Pidana,* cet. 1, (Yogyakarta: Liberti, 1988), hal. 34.

penasihat hukum terdakwa untuk mengadakan alibi dalam usaha membebaskan diri terdakwa dari kesalahannya.[270]

Pemeriksaan terdakwa dilakukan setelah pemeriksaan saksi-saksi dan alat bukti lain setelah selesai diperiksa di persidangan. Baik aturan dalam KUHAP maupun HIR, tidak menyatakan terdakwa perlu disumpah. Menurut KUHAP terdakwa diberikan kesempatan secara bebas dan sukarela yang seluas-luasnya dalam memberikan keterangan. Bahkan sistem hukum acara di Belanda dan negara *Common Law* memberikan hak untuk menolak menjawab pertanyaan atau hak diam bagi terdakwa (*the rights to remain the silent)*.

Dalam kasus, Agung mengakui bahwa dirinya melakukan *chatting* dengan Qital. Akan tetapi, hubungannya hanya dilakukan melalui dunia maya. Agung bersedia mendaftarkan *domain* dan *hosting website* tersebut karena permintaan Qital setelah memberikan uang atas imbalan jasa konsultasi, namun Qital tidak dapat melakukan pendaftaran sendiri sehingga Agung yang melakukan pendaftaran tersebut. Keterangan M. Agung Prabowo ini telah memenuhi ketentuan dalam Pasal 189 ayat (1) KUHAP, yaitu disampaikan di hadapan sidang tentang

---

[270] R. Soesilo, *RIB/HIR Dengan Penjelasannya* (Bogor: Politea, 1995), hal. 76.

perbuatan yang ia lakukan sendiri. Berdasarkan Pasal 189 ayat (3) KUHAP, meskipun M. Agung Prabowo telah mengakui perbuatannya, tidak serta merta dia dapat dijatuhi vonis karena keterangan terdakwa harus disertai dengan alat bukti yang lain dan juga harus memenuhi standar pembuktian sebagaimana diatur dalam Pasal 183 KUHAP.

C. Penggunaan Bukti Digital Berupa Kode Sumber *Website* Anshar Sebagai Alat Bukti dalam Tindak Pidana Terorisme

Sebuah bukti digital yang dihasilkan oleh suatu media yang berjalan sebagaimana mestinya dan berdasarkan pendapat ahli, media tersebut dalam keadaan baik, memiliki nilai otentifikasi yang seharusnya tidak bisa disangkal serta memiliki nilai pembuktian yang mutlak, kecuali berhasil dibuktikan sebaliknya.[271]

Pasal 27 Undang-undang Nomor 15 Tahun 2003 memperkenalkan suatu alat bukti yang baru dalam hukum acara pidana, yaitu adanya alat bukti digital. Dengan demikian, telah jelas mengenai status hukum dari penggunaan bukti

[271] Makarim, *op. cit.*, hal. 241.

digital dalam suatu persidangan. Setelah sebelumnya penggunaan bukti digital dalam Undang-undang Nomor 20 Tahun 2001 Tentang Perubahan Atas Undang-undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi, bukti digital hanya dijadikan perluasan dari sumber menemukan alat bukti petunjuk sebagaimana diatur dalam Pasal 188 ayat (2) KUHAP.

Untuk itu perlu dikaji lebih lanjut penggunaan bukti digital berupa kode sumber *website* dalam perkara tindak pidana terorisme pada kasus www.anshar.net. Sebelumnya, terlebih dahulu perlu dijelaskan mengenai uraian unsur dari tindak pidana terorisme yang terkait dengan *website* www.anshar.net ini.

1. Unsur Tindak Pidana Terorisme dalam Kasus *Website* Anshar.net

Seseorang hanya dapat dipidana apabila dalam persidangan terbukti secara sah dan meyakinkan dengan minimal alat bukti dan dengan alat bukti tersebut hakim memperoleh keyakinan, terdakwa adalah benar telah memenuhi seluruh unsur tindak pidana yang didakwakan kepadanya.

Karena apabila terdapat salah satu unsur dari yang didakwakan oleh Jaksa Penuntut Umum ada yang tidak terbukti, maka terdakwa akan mendapatkan putusan bebas atau diyatakan bebas dari tuntutan hukum.[272]

Dalam kasus ini, M. Agung Prabowo dipidana karena telah terbukti secara sah dan meyakinkan melakukan tindak pidana sebagaimana diatur dalam Pasal 13 huruf c Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme. Untuk itu perlu dikaji mengenai penerapan pasal tersebut dalam kasus www.anshar.net ini dengan cara menguraikan unsur per unsur dari pasal tersebut. Adapun uraian unsur dari Pasal 13 huruf c Undang-undang Nomor 15 Tahun 2003 sebagai berikut.

> Setiap orang yang dengan sengaja memberikan bantuan atau kemudahan terhadap pelaku tindak pidana terorisme, dengan:
>
> a. ...
> b. ...
> c. menyembunyikan informasi tentang tindak pidana terorisme

[272] Harahap, *op. cit.*, hal. 347.

Setiap orang

Berdasarkan Pasal 1 angka 2 Undang-undang Nomor 15 Tahun 2003, yang dimaksud dengan setiap orang adalah orang perseorangan, kelompok orang baik sipil, militer, maupun polisi yang bertanggung jawab secara individual, atau korporasi. Pengertian “setiap orang” berdasarkan Yurisprudensi Mahkamah Agung RI No. 1399.K/Pid/1994 tanggal 30 Juni 1995 dipersamakan dengan pengertian “barang siapa”. Dengan demikian, kata setiap orang dalam unsur ini merujuk pada kepada subjek hukum yang mampu bertanggung jawab dan padanya tidak ada dasar pemaaf maupun pembenar sebagaimana yang diatur dalam Undang-undang.

Dalam pemeriksaan di persidangan, terdakwa mengikuti persidangan tersebut dengan baik dan secara cermat menjawab segala pertanyaan yang diajukan kepadanya. Selain itu berdasarkan keterangan saksi Yuda Pratiyoko yang mengenal terdakwa, menyatakan terdakwa adalah orang yang dikenal pintar, sehigga tidak ada masalah terhadap kejiwaan serta kepribadian sebagai alasan adanya dasar pemaaf maupun pembenar. Dengan demikian, unsur setiap orang telah terpenuhi.

dengan sengaja

Sengaja berarti mengetahui dan menghendaki (*willens en wetens*). Menurut *Memorie van Toelichting* (MvT) Kesengajaan dibagi menjadi tiga yaitu:

1) Kesengajaan sebagai maksud, bahwa perbuatan yang dilakukan pelaku merupakan manifestasi dari niat yang timbul dari Pelaku.
2) Kesengajaan sebagai keinsafan kemungkinan, bahwa pelaku menyadari atau sepatutnya menyadari perbuatan yang dilakukannya membawa kemungkinan terjadinya tindak pidana.
3) Kesengajaan sebagai keinsafan kepastian, bahwa pelaku menyadari atau sepatutnya menyadari perbuatan yang dilakukannya pasti akan menjadikan terjadinya tindak pidana.

Berdasarkan fakta dipersidangan dan alat bukti yang ada, terungkap terdakwa atas permintaan Qital mendaftarkan dan membeli *domain name* serta *web hosting* dengan menggunakan *credit card* milik orang lain (*carding*). Atas perbuatannya itu terdakwa mendapatkan upah. Dalam hal ini, terlihat terdakwa memang bermaksud untuk mendaftarkan

website tersebut untuk mendapatkan upah. Selain itu, berdasarkan keterangan ahli Ir. Budi Rahardjo, dalam pembuatan *website* diperlukan beberapa tertentu yang membutuhkan suatu proses dan ketika terdakwa melakukan proses tersebut pasti terdakwa mengetahui apa yang ia lakukan dan ia menghendaki akibat yang timbul dari perbuatannya yaitu terdaftarnya *website* dan web *hosting* www.anshar.net untuk kemudian terdakwa mendapatkan upah.

Ketika kemudian hari terdakwa mengetahui kalau *website* yang dibelinya untuk Qital digunakan sebagai media publikasi kegiatan terorisme dan ternyata Qital telah ditangkap sebagai pelaku tindak pidana terorisme, tetapi terdakwa tidak melapor kepada polisi melainkan terdakwa malah memindahkan name server *website* www.anshar.net ke server lain. Terihat dari tindakan terdakwa yang mengalihkan name server, terdakwa mengetahui segala tindakannya merupakan tindakan yang termasuk dalam tindak pidana dan terdakwa menghendaki melakukannya, dengan demikian terpenuhi unsur mengetahui dan menghendaki sebagai unsur dari adanya sengaja. Lebih lanjut, kesengajaan yang dilakukan terdakwa memang ia maksudkan, sehingga terpenuhi lah unsur kesengajaan dalam gradasi kesengajaan sebagai

maksud. Dengan demikian unsur dengan sengaja telah terpenuhi.

memberikan bantuan atau kemudahan terhadap pelaku tindak pidana terorisme

Berdasarkan Penjelasan Pasal 13 Undang-undang Nomor 15 Tahun 2003 yang dimaksud dengan "bantuan" adalah tindakan memberikan bantuan baik sebelum maupun pada saat tindak pidana dilakukan, sedangkan yang dimaksud dengan "kemudahan" adalah tindakan memberikan bantuan setelah tindak pidana dilakukan.

Dari rangkaian fakta dipersidangan terdapat beberapa hal yang mengarah pada unsur ini, yaitu sebagai berikut. Pada awalnya, terdakwa hanya dimintai bantuan dalam hal membuat tutorial terkait cara *carding*, termasuk cara pembelian *domain name* serta *web hostingnya* oleh seseorang ber-*nickname* Qital di channel IRC #cafeislam. Atas permintaan tersebut, terdakwa memandu Qital dalam proses pendaftaran dan pembelian domain name serta web hostingnya, tetapi ternyata Qital tidak berhasil. Akhirnya Qital meminta terdakwa untuk memdaftarkan serta

membelikan domain beserta hosting-nya tersebut dan terdakwa akan diberi upah atas pekerjaannya.

Setelah terdakwa berhasil mendaftarkan dan membeli domain tersebut beserta *web hosting*-nya, *account* dari *web hosting* tersebut diberikan kepada Qital. Kemudian oleh Qital di-*upload* lah konten *website* tersebut dengan ragam materi yang berisi antara lain tetang wasiat Syekh Mukhlas, taktik berperang, teknik persenjataan, teknik meledakkan bom dan teknik penembakan. Pada September 2005, *website* tersebut sudah *online* dan dapat dikunjungi siapa saja yang terhubung dengan internet.

Terdakwa kemudian pada 18 Nopember 2005 mengetahui dari *Koran Tempo*, situs yang didaftarkan serta dibeli olehnya adalah situs terorisme sedangkan Abdul Aziz alias Ja'far alias Qital yang memintanya untuk membelikan *website* tersebut adalah orang yang ditangkap Polisi karena terkait dengan peledakan bom Bali ke-2. Setelah mengetahui hal tersebut, terdakwa mengalihkan name server dari domain www.anshar.net yang semula diarahkan ke ns.openhosting.co.uk kemudian diarahkan ke name server lainnya, yaitu ns.israel-webhosting.com. Dengan demikian, *website* tidak bisa diakses lagi, karena pengalihan name

server tersebut tidak serta merta memindahkan dokumen HTML yang ter-hosting di www.openhosting.co.uk.

Berdasarkan rangkaian peristiwa tersebut terlihat adanya bantuan yang diberikan oleh terdakwa terhadap pelaku tindak pidana terorisme, yaitu Qital. Hal ini sejalan dengan keterangan ahli hukum Prof. DR. Romli Atsasmita yang menyatakan tedakwa telah memberi bantuan kepada pelaku tindak pidana dengan cara melakukan pendaftaran dan pembelian *domain name* beserta *web hosting*-nya yang kemudian *account*-nya diberikan kepada Qital (pelaku tindak pidana terorisme).

Selain memberikan bantuan, terdakwa juga memberikan kemudahan kepada pelaku tindak pidana terorisme. Adapun cara yang diberikan oleh terdakwa adalah dengan menyembunyikan informasi tentang tindak pidana terorisme, yaitu melalui pengalihan *name server* yang berakibat adanya penyesatan informasi dengan tujuan untuk menghindarkan diri dari tertangkapnya pelaku oleh petugas hukum. Dengan uraian tersebut, maka unsur memberikan bantuan atau kemudahan terhadap pelaku tindak pidana terorisme dengan cara menyembunyikan informasi tentang tindak pidana terorisme telah terpenuhi. Dapat disimpulkan, dengan terpenuhinya

seluruh unsur tersebut dan didukung oleh alat bukti yang sah. Secara sah dan meyakinkan terdakwa di vonis telah melakukan tindak pidana sebagaimana diatur dalam Pasal 13 huruf c Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme. Untuk itu terdakwa harus menjalani hukuman penjara selama 3 tahun, potong masa tahanan.[273]

2. Penggunaan Kode Sumber *Website* Sebagai Alat Bukti Sebagaimana Diatur dalam Pasal 27 Undang-undang Nomor 15 Tahun 2003

Kasus yang menimpa M. Agung Prabowo terkait secara langsung dan erat dengan keberadaan *website* www.anshar.net, karena apabila M. Agung Prabowo tidak melakukan pendaftaran dan pembelian *domain name* beserta *web hosting website* tersebut maka ia tidak akan terlibat dalam tindak pidana terorisme dan melanggar ketentuan hukum sebagaimana diatur dalam Pasal 13 huruf c Undang-undang Nomor 15 Tahun 2003.

---

[273] "Pembuat situs www.anshar.net Divonis 3 Tahun Penjara," <http://www.okezone.com/Pembuat%20Situs%20Anshar%20Divonis%203%20Tahun> diakses 20 Juni 2007.

Keberadaan *website* tersebut yang isinya antara lain adalah *Kajian Manhaj* yang merupakan wasiat Muklas (Ali Gufron) dan wasiat ulama lain dan beberapa artikel tentang jihad, *Askariyah* merupakan taktik dan strategi perang meliputi gambar di jalan dengan cara memanfaatkan antrian mobil di pintu tol, kemacetan, *shopping mall,* pusat hiburan, pusat olahraga, hotel, dan sebagainya, *Mutafajjrot* yang merupakan teori tentang bahan peledak, dan Silah yang merupakan teori persenjataan yang seluruhnya bersumber dari Noordin M. Top.

Website ini dikatakan sebagai *website* teroris karena pada dasarnya dalam konten *website* ini terlihat adanya upaya dengan sengaja menggunakan kekerasan atau ancaman kekerasan bermaksud untuk menimbulkan suasana teror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal dengan cara merampas kemerdekaan atau hilangnya nyawa atau harta benda orang lain, atau untuk menimbulkan kerusakan atau kehancuran terhadap obyek-obyek vital yang strategis, atau lingkungan

hidup, atau fasilitas publik, atau fasilitas internasional.[274]

Untuk membuktikan *website* ini telah menimbulkan suasana teror atau rasa takut terhadap orang secara meluas dapat dikutip pernyataan ahli psikologi, Prof. DR. Sarlito Wirawan seorang ahli dalam bidang psikologi, yaitu sebagai berikut.

> Bahwa gambar dalam tampilan *website* www.anshar.net tidak ada makna lain kecuali situasi yang menakutkan yaitu mengandung suatu ancaman kekerasan atau bahaya yang tidak dapat diatasi oleh orang yang bersangkutan sehingga akan menimbulkan rasa takut.

Keterangan ahli juga diperkuat oleh keterangan saksi yang melihat *website* tersebut, yaitu Vivi Normasari yang telah melihat *website* www.anshar.net dan saksi merasa takut, resah, dan trauma dengan keberadaan *website* tersebut. Selain saksi Vivi Normasari terdapat saksi lainnya yang merasakan hal yang sama, yaitu Febby Firmansyah yang merupakan korban peledakan bom di Hotel J. W. Marriot, saksi mengetahui www.anshar.net melalui stasiun Metro TV. Saksi mengetahui *content website* tersebut karena

---

[274] Indonesia (a), *op. cit.*, ps. 7.

saksi sengaja membukanya. Isi *website* tersebut adalah peta atau tempat yang akan menjadi sasaran pengeboman atau penembakan para teroris. Dengan adanya *website* tersebut saksi merasa takut, bahkan keluarga saksi pun turut takut dan trauma.

Seperti yang telah dijelaskan, kaitan pemidanaan M. Agung Prabowo dengan *website* www.anshar.net ini sangat erat. Lebih lanjut, melihat pada salah satu barang bukti yang disita penyidik yaitu satu unit *hard disk* merek Seagate tipe barracuda ATA IV, model ST 3200 11 A, kapasitas 20 GB, nomor seri 3HT4HM8, maka adalah tepat menerapkan penggunaan bukti digital dalam kasus ini.

Tidak ditemukan suatu definisi khusus mengenai apa itu alat bukti, namun secara umum yang dimaksud dengan alat bukti adalah alat bukti yang tercantum dalam pasal 184 ayat (1) KUHAP.[275] Fungsi dari alat bukti itu sendiri adalah untuk membuktikan adalah benar terdakwa yang melakukan tindak pidana dan untuk itu terdakwa harus mempertanggungjawabkan perbuatannya.[276]

---

[275] Prakoso, *op.cit.*, hal. 37.

[276] Harahap, *op. cit.*, hal. 285.

Penggunaan bukti digital dalam perkara tindak pidana terorisme telah diakomodir dalam Pasal 27 huruf b dan c Undang-undang Nomor 15 Tahun 2003, yang menjelaskan sebagai berikut.

> Alat bukti pemeriksaan tindak pidana terorisme meliputi:
> a. ...
> b. alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan
> c. data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada :
> 1) tulisan, suara, atau gambar;
> 2) peta, rancangan, foto, atau sejenisnya;
> 3) huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.

Berdasarkan Pasal tersebut, termasuk dalam alat bukti yang manakah kode sumber *website*? Untuk menjawabnya, akan dikaji dengan menguraikan usur dari tiap hurufnya. *Pertama* adalah Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003, yang unsurnya sebagai berikut.

1. Alat bukti. Tidak terdapat definisi khusus mengenai alat bukti, tetapi berdasarkan fungsi, alat bukti

adalah suatu alat yang digunakan dalam pembuktian untuk tujuan membuktian adalah benar terdakwa yang melakukan tindak pidana dan untuk itu terdakwa harus mempertanggungjawabkan perbuatannya.

2. Informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. Informasi adalah suatu data, yakni mencakup semua fakta yang direpresentasikan sebagai input, baik dalam dalam bentuk untaian kata (*text*), angka (*numerik*), gambar pencitraan (*images*), suara (*voices*), ataupun gerak (sensor), yang telah diproses ataupun telah mengalami perubahan bentuk atau pertambahan nilai menjadi suatu bentuk yang lebih berarti sesuai dengan konteksnya.[277] Kemudian, yang dimaksud dengan elektronik adalah segala perangkat yang dioperasikan dengan cara mengontrol aliran elektron atau partikel bermuatan listrik dalam suatu alat seperti komputer, peralatan elektronik, termokopel, semikonduktor, dan lain sebagainya.[278] Merujuk pada penjelasan Pasal 26A huruf a Undang-

[277] Makarim, *op. cit.*, hal,. 34.

[278] http://id.wikipedia.org/wiki/Elektronik

undang Nomor 20 Tahun 200 Tentang Perubahan Atas Undang-undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi dijelaskan yang dimaksud dengan “disimpan secara elektronik” misalnya disimpan dalam mikro film, *Compact Disk Read Only Memory* (CD-ROM) atau *Write Once Read Many* (WORM). Sebagai tambahan, dalam penjelasan tersebut dijelaskan pula dengan yang dimaksud “alat optik atau yang serupa dengan itu” dalam hal ini tidak terbatas pada data penghubung elektronik (*electronic data interchange*), surat elektronik (*e-mail*), telegram, teleks, dan faksimili.

Pengkajian yang kedua dilakukan terhadap Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003 dengan unsur sebagai berikut.

1. data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar. Secara esensial, suatu informasi berawal dari data (lihat penguraian terhadap unsur “informasi” sebelumnya), dengan demikian pencantuman unsur “informasi” sudah dapat mewakili unsur data dan rekaman. Sedangkan unsur dapat dilihat, dibaca, dan/atau didengar, sesungguhnya merupakan

hasil representsi dari suatu informasi yang telah diproses ataupun telah mengalami perubahan bentuk atau pertambahan nilai menjadi suatu bentuk yang lebih berarti sesuai dengan konteksnya. Hal ini terkait dengan kemampuan panca indra dalam mengeolah informasi yang ada.

2. yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana. Unsur ini menjelaskan mengenai perangkat yang digunakan dalam memproses informasi untuk menghasilkan *output*, karena berdasarkan atas peranan dan fungsinya, suatu sistem informasi terdiri atas keberadaan fungsi-fungsi *input*, proses, *storage*, dan *communication*.[279]
3. baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik. Unsur ini menyangkut media dimana informasi tersebut tersimpan (*storage*) juga termasuk media *output* atau akhir dari suatu proses informasi.

[279] Makarim, *op. cit.*, hal 41.

Suatu *website* pada dasarnya terdiri dan terbangun atas susunan bahasa program yang disebut HTML. HTML adalah *markup language* yang digunakan untuk membuat sebuah dokumen *hypertext* agar dapat berdiri secara independen. HTML sendiri adalah dokumen berbasiskan SGML yang dilengkapi seperangkat bahasa generik yang dapat disesuaikan untuk dapat merepresentasikan dokumen disebuah *Website*.

Dalam hal ini HTML sendiri adalah sebuah data yang terdiri dari serangkaian (*text*), angka (*numerik*), gambar pencitraan (*images*), suara (*voices*), ataupun gerak (sensor), yang kemudian diproses sehingga mengalami perubahan bentuk atau pertambahan nilai menjadi suatu bentuk yang lebih berarti sesuai dengan konteksnya, yaitu menjadi sebuah representasi dan presentasi tampilan sebuah *Website*. Setelah terpresentasi menjadi sebuah *website*, maka data (HTML) tersebut kini telah menjadi informasi yang dapat dilihat, dibaca, dan/atau didengar.

Untuk menjadikan sebuah *website* sebagai informasi yang dapat dilihat, dibaca, dan/atau didengar, diperlukan suatu proses dengan bantuan suatu sarana yaitu, perangkat transmisi HTML yang dikenal dengan protokol *HyperText Transfer Protocol* (HTTP) serta perangkat lunak yang menjadi

engine, yaitu *httpd* (*http daemon/server*).[280] Proses itu menghasilkan representasi kode HTML menjadi teks, gambar, atau suara yang dapat dilihat, dibaca, dan didengar secara luas. Mengenai output dari data berupa HTML adalah berupa data elektronik (hasil representasi dan presentasi dari HTML) yang tersimpan (*storage*) secara elektronik pula pada media yang disebut *web hosting*.[281]

Berdasarkan penjelasan tersebut, dapat diperoleh simpulan, kode sumber sebuah *website* memenuhi unsur alat bukti sebagaimana dimaksud dalam Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme. Argumentasi ini diperkuat dengan salah satu contoh yang diberikan Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003, yaitu: "huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya."

Contoh yang diberikan oleh Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003 tersebut seluruhnya memenuhi

---

[280] Dalam Internet terdapat beberapa http server yang lazim digunakan, antara lain web server apache yang berbasis open source, dengan pengguna lebih dari lima puluh persen. Selanjutnya ada webserver lain, yaitu IIS yang merupakan web server buatan Microsoft. Lebih lanjut lihat www.pcmedia.co.id/detail.asp?Id=165&Cid=23&Eid=6

[281] Makarim, *op. cit.*, hal. 43.

kriteria dari sebuah dokumen HTML. Dalam bab tiga telah dijelaskan mengenai karakteristik dari HTML, di mana pada pokoknya sebuah dokumen HTML terdiri dari huruf (huruf digunakan dalam penulisan karena HTML tidak berbasis *machine laguage*), tanda (*tag*), angka (*HTML value*), simbol (penggunaan simbol "< >" untuk permulaan sintak), atau perforasi (penggunaan struktur dan bahasa *markup-language* pada HTML) yang dapat dipahami oleh orang yang mampu membaca atau memahaminya, yaitu orang yang memiliki kemampuan *programing* khususnya *web programing*.

Kembali pada kasus *website* www.anshar.net. Pada kasus tersebut, meski telah menerapkan hukum acara dalam Undang-undang Nomor 15 Tahun 2003, tetapi khusus pada penggunaan alat bukti, ternyata alat bukti digital belum diterapkan. Berdasarkan informasi yang diperoleh, alasan tidak digunakannya bukti digital adalah untuk efisiensi proses persidangan dan masih terdapat keraguan mengenai nilai otentifikasi sebuah bukti digital.[282] Kedua alasan tersebut pada dasarnya tidak bisa diterima. Pertama, jika beralasan

[282] Hasil wawancara dengan Ibu Fitri, salah satu Jaksa Penuntut Umum dalam kasus www.anshar.net. Keterangan serupa juga diberikan oleh Bapak Markus dari Ikatan Penasehat Hukum Indonesia (IPHI) yang menjadi penasehat hukum dari M. Agung Prabowo, wawancara dilakukan di Pengadilan Negeri Semarang pada 11 Juni 2007.

tidak digunakannya bukti digital untuk alasan efisiensi, maka hal ini sungguh kontradiktif dengan kenyataan yang ada di mana pada kasus tersebut terdapat barang bukti *hard disk* milik M. Agung Prabowo.[283] Apabila diperhatikan, *hard disk* tersebut sesungguhnya dapat dimasukkan kedalam alat bukti sebagaimana disebut dalam Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003.

Menjadikan sebuah *hard disk* sebagai barang bukti justru mengakibatkan tidak efisienan proses pembuktian. Meskipun pernah barang bukti dalam penyelesaian perkara pidana sangat penting, tetapi perlu diingat, berdasarkan ketentuan dalam Pasal 183 KUHAP suatu barang bukti tidak dapat dijadikan dasar penjatuhan vonis terhadap terdakwa. Dalam kasus tersebut *hard disk* dijadikan barang bukti, maka hard disk tidak memiliki kekuatan pembuktian, karena berapapun saja barang bukti yang diajukan di persidangan mengenai suatu tindak pidana kalau tidak didukung minimal dua alat bukti dan hakim tidak yakin atas kesalahan yang

[283] Lihat kembali daftar barang bukti pada pembahasan kasus posisi.

dilakukan terdakwa, maka terdakwa tidak dihukum (dibebaskan/*vrijspraak* atau dilepaskan/*ontslag*.[284]

Dengan menjadikan *hard disk* hanya sebagai barang bukti, berarti Jaksa Penuntut Umum perlu meluangkan waktu kembali untuk mencari alat bukti lainnya. Semestinya, hard disk tersebut dijadikan alat bukti saja, sehingga tidak perlu untuk mencari alat bukti lain yang akan digunakan untuk menjelaskan perihal hard disk tersebut, misalnya mencari alat bukti keterangan ahli.

Mengenai keraguan kedua, yaitu nilai otentifikasi dari bukti digital. Telah berulang kali dijelaskan, bukti digital yang dihasilkan oleh suatu sistem yang berjalan sebagaimana mestinya seharusnya dapat diterima dan memiliki nilai otentik serta memiliki kekuatan dalam hal pembuktian. Karena pada dasarnya bukti digital yang dihasilkan sebuah sistem memiliki sifat yang netral dan objektif.

Sebagai tambahan, seharusnya Jaksa Penuntut Umum melihat pada kasus Gun Gun Rusman Gunawan alisa Abdul Hadi alias Abdul Karim alias Bukhori terpidana kasus terorisme yang telah diadili di Pengadilan Negeri Jakarta Pusat

---

[284] Ratna Nurul Afiah, *Barang Bukti dalam Proses Pidana* (Jakarta: Sinar Grafika, 1989), hal. 17.

dengan Nomor Register Perkara 1001/PID.B/2004/PN JKT PST. Secara singkat dapat dijelaskan dalam kasus tersebut. Gun Gun Rusman terbukti telah melanggar pasal 16 jo pasal 11 jo pasal 6 UU nomor 15/2003 tentang Pemberantasan Tindak Pidana Terorisme.[285]

Gun Gun telah mengirimkan uang US$ 12 ribu atas perintah Hambali kepada Amar al-Baluchi pada Desember 2002 sampai dengan Februari 2003. Hal ini berdasarkan keterangan saksi Bambang Wahyu, penyidik yang menjemputnya saat di Pakistan. Atas perintah Hambali - abang kandung terdakwa Gun Gun - jumlah uang itu kemudian ditingkatkan menjadi US$ 50 ribu.

Amar al-Baluchi yang menerima uang itu kemudian meneruskan uang tersebut kepada Madjid Khan sebesar US$ 30 ribu untuk diteruskan kepada Zubir. Dari Zubir, dana itu beralih tangan ke Mamat alias Johan.[286]

Adanya aliran dana itu juga diperkuat dengan hasil investigasi Federal Bureau of Investigation (FBI) terhadap

---

[285] "Gun Gun Rusman, Adik Hambali di vonis Empat Tahun Penjara," <http://www.detikinet.com/index.php/detik.read/tahun/2004/bulan/10/tgl/26/time/160528/idnews/230900/idkanal/10, diakses 24 Juni 2007.

[286] "Empat Tahun Penjara Untuk Adik Hambali,"< http://www.korantempo.com/news/2004/10/27/nasional/18.html>, diakses 24 Juni 2007.

surat elektronik milik Gun Gun. Surat elektronik yang beralamatkan gundulijo@yahoo.com itu mengirim pesan kepada Amar al-Baluchi di jeointhehouse@yahoo.com tentang adanya 30 dokumen yang telah dikirimkan. Amar kemudian mengirimkan pesan kepada Madjid Khan melalui e-mail di mosser12@hademail.com yang dibalas melalui alamat greeting's@yahoo.com. Kata “30 dokumen” itu merupakan kata sandi yang berarti adanya “30 ribu uang yang telah dikirimkan”.

Dalam kasus tersebut, yang juga merupakan kasus terkait tindak pidana terorisme dan menggunakan Undang-undang Nomor 15 Tahun 2003 sebagai dasar hukumnya. Dalam kasus itu Hakim menerapkan penggunaan alat bukti digital. Alat bukti digital dalam kasus tersebut adalah *log e-mail* terdakwa yang diperoleh dari server utama penyedia layanan e-mail (e-*mail provider*) Yahoo!. *Log* itu sendiri berisi informasi terkait pencatatan waktu serta alamat pengiriman email, termasuk isi dari email yang digunakan terdakwa. Jika dikaitkan dengan alat bukti dalam Undang-undang Nomor 15 Tahun 2003, maka alat bukti berupa *log e-mail* tersebut sesuai dengan Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003.

Dengan demikian terbukti, penggunaan bukti digital dalam suatu perkara pidana, khususnya terkait dengan tindak pidana terorisme telah memiliki payung hukum yang kuat. Sehingga dalam menggunakan bukti digital tidak perlu meragukan keabsahan bukti digital tersebut pada saat persidangan di Pengadilan.

3. Penggunaan Alat Bukti Berupa Informasi Elektronik Terkait Penyelenggaraan Sistem Elektronik Berdasarkan Rancangan Undang-undang Informasi dan Transaksi Elektronik

Berdasarkan analisis sebelumnya, penggunaan bukti digital pada suatu proses peradilan telah dimungkinkan dengan adanya dasar hukum yang salah satunya adalah Pasal 27 Undang-undang Nomor 15 Tahun 2003. Meskipun demikian, menurut Edmon Makarim, S. Kom., S. H., LL. M, secara umum paling tidak terdapat tiga hal yang harus diperhatikan pada keberadaan suatu informasi elektronik (arsip elektronik) terkait penggunaannya sebagai alat bukti digital, yaitu (i) substansi informasi; (ii) metodologi fiksasi dan media

penyimpanan yang mengonkretkan bentuk dari informasi itu; serta (iii) identifikasi subjektifnya.[287]

Hal tersebut terkait dari subjektifitas informasi itu sendiri, sehingga semestinya suatu informasi baru dapat dipercaya jika jelas siapa subjek pengirimnya. Namun, apabila informasi tersebut merupakan hasil otomatisasi dari suatu sistem yang berjalan sebagaimana mestinya, maka informasi tersebut tidak perlu dipertanyakan unsur subjektifitasnya, melainkan hanya perlu membuktikan sistem yang menghasilkan informasi tersebut berjalan dengan baik.[288]

Begitu pula dalam penerapan bukti digital pada proses persidangan. Agar suatu bukti digital memiliki nilai otentik dan dapat digunakan sebagai alat bukti, bukti digital tersebut harus diperoleh dari suatu sistem elektronik yang dapat melindungi keotentikan, integritas, kerahasiaan, ketersediaan, dan keteraksesan dari informasi elektronik pada sistem elektronik tersebut.

Saat ini belum ada hukum positif yang mengatur mengenai bagaimana mekanisme kerja suatu sistem elektronik

---

[287] Makarim. *op. cit.*

[288] *Ibid.*

agar keluaran (*output*) yang dihasilkan berupa informasi elektronik atau dokumen elektronik dapat memiliki nilai otentik dan terjaga integritasnya hingga dapat dijadikan sebagai suatu alat pembuktian di pengadilan. Namun, bila merujuk pada Rancangan Undang-undang Tentang Informasi dan Transaksi Elektronik (RUU ITE) yang saat ini tengah dalam pembahasan di Dewan Perwakilan Rakyat, maka pengaturan terkait penyelenggaraan sistem elektronik tersebut dapat ditemukan.

Pasal 1 angka 21 RUU ITE menjelaskan "Penyelenggaraan sistem elektronik adalah pemanfaatan sistem elektronik oleh Pemerintah dan atau swasta."[289] Sistem elektronik sendiri adalah suatu sistem untuk mengumpulkan, mempersiapkan, menyimpan, memproses, mengumumkan, menganalisa, dan menyebarkan informasi elektronik.[290]

Berdasarkan hal tersebut, terlihat cakupan dari penyelenggara sistem elektronik tidak hanya meliputi sistem elektronik yang diselenggarakan oleh pemerintah tetapi termasuk sistem elektronik yang dijalankan oleh swasta. Salah satu contoh penyelenggaraan sistem elektronik oleh

---

[289] Indonesia (c), *op. cit.,* ps. 1 angka 3.

[290] *Ibid.*, ps. 1 angka 4.

swasta yang sesuai dengan kasus pada penelitian ini adalah penyelenggaraan jasa *web hosting* oleh suatu perusahan swasta.

Lebih lanjut dalam Pasal 15 RUU ITE dijelaskan informasi dan transaksi elektronik diselenggarakan oleh penyelenggara sistem elektronik secara andal, aman, dan beroperasi sebagaimana mestinya. Penjelasan Pasal 15 RUU ITE menguraikan yang dimaksud andal adalah sistem elektronik tersebut memiliki kemampuan yang sesuai dengan kebutuhan pengguna; aman artinya sistem elektronik tersebut terlindungi baik secara fisik maupun non fisik; dan yang dimaksud dengan beroperasi sebagaimana mestinya adalah sistem elektronik tersebut memiliki kemampuan sesuai spesifikasinya.

Untuk memenuhi standar yang ditentukan oleh Pasal 15 RUU ITE, setiap penyelenggara sistem elektronik harus mengoperasikan sistem elektronik yang memenuhi persyaratan minimum sebagai berikut:

a. dapat menampilkan kembali informasi elektronik yang berkaitan dengan penyelenggaraan sistem elektronik yang telah berlangsung;

b. dapat melindungi keotentikan, integritas, kerahasiaan, ketersediaan, dan keteraksesan dari informasi elektronik dalam penyelenggaraan sistem elektronik tersebut;
c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik tersebut;
d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik tersebut; dan
e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan pertanggungjawaban prosedur atau petunjuk tersebut;[291]

Dengan demikian dapat disimpulkan, suatu informasi elektronik yang telah diselenggarakan oleh penyelenggara sistem elektronik secara andal, aman, dan beroperasi sebagaimana mestinya, kemudian penyelenggara sistem elektronik telah mengoperasikan sistemnya sebagaimana diatur dalam Pasal 16 RUU ITE. Maka informasi elektronik dan atau hasil cetak dari informasi elektronik yang

[291] *Ibid.*, ps. 16.

dihasilkannya merupakan alat bukti yang sah dan memiliki akibat hukum yang sah pula, serta dapat digunakan sebagai perluasan alat bukti sebagaimana diatur dalam Hukum Acara di Indonesia.[292]

Jika RUU ITE ini kemudian dijadikan Undang-undang, maka bertambah lah payung hukum dalam penerapan dan penggunaan bukti digital pada proses persidangan. Sehingga tidak terdapat lagi keraguan terkait otentifikasi dan integritas terhadap bukti digital, sepanjang perolehan bukti digital tersebut berasal dari sistem elektronik yang penyelenggaraan sistemnya telah secara andal, aman, dan beroperasi sebagaimana mestinya.

[292] *Ibid.*, ps. 5 ayat (1) dan (2).

BAB V

PENUTUP

A. Simpulan

Berdasarkan uraian terdahulu, hasil penelitian yang berjudul “Kode Sumber (*Source Code*) Website Sebagai Alat Bukti Dalam Tindak Pidana Terorisme di Indonesia (Studi Kasus Website Anshar.net)” ini dapat disimpulkan sebagai berikut.

1. Telah terdapat aturan mengenai penggunaan alat bukti digital berupa informasi elektronik dalam peraturan perundang-undangan di Indonesia, khususnya peraturan-perundangan yang mengatur ketentuan Hukum Acara Pidana. Pengaturannya sendiri tersebar dalam beberapa undang-undang, antara lain Undang-undang Nomor 15 Tahun 2002 Tentang Tindak Pidana Pencucian Uang, Undang-undang Nomor 20 Tahun 2001 Tentang Perubahan Atas Undang-undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi, dan Undang-undang

Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme, Menjadi Undang-undang. Meskipun ketiga undang-undang tersebut mengatur penggunaan bukti digital, terdapat perbedaan dalam penggunaan bukti digital tersebut sebagai alat bukti. Dalam Pasal 26A Undang-undang Nomor 20 Tahun 2001 Tentang Perubahan Atas Undang-undang Nomor 31 Tahun 1999 Tentang Pemberantasan Tindak Pidana Korupsi dijelaskan bukti digital dalam tindak pidana korupsi sebagai sumber perolehan petunjuk bagi hakim selain yang dimaksud dalam Pasal 188 ayat (2) KUHAP. Sedangkan ketentuan penggunaan bukti digital dalam Pasal 38 Undang-undang No. 15 Tahun 2002 Tentang Tindak Pidana Pencucian Uang dan Pasal 27 Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme dinyatakan sebagai alat bukti yang berdiri sendiri dan tidak merupakan perluasan dari alat bukit yang diatur dalam Pasal 184 KUHAP. Dalam Pasal 27 Undang-undang Nomor 15 Tahun 2003 sendiri terkandung dua jenis bukti digital, yaitu informasi elektronik dan dokumen elektronik. Untuk

mendapat penjelasan mengenai informasi elektronik dan dokuemen elektronik, digunakan rujukan yaitu Pasal 3 dan 14 Rancangan Undang-undang Tentang Informasi dan Transaksi Elektronik.

2. Kode sumber suatu *website* dapat digunakan sebagai alat bukti dalam tindak pidana terorisme sebagaimana diatur dalam Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003, yaitu sebagai data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik. Kode sumber website dikateogrikan sebagai bukti digital dalam Pasal 27 huruf c karena pada dasarnya suatu kode sumber terdiri dan terbangun atas susunan bahasa program yang disebut HTML. HTML adalah *markup language* yang digunakan untuk membuat sebuah dokumen *hypertext* agar dapat berdiri secara independen. HTML sendiri adalah dokumen berbasiskan SGML yang dilengkapi seperangkat bahasa generik yang dapat disesuaikan untuk dapat merepresentasikan dokumen disebuah *Website*. Dalam hal ini HTML sendiri adalah

sebuah data yang terdiri dari serangkaian (*text*), angka (*numerik*), gambar pencitraan (*images*), suara (*voices*), ataupun gerak (sensor), yang kemudian diproses sehingga mengalami perubahan bentuk atau pertambahan nilai menjadi suatu bentuk yang lebih berarti sesuai dengan konteksnya, yaitu menjadi sebuah representasi dan presentasi tampilan sebuah *Website*. Setelah terpresentasi menjadi sebuah *website*, maka data (HTML) tersebut kini telah menjadi informasi yang dapat dilihat, dibaca, dan/atau didengar. Untuk menjadikan sebuah *website* sebagai informasi yang dapat dilihat, dibaca, dan/atau didengar, diperlukan suatu proses dengan bantuan suatu sarana yaitu, perangkat transmisi HTML yang dikenal dengan protokol *HyperText Transfer Protocol* (HTTP) serta perangkat lunak yang menjadi *engine*, yaitu *httpd* (*http daemon/server*). Proses itu menghasilkan representasi kode HTML menjadi teks, gambar, atau suara yang dapat dilihat, dibaca, dan didengar secara luas. Mengenai output dari data berupa HTML adalah berupa data elektronik (hasil representasi dan presentasi dari HTML) yang tersimpan (*storage*) secara elektronik pula pada media yang

disebut *web hosting*. Berdasarkan penjelasan tersebut, dapat dijelaskan kode sumber sebuah *website* memenuhi unsur alat bukti sebagaimana dimaksud dalam Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme. Argumentasi ini diperkuat dengan salah satu contoh yang diberikan Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003, yaitu: “huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.” Contoh yang diberikan oleh Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003 tersebut seluruhnya memenuhi kriteria dari sebuah dokumen HTML. Dalam bab tiga telah dijelaskan mengenai karakteristik dari HTML, di mana pada pokoknya sebuah dokumen HTML terdiri dari huruf (huruf digunakan dalam penulisan karena HTML tidak berbasis *machine laguage*), tanda (*tag*), angka (*HTML value*), simbol (penggunaan simbol “< >” untuk permulaan sintak), atau perforasi (penggunaan struktur dan bahasa *markup-language* pada HTML) yang dapat dipahami oleh orang yang mampu membaca atau memahaminya, yaitu

orang yang memiliki kemampuan *programing* khususnya *web programing*.

3. Dalam praktek terdapat dua perbedaan penerapan bukti digital sebagaimana dimaksud dalam Pasal 27 Undang-undang Nomor 15 Tahun 2007. Pada kasus tindak pidana terorisme terkati dengan website www.anshar.net, kode sumber website www.anshar.net tidak digunakan sebagai alat bukti. Hal ini terkait dengan tidak diajukannya kode sumber ini sebagai alat bukti oleh Jaksa Penuntut Umum. Berdasarkan Surat Tuntutan (*Requisitor*) Nomor Register Perkara PDM-376/SEMAR/Ep.2/XII/2006, alat bukti yang digunakan dalam kasus M. Agung Prabowo (No. Reg 84/PID/B/2007 PN SMG) adalah keterangan saksi, keterangan ahli, keterangan terdakwa dan petunjuk. Alasan yang digunakan oleh Jaksa Penuntut Umum tidak mengajukan kode sumber website sebagai alat bukti adalah untuk efisiensi biaya perkara dan keraguan mengenai keabsahan bukti digital apabila menggunakan bukti digital sebagai alat bukti. Alasan efisiensi tidak dapat diterima karena, Jaksa Penuntut Umum menjadikan *hard disk* sebagai barang bukti. Sesungguhnya *hard disk* dalam kasus www.anshar.net ini

dapat dikategorikan alat bukti sebagaimana tercantum dalam Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003. Hal ini menyebabkan tidak efisien penyelesaian perkara. Meskipun pernah barang bukti dalam penyelesaian perkara pidana sangat penting, tetapi perlu diingat, berdasarkan ketentuan dalam Pasal 183 KUHAP suatu barang bukti tidak dapat dijadikan dasar penjatuhan vonis terhadap terdakwa. Dalam kasus tersebut *hard disk* dijadikan barang bukti, maka hard disk tidak memiliki kekuatan pembuktian, karena berapapun saja barang bukti yang diajukan di persidangan mengenai suatu tindak pidana kalau tidak didukung minimal dua alat bukti dan hakim tidak yakin atas kesalahan yang dilakukan terdakwa, maka terdakwa tidak dihukum. Alasan kedua mengenai otentifikasi, bukti digital yang dihasilkan oleh suatu sistem yang berjalan sebagaimana mestinya seharusnya dapat diterima dan memiliki nilai otentik serta memiliki kekuatan dalam hal pembuktian. Karena pada dasarnya bukti digital yang dihasilkan sebuah sistem memiliki sifat yang netral dan objektif. Dengan demikian keraguan terhadap otentifikasi penggunaan bukti

digital tidak lah tepat. Berbeda dengan kasus terorisme terkait dengan website www.anshar.net, terdapat kasus terorisme yang pada penyelesaian perkaranya menerapkan penggunaan bukti digital, yaitu pada kasus Gun Gun Rusman Gunawan alisa Abdul Hadi alias Abdul Karim alias Bukhori terpidana kasus terorisme yang telah diadili di Pengadilan Negeri Jakarta Pusat dengan Nomor Register Perkara 1001/PID.B/2004/PN JKT PST. Dalam kasus tersebut Hakim menerapkan penggunaan alat bukti digital. Alat bukti digital dalam kasus tersebut adalah *log e-mail* terdakwa yang diperoleh dari server utama penyedia layanan e-mail (e-*mail provider*) Yahoo!. *Log* sendiri merupakan informasi terkait pencatatan waktu serta alamat pengiriman email, termasuk isi dari email yang digunakan terdakwa. Jika dikaitkan dengan alat bukti dalam Undang-undang Nomor 15 Tahun 2003, maka alat bukti berupa *log e-mail* tersebut sesuai dengan Pasal 27 huruf c Undang-undang Nomor 15 Tahun 2003.

B. Saran

Saran yang dapat diberikan dalam penulisan ini sebagai berikut.

1. Melakukan revisi terhadap Kitab Undang-undang Hukum Acara Pidana, khususnya mengenai alat bukti yang digukanan dalam persidangan. Diharapkan dalam revisi KUHAP tersebut, bukti digital akan dimasukkan sebagai alat bukti, sehingga penggunaan bukti digital tidak hanya terbatas pada tindak pidana khusus seperti tindak pidana terorisme, tindak pidana pencucian uang, dan tindak pidana korupsi. Tetapi, bukti digital juga dapat digunakan sebagai alat bukti dalam tindak pidana lainnya yang terkandung muatan IT. Bentuk perumusan bukti digital dalam KUHAP dapat mengikuti perumusan bukti digital sebagaimana diatur dalam Pasal 27 Undang-undang Nomor 15 Tahun 2003 tetapi dengan penjelasan bukti digital tersebut merujuk pada istilah Informasi Elektronik dan Dokumen Elektronik sebagaimana diatur dalam Rancangan Undang-undang Tentang Informasi dan Transaksi Elektronik.

2. Agar suatu informasi elektronik memiliki kekuatan pembuktian dan bernilai sebagai alat bukti perlu diperoleh melalui tata cara yang diatur oleh suatu peraturan perundang-undangan atau suatu aturan pelaksanaan. Untuk itu perlu adanya Standar Operasional Prosedur (SOP) yang baku, yang akan dijadikan acuan pelaksaaan perolehan suatu informasi elektronik. Dengan adanya SOP yang baku diharapkan tidak akan merusak atau mengakibatkan berkurangnya nilai otentik serta integritas suatu bukti digital. Untuk sementara, Polri dapat menggunakan SOP yang dibuat oleh *International Organization on Computer Evidence* serta merujuk ketentuan penyitaan sebagaimana diatur dalam KUHAP.
3. Perlu adanya edukasi kepada lembaga dan aparat hukum yang ada yaitu Kepolisian, Kejaksaan dan Kehakiman mengenai perkembangan tindak pidana yang saat ini sudah memasukin era baru, yaitu melalui media Informasi dan Teknologi (IT). Bentuk edukasinya dapat berupa seminar atau *workshop* terkait penggunaan alat bukti berupa informasi elektronik dalam suatu tindak pidana. Edukasi juga dapat berupa penerbita buku

panduan singkat mengenai alat bukti berupa informasi elektronik. Sehingga dikemudian hari dalam menangani kasus terorisme atau kasus tindak pidana lainnya yang terkait IT, Kepolisian, Kejaksaan, dan Hakim tidak perlu ragu dalam menerapkan bukti digital terutama terkait otentifikasi dan integritas dari bukti digital tersebut.

4. Dibutuhkan adanya keterbukaan informasi, terutama akses terhadap dunia pengadilan. Dengan adanya keterbukaan informasi dunia peradilan diharapkan akan mempermudah masyarakat mempelajarai, mengkritisi, produk hukum yang dihasilkan oleh pengadilan. Langkah ini juga merupakan suatu bentuk sosialisasi kepada masyarakat luas agar masyarakat mengetahui berjalannya proses peradilan di Indonesia. Termasuk bagaimana pengadilan memutus suatu perkara terorisme yang terkait dengan aspek IT. Dampak lainnya adalah, memberikan efek jera kepada pelaku tindak pidana terorisme khususnya terorisme terkait IT yang selama ini menyangka tidak ada peraturan perundang-undangan yang dapat menjerat tindak pidana terkait IT.

5. Mempercepat proses pembuatan Rancangan Undang-undang Informasi dan Transaksi Elektronik menjadi Undang-undang. Undang-undang ITE dibutuhkan sebagai perangkat hukum yang berfungsi mendukung pengaturan penggunaan alat bukti digital yang telah ada saat ini. Dengan adanya Undang-undang ITE diharapkan adanya *awareness* dari pihak penyelenggara sistem elektronik untuk selalu menjaga agar sistemnya senantiasa andal, aman, dan berfungsi sebagaimana mestinya. Sehingga apabila suatu waktu diperlukan bukti yang diperoleh dari sistem elektronik mereka, bukti tersebut bernilai sebagai alat bukti yang sah.

DAFTAR PUSTAKA

A. Buku

Afiah, Ratna Nurul. *Barang Bukti dalam Proses Pidana.* Jakarta: Sinar Grafika, 1989.

Anwar, H.A.K. Moch. *Beberapa Ketentuan Umum Dalam Buku Pertama KUHP*. Bandung: Alumni, 1981.

Burke, Jason. *Al-Qaeda: The True Story of Radical Islam*. London: TB. Tauris & Co. Ltd.

Bruce Middleton, Bruce. *Cyber crime investigator's field guide.* Florida: CRC Press LCC, 2002.

Dharmabrata, Wahjadi. *Psykiatri Forensic.* Jakarta: EGC, 2003.

G. Cunningham, William *et. al.*, *Terrorism: Concepts, Causes, and Conflict Resolution*. Virginia: Defense Threat Reduction Agency Fort Belvoir, January 2003.

Graner, Bryan A. *Black's Law Dictionary Eighth Edition*. St. Paul: West Thomson, 2004.

Gregg, Michael. *Certified Ethical Hacker Exam Prep.* United States of America: Que Publishing, 2006.

Hamzah, Andi. *Hukum Acara Pidana Indonesia Edisi Revisi.* Jakarta: Sinar Grafika, 2001.

Hardiman, F. Budi, dkk. *Terorisme, Definisi, Aksi dan Regulasi.* Jakarta: Imparsial, 2005.

Harahap, M. Yahya. *Pembahasan Permasalahan dan Penerapan Kitab Undang-undang Hukum Acara Pidana (KUHAP) Jilid II*. Jakarta: Pustaka Kartini, 1988.

Jones, Robert. *Internet Forensics.* United State of America: O'Reilly Publishing, 2005.

Kuffal, H. F. A. *Penerapan KUHAP di Indonesia*. Malang: UMM Press, 2004.

Lamintang, P. A. F. *Dasar-dasar Hukum Pidana Indonesia* . Bandung: Sinar Baru, 1990.

Loqman, Loebby. *Percobaan Penyertaan dan Gabungan Tindak Pidana*. Jakarta: Universitas Tarumanagara UPT Penerbit, 1995.

Makarim, Edmon. *Pengantar Hukum Telematika: Suatu Kompilasi Kajian.* Jakarta: PT RajaGrafindo Persada, 2005.

Marcella, Albert J. and Robert Greenfield. Cyber Forensics — A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. New York: A CRC Press Company, 2001.

Mansur, Dikdik M Arief dan Elisatris Gultom. *Cyber Law: Aspek Hukum Teknologi Informasi.* Bandung: PT. Refika Aditama, 2005.

Moeljatno. *Asas-Asas Hukum Pidana.* cet. 7. Jakarta: PT. Rineka Cipta, 2002.

Nasrullah, T. *Sepintas Tinjauan Yuridis Baik Aspek Hukum Materil Maupun Formil Terhadap Undang-undang No. 15/2003 Tentang Pemberantasan Tindak Pidana Terorisme.* Makalah Pada Semiloka tentang "Keamanan Negara" yang diadakan oleh Indonesia Police Watch bersama Polda Metropolitan Jakarta Raya.

Pangaribuan, Luhut MP. *Hukum Acra Pidana: Surat-surat Resmi di Pengadilan oleh Advocat*. Jakarta: Djambatan, 2005.

Prakoso, Djoko. *Alat Bukti dan Kekuatan Pembuktian di dalam Proses Pidana*. Yogyakarta: Liberty, 1988.

Prints, Prints. *Hukum Acara Pidana dalam Praktik.* Jakarta: Penerbit Djambatan, 1998.

Prodjodikoro, Wirjono. *Asas-asas Hukum Pidana di Indonesia*. cet. 3. Bandung: PT. Rafika Aditama, 2003.

_____. *Hukum Acara Pidana di Indonesia*. Jakarta: Ghalia, 1982.

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

Remmelink, Jan. *Hukum Pidana: Komentar atas Pasal-Pasal Terpenting dari Kitab Undang-undang Hukum Pidana Belanda dan Padanannya dalam Kitab Undang-undang Hukum Pidana Indonesia*. Jakarta: PT Gramedia Pustaka Umum, 2003.

Rukmini, Mien. *Perlindungan HAM Melalui Asas Praduga Tidak Bersalah dan Asas Persamaan Kedudukan dalam Hukum Pada Sistem Peradilan Pidana Indonesia*. Bandung: PT Alumni, 2003.

Sasangka, Hari dan Lily Rosita, *Hukum Petunjuk dalam Perkara Pidana.* Semarang: Mandar Maju, 2003.

Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York: John Wiley & Sons, 1996.

Sianturi, S. R. *Asas-asas Hukum Pidana di Indonesia dan Penerapannya.* Jakarta: Alumni Ahaem – Petehaem, 1989.

Shinder, Debra Littlejohn Shinder. *Scene of The Cybercrime, Computer Forensics Handbook.* United State of America: Syngress Publishing Inc., 2002.

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

Soetomo, A. Hukum *Acara Pidana Indonesia dalam Praktek*. Jakarta: Pustaka Kartini, 1990.

Sriyanto, I dan Desiree Zuraida. *Modul Instrumen HAM Nasional: Hak Untuk Hidup, Hak Berkeluarga dan Melanjutkan Keturunan Serta Hak Mengembangkan Diri.* Jakarta: Departemen Hukum dan HAM RI, Direktorat Jenderal Perlindungan HAM, 2001.

Suradji, Adjie. *Terorisme*. Jakarta: Pustaka Sinar Harapan, 2005.

Taylor, Mark. *Uses of Encryption: Digital Signatures.* USA: Sweet & Maxwell Limited and Contributors, 1999.

Van Bemmelen, J. M. *Hukum Pidana I: Hukum Pidana Material Bagian Umum*. Diterjemahkan oleh Hasan (tanpa tempat: Bina Cipta, 1984.

Wahid, Abdul, Sunardi, Muhamad Imam Sidik*. Kejahatan Terorisme: Perspektif Agama, HAM dan Hukum.* Bandung: PT. Refika Aditama.

Wahid, Abdul dan Muhammad Labib. *Kejahatan Mayantara (Cybercrime).* Bandung: PT. Rafika Aditama, 2005.

B. Internet

“Bertemu di Dunia Maya, Berakhir di Penjara,” *Sinar Harapan*.<http://www.sinarharapan.co.id/berita/0706/21/nas04.html>. 21 Juni 2007.

“Bom Bali Rencananya untuk Peringati Setahun Bom WTC.” <http://www.kompas.com/kompascetak/0308/22/nasional/505322.htm>. 7 Februari 2007.

“Digital Evidence: Standards and Principle.” <http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm#Definition>. 25 Juni 2007.

“European Convention on Human Rights.” <http://en.wikipedia.org/European_Convention_on_Human_Rights_files>. 26 Desember 2006.

“Electronic Civil Defence.” <http://ntrg.cs.tcd.ie/undergrad/4ba2.02/infowar/ecd.html>. 10 Februari 2007.

“Design space tree of the World Wide Web technology.” <http://newdevices.com/publicaciones/www/ch01.html>. 14 Juni 2007.

“Federal Bureau of Investigation (FBI).” *citation* Adam Savino. “Cyber-Terrorism.” <http://www.cybercrimes.net/Terrorism/ct.html>. 15 Februari 2006.

“FBI Standards and Principles Digital Evidence.” < http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm#IOCEIntroduction>. 20 Juni 2007.

“General purpose *hash* function algorithms (C/C++/Pascal/Java/Python/Ruby).”http://www.partow.net/programming/*hash*functions/index.html.

Gibbs, Jack. “Definition of Terrorism.” <http://en.wikipedia.org/wiki/Definition_of_terrorism>. 25 Februari 2007.

“Gun Gun Rusman, Adik Hambali di vonis Empat Tahun Penjara.”<http://www.detikinet.com/index.php/detik.read/tahun/2004/bulan/10/tgl/26/time/160528/idnews/230900/idkanal/10. 24 Juni 2007.

Bernes-Lee, Tim. “Information Management: A Proposal,” World Wide Web Consortium (W3C). <www.w3c.org>, 12 Juni 207.

“Empat Tahun Penjara Untuk Adik Hambali.”< http://www.korantempo.com/news/2004/10/27/nasional/18.html>. 24 Juni 2007.

“International Review of Criminal Policy.” *United Nations Manual on the Prevention and Control of Computer-Related Crime.* <http://www.uncjin.org/Documents/EighthCongress.html>. 20 Juni 2007.

“Imam Samudra Sempat Kendalikan Jaringan Terorisme dari Penjara.”<http://www.kompas.com/ver1/Nasional/0608/23/183643.htm>. 25 Agustus 2006.

“Max Bukan Jaringan Noordin,” <http://www.suaramerdeka.com/harian/0703/27/nas17.htm. 10 Juni 2007.

“Pengacara TPM Dampingi Tersangka Pembuat Laman www.anshar.net.” <http://www.antara.co.id/news>. 1 November 2006.

“Pembuat situs www.anshar.net Divonis 3 Tahun Penjara.” <http://www.okezone.com/Pembuat%20Situs%20Anshar%20Divonis%203%20Tahun>. 20 Juni 2007

Pitoyo, Arif. ”Perlunya Penyempurnaan Hukum Pidana Tangani Cybercrime.”<http://gerbang.jabar.go.id/gerbang/index.php?index=16&idberita=680>. 22 Januari 2007.

Rösler-Garcia, Peter. “Terorisme, Anak Kandung Ekstremisme”, <http://www.kompas.com/kompas-cetak/0210/15/opini/tero30.htm>, diakses 20 Februari 2007.

Request for Comment. “Hypertext Transfer Protocol -- HTTP/1.0,” <http://tools.ietf.org/rfc/rfc1945.txt>. 10 Juni 2007.

Request For Comment. “Hypertext Transfer Protocol -- HTTP/1.1,” <http://tools.ietf.org/rfc/rfc2616.txt>. 10 Juni 2007.

“Situs 'Teroris' Anshar.Net Akan Diblokir Polri.”<http://jkt.detiknews.com/index.php/detik.read/tahun/2005/bulan/11/tgl/22/time/154522/idnews/483936/idkanal/10>. 22 September 2005.

HTTP Performance Overview. <http://www.w3.org/Protocols/HTTP/Performance/>. 11 Juni 2007.

http://www.state.gov/s/ct/c14151.htm. Juni 2006.

http://en.wikipedia.org/wiki/Cyber-terrorism. 10 Februari 2007.

http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm# International.

http://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf

http://library.thinkquest.org/C0126342/ceaser.htm

http://tools.ietf.org/html/rfc1321.

http://www.cryptography.com/cnews/*hash*.html.

http://www.cryptodox.com/MD5.

http://www.metrotvnews.com/berita.asp?id=40825.

http://www.suaramerdeka.com/harian/0706/21/nas14.htm.

“HTTP Authentication: Basic and Digest Access Authentication.” <ftp://ftp.isi.edu/in-notes/rfc2617.txt>. 10 Juni 2007.

The Britanica On-line Encyclopedia. <http://www.britannica.com/eb/article9071797/terrorism>. 21 Februari 2007.

Tyson, Jeff. “How Encryption Works.” <http://computer.howstuffworks.com/encryption1.htm>. 20 Juni 2007.

Wikipedia Online Encyclopedia “Definiton of Source Code.” <http://en.wikipedia.org/wiki/Source_code>. 23 Desember 2006.

Weimann, Gabriel. “www.terror.net: How Modern Terrorism Uses the Internet.” <http://www.usip.org/pubs/specialreports/sr116.pdf>.

“Web Growth Summary.” <http://www.mit.edu/people/mkgray/net/>. 14 Juni 2007.

World Wide Web Consortium (W3C). “About the World Wide Web Consortium (W3C).” <http://www.w3.org/Consortium/>. 14 Juni 2007

Zhang. <http://www.slais.ubc.ca/courses/libr500/04-05-wt1/www/X_Zhang/5ways.htm>. 15 Februari 2007.

C. Jurnal

Brenner, Susan W. “Cybercrime Metrics: Old Wine, New Bottles?” *Virginia Journal of Law & Technology* (Fall 2004): 14.

Golder, Ben and George Williams. “What is ‘Terrorism’? Problems of Legal Definition.” *UNSW Law Journal Vol. 27(2)* (February 2003): 202-286.

Hancock, Nathan. “Terrorism and the Law in Australia: Legislation, Commentary and Constraints.” *Research Paper No 12, Commonwealth Parliament* (02-2001).

Humphreys, Adrian. "One official's 'refugee' is another's 'terrorist'." *National Post* (January 2006).

Khan, Ali. “A Legal Theory of International Terrorism,” *Connecticut Law Review* (1982):1-18.

Record, Jeffrey. “Bounding The Global War On Terrorism.” *Strategic Studies Institute* (December 2003): 1-23.

Lewis, James A. “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.” *Center of Strategic & International Studies* (December 2002).

_____..“Internet and Terrorism,” *Center of Strategic & International Studies* (April 2005).

Withcomb, Carrie Morgan. “An Historical Perspective of Digital Evidence: A Forensic Scientist’s View,” *International Journal of Digital Evidence* (Spring 2002, Vol. 1, Issue 1).

Weimann, Gabriel. “Cyberterrorism: How Real Is the Threat?” *USIP Special Report No. 119* (December 2004), <http://www.usip.org/pubs/specialreports/sr119.html>.

D. Peraturan Perundang-undanangan

Indonesia. *Undang-Undang Tentang Hukum Acara Pidana (KUHAP)*. UU No. 8, LN. No. 76 Tahun 1981, TLN. 3209.

Indonesia. *Undang-undang Tentang Penetapan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme, Menjadi Undang-undang*. UU No. 15, LN. No. 45 Tahun 2003, TLN. No. 4284, Penjelasan umum Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme.

Indonesia. *Undang-undang tentang Komisi Pemberantasan Tindak Pidana Korupsi*. UU No. 30, LN No. 137 Tahun 2002, TLN. No. 4250.

Indonesia, *Undang-undang Tentang Tindak Pidana Pencucian Uang*, UU No. 15, LN. No. 30 Tahun 2002, TLN No.

Indonesia. *Rancangan Undang-undang Tentang Informasi dan Transaksi Elektronik*.

Kitab Undang Undang Hukum Pidana. Prof.Moeljanto, S.H., cet. 21. Jakarta: Bumi Aksara, 2001.

Departemen Kehakiman Republik Indonesia. *Pedoman Pelaksanaan KUHAP*.