Jurnal Judiciary
Vol. 1, No 1 (2018)

SISTEM PEMBUKTIAN DALAM TINDAK PIDANA *NETWORK CUT*

S. Masribut Sardol

Abstrak

Network cut adalah salah satu bentuk kejahatan *cyber crime*, penggunaannya sangat mudah tinggal *download, install, next* terus, *restart* komputer. *Network cut* memanage jaringan berdasar protokol ARP, membuat *list* IP-MAC, mematikan dan menghidupkan koneksi ke jaringan pada komputer yang terhubung dalam LAN juga dapat mematikan dan menghidupkan perangkat jaringan seperti *router, switch*.

Kata kuci: pembuktian, pidana, *network cut*

A. Pendahuluan

Peradaban dunia pada masa kini dicirikan dengan fenomena kemajuan teknologi informasi dan globalisasi yang berlangsung hampir disemua bidang kehidupan. Apa yang disebut globalisasi pada dasarnya bermula dari abad ke-20, yakni pada saat terjadi revolusi transportasi dan elektronika yang menyebarluaskan dan mempercepat perdagangan antar bangsa, disamping pertambahan dan kecepatan lalu lintas barang dan jasa.

Dalam rangka menghadapi pembukaan pasar regional oleh AFTA pada tahun 2003 dan dalam rangka menghadapi liberalisasi perdagangan WTO pada tahun 2010, negara-negara yang aktif terlibat dalam praktik perdagangan internasional mulai membentuk instrumen

hukum yang mengatur masalah prilaku perusahaan dan individu-individunya agar tidak menyalahkan *market power*-nya. Deregulasi dalam liberalisasi diharapkan dapat menciptakan mekanisme pasar yang sehat. Aspek-aspek pendukung seperti ilmu pengetahuan, teknologi informasi, infrastruktur dan sistem sosial yang berkembang secara dinamis mengikuti proses globalisasi merupakan aspek pendukung dalam pembentukan instrumen hukum tersebut.[1]

Menurut **Didik J, Rachbini**, teknologi informasi dan media elektronika dinilai sebagai simbol pelopor, yang akan mengintegrasikan seluruh sistem dunia, baik dalam aspek sosial, budaya, ekonomi dan keuangan. Dari sistem-sistem kecil lokal dan nasional, proses globalisasi dalam tahun-tahun terakhir bergerak cepat, bahkan terlalu cepat menuju suatu sistem global. Dunia akan menjadi "*global village*" yang menyatu, saling tahu dan terbuka, serta saling bergantung satu sama lain.

Penggabungan komputer dengan telekomunikasi melahirkan suatu fenomena yang mengubah konfigurasi model komunikasi konvensional, dengan melahirkan kenyataan dalam dimensi ketiga. Jika dimensi pertama adalah kenyataan keras dalam kehidupan empiris (biasa disebut *hard reality*), dimensi kedua merupakan kenyataan dalam kehidupan simbolik dan nilai-nilai yang dibentuk (dipadankan dengan *soft reality*), maka dengan dimensi ketiga dikenal kenyataan maya (*virtual reality)* yang melahirkan format masyarakat lainnya.

[1] Dikdik M.Arief Mansur, *Cyber Law Aspek HukumTeknologi Informasi*, PT. Refika Aditama, Bandung, 2009, hal 1

Berkenaan dengan pembangunan teknologi, dewasa ini seperti kemajuan dan perkembangan teknologi informasi melalui *internet* (*inter connection network),* peradaban manusia dihadapkan pada fenomena baru yang mampu mengubah hampir setiap aspek kehidupan manusia. Pembangunan dibidang teknologi (dengan segala aspek pendukungnya) diharapkan akan membawa dampak positif bagi kehidupan manusia, yang pada akhirnya akan bermuara pada terciptanya peningkatan kesejahteraan umat manusia.[2]

Bersamaan dengan perkembangan teknologi informasi melalui *internet*, dibarengi pula dengan dampak negatif yang sangat luas dampak negatif tersebut lebih dikenal dengan kejahatan-kejahatan baru didunia maya. Bentuk-bentuk kejahatan didunia maya salah satunya adalah tindak pidana *network cut* dimana cukup sulit untuk menjerat para pelakunya yang berhubungan dengan sistem pembuktian tindak pidana tersebut.

Alat bukti yang digunakan sesuai dengan Pasal 44 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik selanjutnya disebut UU ITE, huruf (a) mengacu pada Pasal 184 ayat (1) KUHAP, bahwa alat bukti yang sah adalah :

a) Keterangan saksi.
b) Keterangan ahli
c) Surat.
d) Petunjuk.

[2] Didik J Rachbini, *Mitos dan Implikasi Globalisasi: Catatan Untuk Bidang Ekonomi Dan Keuangan*,Yayasan Obor, Jakarta, 2001, hal 2

e) Keterangan terdakwa.[3]

Sedangkan alat bukti dalam kasus *network cut* ini keseluruhan merupakan angka-angka digital dan data-data elektronik. Dengan alat bukti semacam itu (data-data digital) Pasal 184 ayat (1) KUHAP sebagai hukum acara pidana tidak mengatur secara eksplisit.

Dalam Pasal 44 UU ITE huruf (b) dinyatakan bahwa terdapat alat bukti lain berupa informasi elektronik dan/ dokumen elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 informasi elektronik satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, EDI, surat elektronik, telegram, teleks, telecopy, atau sejenisnya, huruf, tanda, angka, kode akses, symbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Angka 4 dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, atau sejenisnya, huruf , tanda, angka, kode akses, symbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. Serta Pasal 5 ayat (1) informasi elektronik dan/atau dokumen elektronik dan/hasil cetaknya merupakan alat bukti hukum yang sah. Ayat (2) informasi elektronik

[3]*Op cit* hal 101

dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Ayat (3) informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam undang-undang ini.

Tindak pidana *network cut* adalah memotong akses internet pada *public/private WIFI hotspot*, ataukah sebuah PC LAN *workgroup* dari *client* ke *server* atau sebaliknya. Tindak pidana *network cut* pada umumnya dipergunakan oleh pengguna jaringan yang ingin mengambil *quota* (jatah) *bandwith* untuk dipakai sendiri tanpa mau dishare kepada *client* yang lain.

B. Rumusan Masalah

Berdasarkan penjabaran diatas maka rumusan masalahnya adalah sebagai berikut:

1. Bagaimana keterkaitan tindak pidana *network cut* dengan *hacking* ?
2. Bagaimana sistem pembuktian dalam tindak pidana *network cut* ?

C. Pembahasan

1. Keterkaitan Tindak Pidana *Network Cut* dengan *Hacking*

Pengertian dari *hacking* adalah suatu tindakan memperluas jaringan komputer secara tidak sah dengan jalan menyambungnya dengan jaringan komputer yang sudah ada tanpa izin dari pemilik jaringan tersebut, sehingga terjadilah jalinan rangkaian jaringan

komputer antara yang sah dan yang tidak sah. Kejahatan *hacking* ini sangat banyak terjadi dan sangat ditakuti dalam praktek. Sebab, dengan perbuatan *hacking* ini, data bisa hilang atau dicuri orang, sehingga berpotensi akan adanya kerugian.[4]

Tindak pidana *network cut* adalah memotong akses jaringan internet pada *public/private WIFI hotspot*, ataukah sebuah PC LAN *workgroup* dari *client* ke *server* atau sebaliknya. Tindak pidana *network cut* pada umumnya dipergunakan oleh pengguna jaringan yang ingin mengambil *quota* (jatah) *bandwith* untuk dipakai sendiri tanpa mau *dishare* kepada *client* yang lain. Berdasarkan pengertian mengenai *hacking* dan *network cut* diatas dapat kita ketahui bahwasannya cara kerja kejahatan *network cut* memotong jaringan internet pada *public/private WIFI hotspot*, ataukah sebuah PC LAN *workgroup* dilakukan tanpa sepengetahuan pemilik jaringan tersebut yang berakibat tidak bisa diaksesnya internet secara sempurna. Hal tersebut sama dengan *hacking* karena perbuatan *hacking* dilakukan tanpa sepengetahuan pemilik jaringan. Berbagai macam akibat yang ditimbulkan oleh *hacking* seperti dicurinya data-data, dimasukkannya virus kedalam komputer, mengganggu sistem jaringan, akibat tersebut lebih besar dibandingkan dengan kejahatan *network cut*. Dalam hal ini bisa diartikan bahwa kejahatan *network cut* adalah bagian dari *hacking* yaitu yang keduanya sama-sama bertujuan untuk merusak privasi

[4] Munir Fuady, *Bisnis kotor Anatomi Kejahatan Kerah Putih*, PT. Citra Aditya Bhakti, Bandung, 2004, hal 131

pemilik jaringan (*client*). Kejahatan *network cut* bisa disamakan juga dengan *cracker*.[5]

Kemampuan *hacking* bagi seorang *hacker* atau *cracker* bukanlah kemampuan yang diperoleh secara singkat atau instant. Proses belajar dan diskusi dengan kalangan *hacker* adalah kata kunci untuk memiliki kemampuan itu. Kemampuan itu juga tidak berarti apabila tidak pernah digunakan atau dieksploitasi. Penguasaan bahasa pemrograman, sistem operasi dan eksperimen akan semakin meningkatkan kemampuan *hacker* atau *cracker* dalam masalah *hacking.*

Seorang *hacker* atau *cracker* apabila hendak melakukan *hacking* tidak dilakukan secara sembarangan, artinya ada motif atau niat tertentu dibalik *hacking* itu. Peralatan untuk melakukan *hacking*, seorang *hacker* atau *cracker* dapat menggunakan komputer sederhana atau minimal yang bisa dipakai untuk mengakses internet meskipun semakin baik atau tinggi kemampuan komputer yang dipakai akan semakin baik proses dan hasilnya. Hal ini tidak bisa terlepas dari ciri atau sifat *hacker* yang selalu berusaha untuk melakukan sesuatu yang melebihi kemampuan aslinya (dalam hal ini kemampuan komputer itu).

Selain motif atau niat dan komputer yang dipakai, maka langkah atau tahap yang harus dilalui oleh seorang *hacker* atau *cracker* untuk melancarkan aksinya adalah sebagai berikut.

[5] Andri Kristanto, *Hacker Vs Cracker,* Cable Book, Klaten, 2010, hal 65

1. Menggumpulkan dan mempelajari informasi yang ada mengenai sistem operasi komputer atau jaringan komputer yang dipakai pada target sasaran.

Pengetahuan mengenai sistem operasi yang dipakai ini penting karena akan membantu *hacker* atau *cracker* dalam mengeksploitasi kelemahan sistem operasi target sasaran. Para *hacker* atau *cracker* biasanya menggunakan UNIX atau Windows berbagai variannya seperti *RedHat, FreeBSD. Slackware* maupun *OpenBSD*, meski demikian banyak juga program *hacker* yang ditulis untuk windows bahkan DOS. Akan tetapi *hacker* yang benar-benar serius menggunakan UNIX atau linux karena fasilitas atau perintah untuk jaringan yang lebih baik.

Cara yang lebih muda adalah dengan menggunakan 1 (satu) unit komputer, akses ke internet, telnet dan untuk mempermudah atau memperlancar dapat digunakan program khusus, seperti *prefix scanner, port scanner, daemon dialer* atau *war dialer.*

Cara lainnya adalah dengan mencari sasaran diantara komputer-komputer *host* yang ada. Pada saat ini yang dicari bukanlah komputernya, melainkan pintu masuk (*port*) yang bisa dimanfaatkan dalam sistem operasi komputer itu. *Port* atau pintu masuk ini berupa jalur-jalur keluar masuknya data dari dan kesuatu komputer. Pengaksesan komputer melalui *port* disebut *port surfing.* Pencarian *port* dapat dilakukan dengan program khusus yang disebut *port scanner*, seperti *rebellion, part pro,* dan *port scanner*. *Port scanner* adalah suatu alat yang berfungsi untuk men-scan berbagai macam *port* dalam suatu *client* itulah *hacker* bisa masuk kedalamnya.

Selain hal tersebut diatas seorang *hacker* atau *cracker* juga memerlukan pengetahuan tentang *whois, nslookup, ping* dan *traceroute* untuk mengetahui suatu sistem operasi komputer ditarget sasaran. *Whois* biasanya digunakan untuk mencari nama-nama domain yang ada di internet, tetapi dapat digunakan juga untuk mencari informasi berharga tentang suatu server. *Nslookup* digunakan untuk melihat (*look up*) alamat dari nama domain dari suatu alamat *internet protocol* (IP *address*). *Ping* adalah suatu perintah pengiriman suatu paket yang berisi sejumlah *byte* dari suatu *client* ke *client* yang lain sampai kembali ke si pengirim, sedangkan *traceroute* adalah suatu perintah yang bekerja seperti *ping*, tetapi ia akan menunjukkan masing-masing *router* yang dilewati dan melewati *client* tersebut. *Tracerouter* biasanya diperlukan untuk melacak komputer yang berada dalam sistem jaringan.

2. Menyusup atau mengakses jaringan komputer target sasaran

Untuk masuk atau mengakses jaringan komputer target sasaran dapat dilakukan dengan menaklukkan atau menipu sistem pengaman yang ada pada jaringan komputer. Ada beberapa cara untuk menembus sistem pengaman yang ada pada jaringan komputer, diantaranya adalah *social engineering*, menebak dan memecah *password*, menyadap *password*, mengeksploitasi kelemahan pada sistem sasaran dan *trashing.*

3. Menjelajah sistem komputer (mencari akses yang lebih tinggi)

Setelah seorang *hacker* berada dalam sebuah sistem, ia kemungkinan akan berkeliling, melihat-lihat isi dari sistem yang baru

saja dimasukinya dan mencoba perintah untuk mengetahui fungsinya. Salah satu perintah yang paling sering digunakan dalam sistem UNIX adalah perintah *is.* Perintah ini serupa dengan perintah dir pada DOS, yang gunanya untuk melihat isi direktori. Perintah lain yang banyak digunakan adalah man, yang digunakan untuk menampilkan *manual online* dari suatu perintah.

4. Membuat *backdoor* dan menghilangkan jejak

Seorang *hacker* atau *cracker* yang ahli akan berusaha agar aksi dan keberadaannya tidak diketahui oleh pemilik sistem yang dimasukinya, sebab jika ketahuan urusannya akan panjang apalagi jika tertangkap, ujungnya pasti tidak enak. Berkaitan dengan waktu pengguna, cara untuk memperkecil kemungkinan terdeteksi adalah dengan melakukan aktivitasnya disaat sistem yang akan dimasukinya tidak atau kurang diawasi. Berkaitan dengan teknik, salah satu cara yang paling umum adalah mengedit file-file *log (*catatan aktivitas*)* pada sistem yang dimasukinya dan menghilangkan semua entry yang berkaitan dengan dirinya. Aktivitas yang berlangsung selama *hacking* misalnya aktivitas *scanning.*[6]

2. Sistem Pembuktian dalam Tindak Pidana *Network Cut*

[6] Agus Raharjo, op.cit, hal 169

Dalam kaitannya dengan hubungan hukum yang terjadi didunia *cybercrime* dalam kaitannya dengan *network cut*, yang menjadi pertanyaan adalah apakah untuk pembuktian tentang berbagai peristiwa hukum yang terjadi di *cybercrime* dapat diterapkan kaidah-kaidah hukum di dunia non virtual.

Keberadaan Undang-undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan telah mulai menjangkau ke arah pembuktian data elektronik. Dalam Undang-undang Dokumen Perusahaan meskipun tidak mengatur masalah pembuktian, namun melalui Undang-undang ini, pemerintah berusaha mengatur pengakuan atas *microfilm* dan media lainnya (alat penyimpanan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan misalnya *Compact Disk-Read Only Memory* (CD-ROM) dan *Write-One-Read-Many* (WORM), yang diatur dalam Pasal 12 Undang-undang Dokumen Perusahaan sebagai alat bukti yang sah.

Pasal 12 Undang-undang Dokumen Perusahaan berbunyi sebagai berikut:

1. Dokumen perusahaan dapat dialihkan kedalam *microfilm* atau media lainnya.
2. Pengalihan dokumen perusahaan kedalam *microfilm* atau media lainnya sebagaimana dimaksud dalam ayat (1) dapat dilakukan sejak

dokumen tersebut dibuat atau diterima oleh perusahaan yang bersangkutan.

3. Dalam mengalihkan dokumen perusahaan sebagaimana dimaksud dalam ayat (1), pimpinan perusahaan wajib mempertimbangkan kegunaan naskah asli dokumen yang perlu tetap disimpan karena mengandung nilai tertentu demi kepentingan perusahaan atau demi kepentingan nasional.
4. Dalam hal dokumen perusahaan yang dialihkan kedalam *microfilm* atau sarana lainnya adalah naskah asli yang mempunyai kekuatan hukum pembuktian otentik dan masih mengandung kepentingan hukum tertentu, pimpinan perusahaan wajib tetap menyimpan naskah asli tersebut.[7]

Di samping itu, Pasal 3 Undang-undang Dokumen Perusahaan telah memberi peluang luas terhadap pemahaman atas alat bukti, yaitu: "dokumen keuangan terdiri dari catatan, bukti pembukuan, dan data pendukung administrasi keuangan, yang merupakan bukti adanya hak dan kewajiban serta kegiatan usaha suatu perusahaan." Selanjutnya, dalam Pasal 4 menyatakan "dokumen lainnya terdiri dari data atau setiap tulisan yang berisi keterangan yang mempunyai nilai guna bagi perusahaan meskipun tidak terkait langsung dengan dokumen perusahaan."

[7] Dikdik M. Arief Mansur, op.cit, hal 108

Sebuah dokumen perusahaan baru mempunyai kekuatan sebagai alat bukti setelah dilakukan proses pengalihan yang kemudian dilanjutkan dengan proses legalisasi, yang diatur dalam Pasal 13 dan 14 Undang-undang Dokumen Perusahaan. Setelah proses pengalihan dan legalisasi, dokumen perusahaan tersebut dinyatakan sebagai alat bukti yang sah, sebagaimana tersebut dalam Pasal 15 Undang-undang Dokumen Perusahaan.

Berkenaan dengan hukum pembuktian dalam proses peradilan baik dalam perkara pidana maupun perdata, mengenai keabsahan transaksi dan kekuatan pembuktian, transaksi elektronik tidak memerlukan *hard copy* atau warkat kertas, namun demikian setiap transaksi yang melibatkan eksekusi diberikan tanda bukti berupa nomor atau kode yang dapat disimpan atau direkam dikomputer atau dicetak.

Di Indonesia sendiri terdapat putusan pengadilan yaitu putusan MARI Nomor 9/KN/1999, yang dalam putusannya hakim menerima hasil *print out* sebagai alat bukti surat. Kemudian kasus pidana yang diputus di pengadilan Negeri Jakarta Timur mengetengahkan bukti e-mail (*elektronik mail*) sebagai salah satu alat bukti.setelah mendengar keterangan ahli bahwa dalam transfer data melalui *e-mail* tersebut tidak terjadi tindakan manipulatif hakim memvonis terdakwa dengan hukuman satu tahun penjara.[8] Berbagai macam trobosan hukum dilakukan untuk menjerat pelaku kejahatan didunia maya sebelum

[8]http://www.hukumonline.com/artikel_detail asp?id=8034> Diakses Tanggal 10 Juni 2011

disahkannya UU ITE. Setelah disahkannya UU ITE maka alat bukti elektronik merupakan perluasan alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia.

Di dalam Pasal 44 UU ITE huruf (b) dinyatakan bahwa terdapat alat bukti berupa informasi elektronik dan/ dokumen elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 informasi elektronik satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, EDI, surat elektronik, telegram, teleks, telecopy, atau sejenisnya, huruf, tanda, angka, kode akses, symbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Angka 4 dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, atau sejenisnya, huruf , tanda, angka, kode akses, symbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. Serta Pasal 5 ayat (1) informasi elektronik dan/atau dokumen elektronik dan/hasil cetaknya merupakan alat bukti hukum yang sah. Ayat (2) informasi elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Ayat (3) informasi elektronik dan/atau dokumen

elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam Undang-undang ini.

Tindak pidana *network cut* adalah memotong akses internet berupa kode akses dalam bentuk angka-angka digital pada *public/private WIFI hotspot*, ataukah sebuah PC LAN *workgroup* dari *client* ke *server* atau sebaliknya. Dengan menggunakan kode akses dalam bentuk angka-angka digital sesuai dengan macam-macam alat bukti elektronik dalam UU ITE maka, alat bukti elektronik tersebut dapat digunakan sebagai alat bukti dalam tindak pidana *network cut.*

Pada dasarnya pemeriksaan dalam persidangan pengadilan adalah semua kegiatan pengungkapan fakta-fakta dari sesuatu peristiwa yang lalu. Bila fakta-fakta tersebut dirangkai dapat menggambarkan suatu peristiwa yang sebenarnya atau setidak-tidaknya mendekati kebenaran materiil untuk dapat dipastikan atau tidaknya muatan tindak pidana dalam peristiwa tersebut menurut akal sebagaimana yang didakwakan JPU.

Dalam sidang pengadilan pidana terdapat tiga pihak, yakni majelis hakim berikut panitera pengganti, JPU, dan terdakwa (dapat) didampingi oleh penasihat hukum. Dalam usaha pengungkapan/pengalihan fakta, masing-masing pihak akan berusaha dengan sebaik-baiknya untuk untuk mendapatkan fakta yang sesuai dengan fungsi dan tugasnya. Oleh sebab itu, tiga pihak akan mengarahkan pemeriksaan dalam sidang melalui pertanyaan-pertanyaan pada saksi dan terdakwa serta dialog maupun perdebatan satu dengan

yang lain untuk memperoleh fakta hukum yang menguntungkan dari sudut fungsi dan tugasnya.[9]

Majelis hakim mengarahkan persidangan untuk mendapatkan fakta-fakta sebenarnya, baik yang meringkan atau memberatkan kesalahan dan beban pertanggungjawaban pidana terdakwa. Fakta-fakta tersebut pada akhirnya dirangkai hingga menggambarkan suatu peristiwa yang sesungguhnya terjadi untuk dapat dipastikan benar atau tidaknya telah terjadi tindak pidana yang didakwakan terdakwa dalam peristiwa tersebut berdasarkan syarat-syarat pembuktian dan akal.

JPU akan mengarahkan persidangan untuk mendapatkan fakta-fakta yang akan dirangkai menjadi suatu gambaran peristiwa yang sebenarnya, yang mengandung muatan tindak pidana sebagaimana yang didakwakan dalam peristiwa tersebut.

Sedangkan PH akan berusaha mendapatkan fakta hukum yang dapat dirangkai menjadi suatu peristiwa yang sebenarnya tidak mengandung muatan tindak pidana sebagaimana yang didakwakan, atau menjadi suatu peristiwa yang sebenarnya dapat menghapuskan kesalahan dan atau sifat melawan hukumnya perbuatan, atau setidak-tidaknya dapat meringankan kesalahan dan beban pertanggungjawaban pidana terdakwa. Seluruh rangkaian kegiatan dalam persidangan yang dilakukan dan diikuti oleh tiga pihak tersebut dapat juga disebut dengan kegiatan atau proses pembuktian disidang pengadilan. Bagi majelis hakim sebagai

[9] Adami Chazawi, *Kemahiran Dan Keterampilan Praktik Hukum Pidana*, Banyumedia Publishing, Malang, hal 199

pimpinan sidang dan pemutus perkara, hasil pembuktian akan berakhir pada titik kesimpulan sebagai berikut:

1. Terbukti atau tidaknya tindak pidana yang didakwakan JPU.
2. apabila terbukti, seberapa berat kadar kesalahan terdakwa sehingga dapat ditetapkan sejauh mana beban pertanggungjawaban pidana terdakwa yang menimbulkan peristiwa yang mengandung muatan tindak pidana yang didakwakan tersebut.
3. Apabila tidak terbukti, maka diikuti amar pembebasan terdakwa.

Namun sebelum majelis hakim sampai pada titik akhir tersebut, sebagai pendakwa wajib JPU dapat membuktikan dan meyakinkan majelis hakim bahwa telah terjadi tindak pidana dakwaan dan terdakwa bersalah melakukannya. Kewajiban JPU tersebut berlandaskan prinsip dasar sistem pembebanan pembuktian "siapa yang mendakwakan sesuatu, maka dialah yang harus membuktikan" dan sistem pembuktian negatif menurut UU yang terbatas (*negatief wettelijke*) yang dianut KUHAP.

D. Kesimpulan

Dari pembahasan diatas, maka penulis memberikan kesimpulan sebagai berikut:

1. Perbedaan *hacker*, *cracker* dengan *bogus hacker* yang utama dalam hal niat, kemampuan, sifat, dan etika. Berdasarkan pengertian mengenai *hacking* dan *network cut* diatas dapat kita ketahui bahwasannya cara kerja kejahatan *network cut* memotong jaringan internet pada

public/private WIFI hotspot, ataukah sebuah PC LAN *workgroup* dilakukan tanpa sepengetahuan pemilik jaringan tersebut yang berakibat tidak bisa diaksesnya internet secara sempurna. Hal tersebut sama dengan *hacking* karena perbuatan *hacking* dilakukan tanpa sepengetahuan pemilik jaringan. Berbagai macam akibat yang ditimbulkan oleh *hacking* seperti dicurinya data-data, dimasukkannya virus kedalam komputer, mengganggu sistem jaringan, akibat tersebut lebih besar dibandingkan dengan kejahatan *network cut*. Dalam hal ini bisa diartikan bahwa kejahatan *network cut* adalah bagian dari *hacking* yaitu yang keduanya sama-sama bertujuan untuk merusak privasi pemilik jaringan (*client*). Kejahatan *network cut* bisa disamakan juga dengan *cracker.*

2. Alat bukti dalam tindak pidana *network cut* disamping mengacu pada Pasal 184 ayat (1) KUHAP juga pada UU yang bersifat khusus yaitu Pasal 44 UU ITE dengan sistem pembuktian. Tindak pidana *network cut* adalah memotong akses internet berupa kode akses dalam bentuk angka-angka digital pada *g*, ataukah sebuah PC LAN *workgroup* dari *client* ke *server* atau sebaliknya. Dengan menggunakan kode akses dalam bentuk angka-angka digital sesuai dengan macam-macam alat bukti elektronik dalam UU ITE maka, alat bukti elektronik tersebut dapat digunakan sebagai alat bukti dalam tindak pidana *network cut* dan untuk menemukan pelaku tindak pidana *network cut* dapat dilakukan dengan menggunakan *billing* atau *remote desktop* pada PC LAN *workgroup* pada admin atau *server*.

E. Daftar Pustaka

Buku

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

Adami Chazawi, *Kemahiran Dan Keterampilan Praktik Hukum Pidana*, Banyumedia Publishing, Malang.

Agus Raharjo, *Cyber crime Pemahaman Dan Upaya Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung, 2002.

Andi Hamzah, *Hukum Acara Pidana Indonesia*, Sinar Grafika, Jakarta, 2006.

Barda Nawawi Arief, *Beberapa Aspek Kebijakan Penegakan Dan Pengembangan Hukum Pidana*, Citra Aditya Bhakti, Bandung, 1998.

Dikdik M.Arief Mansur, *Cyber Law Aspek HukumTeknologi Informasi*, PT. Refika Aditama, Bandung, 2009.

Didik J Rachbini, *Mitos dan Implikasi Globalisasi: Catatan Untuk Bidang Ekonomi Dan Keuangan,*Yayasan Obor, Jakarta, 2001.

D. Simons, *Beknopte Hard Tot Het Wetbook Van Strafvordering*, Harlem, De Erven f.bohn, 1925.

Lain-lain

http://www.cs.utah.edu/elb/node3.html Diakses Tanggal 20 Mei 2011

http://www.im.lcs.mit.edu/gilliam/hacker-one.html Diakses Tanggal 26 Mei 2011

http://www-mitpress.mit.edu/seb/book-home/026280920.htm Diakses Tanggal 27 Mei 2011

Munir Fuady, *Bisnis kotor Anatomi Kejahatan Kerah Putih*, PT. Citra Aditya Bhakti, Bandung, 2004, hal 131[1] Andri Kristanto, *Hacker Vs Cracker,* Cable Book, Klaten, 2010.

http://www.hukumonline.com/artikel_detail asp?id=8034> Diakses Tanggal 10 Juni 2011

http://islam-download.net/tag/fungsi-remote-desktop Diakses Tanggal 18 Juni 2011