# BAB IV

# ANALISIS HUKUM ATAS TINDAK PIDANA *CRACKING* MENGGUNAKAN *BOTNET* TERHADAP SISTEM KOMPUTER BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

## A. Ketentuan Hukum Mengenai Tindak Pidana *Cracking* Menggunakan *Botnet* Terhadap Sistem Komputer Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Pesatnya teknologi informasi melaui internet telah mengubah aktivitas-aktivitas kehidupan yang semula perlu dilakukan secara kontak fisik, kini dengan menggunakan media *cyberspace*, aktivitas keseharian dapat dilakukan secara vitual atau maya. Masalah rumit yang dihadapi penegak hukum saat ini adalah bagaimana menjaring pelaku *cybercrime* yang mengganggu rasa keadilan tersebut dikaitkan dengan ketentuan pidana yang berlaku.

KUHP tidak mampu mengkoordinir segala bentuk kejahatan yang sudah berkembang pesat. Hal ini karena KUHP merupakan produk lama sementara *cybercrime* merupakan dunia masa kini yang mengandalkan teknologi tinggi. Untuk itulah diperlukan perangkat hukum yang baru pula untuk mengimbangi perkembangan zaman yang tanpa sadar telah melampaui jangkauan ketentuan hukum yang ada. Hukum diyakini sebagai alat untuk memberikan kepastian

hukum dalam pergaulan hidup. Layaknya suatu alat, hukum akan dibutuhkan jika kemudian timbul suatu kebutuhan atau keadaan yang luar biasa dalam masyarakat. Maka, disahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang diharapkan mampu menutupi setiap kejahatan berteknologi tinggi.

Teknologi informasi telah berkembang pesat dalam berbagai bidang, tidak terkecuali bidang kejahatan yang sekarang sudah sering dilakukan melalui teknologi informasi. Oleh karena itu negara harus menciptakan sistem keamanan agar tidak terjadi hal yang merugikan kepada masyarakat pengguna teknologi informasi. Hal ini berdasarkan Pasal 40 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

> "Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan".

*Botnet* adalah salah satu bentuk *cyber crime* yang tergolong baru yang dilakukan tersangka melakukan tindak pidana *cracking* melalui *botnet* adalah perbuatan melawan hukum dengan ranah hukum pidana. *Botnet* adalah suatu program yang berbahaya yang dapat menyusup dalam jaringan komputer. Program tersebut dapat dikendalikan dari jarak jauh *(remote)* sehingga dapat dioperasikan secara lintas negara (transnasional). Pelaku dan korban dapat berada di negara yang berbeda. *Botnet* merupakan suatu teknik hasil dari

perkembangan teknologi informasi. Hal inilah yang membuat *botnet* perlu diwaspadai. Teknik botnet sejalan dengan Pasal 1 angka (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu:

> "Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi".

Setiap teknik yang dilakukan melalui komputer atau pun jaringan komunikasi (internet) akan tersimpan dalam sebuah catatan atau dokumen (*log.*) dilalam sistem komputer itu sendiri. Berdasarkan pasal 1 angka (4) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu:

> "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, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya".

Berdasarkan pasal di atas, dapat diketahui bahwa suatu teknik dalam *botnet* dapat dikatakan merupakan kumpulan dokumen elektronik. Ini dikarenakan *botnet* merupakan teknik dalam menggabungkan *file-file* dalam dokumen-dokumen elektronik dalam komputer (yang terkoneksi kedalam jaringan internet) dalam teknologi informasi sebagai akibat negatif dari munculnya *cyberspace*.

Pemanfaatan suatu teknologi informasi merupakan hal penting dalam *cyberspace*. Ini dikarenakan suatu perbuatan dengan dasar kesadaran (kesengajaan) dikatakan legal jika sesuai dengan pemanfaatanya yang dinilai positif, sebaliknya jika dimanfaatkan secara negatif maka akan memunculkan suatu perbuatan yang illegal. Hal ini sejalan dengan Pasal 3 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Eletronik, yaitu:

> "Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi".

Tindak pidana *cracking* menggunakan *botnet* merupakan gabungan dari:

1. Membuat virus, virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus komputer dapat merusak (misalnya dengan merusak data pada dokumen).
2. Melakukan serangan DoS (*Deniel of Service*) ke sebuah web, DoS (Denial of Service) Attack merupakan penyerangan sekaligus perusakan terhadap system DoS.
3. *The Trojan Horse, Trojan horse* atau lebih dikenal sebagai *Trojan* dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (*malicious software*/*malware*) yang dapat merusak sebuah sistem atau jaringan. Tujuan dari *Trojan*

adalah memperoleh informasi dari target (password, kebiasaan *user* yang tercatat dalam *system log*, data, dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target).

4. Berbagai teknik yang digabungkan sehingga dapat menciptakan suatu zombie (*botnet*) misal teknik XSS (*Cross site scripting*). XSS (*Cross site scripting*) adalah suatu teknik untuk mendapatkan *cookie* seorang *user* tertentu dengan menyamarkan diri sebagai *hyperlink* atau menambahkan *script* yang dapat meragukan pengunjung *website*. XSS dapat mencuri banyak data pelanggan. XSS dapat digunakan untuk mengetahui atau mencuri *cookie* dari pengunjung *website* tersebut dengan cara memasukan *script* <script>alert(document.cookie)</script>.

Pada kasus botnet tersangka dengan sengaja menanamkan *payload* yang ditanam dan diinstruksikan untuk penyebaran virus/*worm*, *spam*, *phising*, *spyware* juga teknik XSS untuk pencurian data, dan bahkan secara serentak menyerang dan merusak DoS (*Denial of Service*) melalui *search bot* dan mengumpulkan data, membuat data *base*-nya dan melakukan *hacking online.* Perbuatan tersangka tersebut dapat dijerat dengan menggunakan Pasal 32 ayat (1) juncto Pasal 33 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 32 ayat (1), yaitu:

> “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan

suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik".

Penggunaan pasal tersebut karena dianggap telah memenuhi unsur-unsur yang terdapat pada pasal tersebut, yaitu:

1. Dengan sengaja dan tanpa hak atau melawan hukum;

   Dengan sengaja dan tanpa hak adalah tindakan yang dilakukan oleh pelaku kejahatan telah direncanakan atau diniatkan terlebih dahulu dan tanpa sepengetahuan dari orang yang berhak serta telah melanggar ketentuan perundang-undangan.

2. Setiap Orang;

   Orang adalah orang perseorangan, baik warga Negara Indonesia, warga negara asing, maupun badan hukum.

3. Dengan cara apa pun;

   Dengan menghalalkan segala cara, merusak termasuk cara melalui pemanfaatan teknologi.

4. Informasi Elektronik dan/atau Dokumen Elektronik;

   Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (*EDI*), surat elektronik (*electronic mail)*, telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Sedangkan 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, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

5. Milik orang lain atau milik publik;

   Kepemilikannya merupakan bukan milik pelaku.

Berdasarkan Pasal 33 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

> “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya”.

Penggunaan pasal tersebut karena dianggap telah memenuhi unsur-unsur yang terdapat pada pasal tersebut, yaitu:

1. Dengan sengaja dan tanpa hak atau melawan hukum;

   Dengan sengaja dan tanpa hak adalah tindakan yang dilakukan oleh pelaku kejahatan telah direncanakan atau diniatkan terlebih dahulu

dan tanpa sepengetahuan dari orang yang berhak serta telah melanggar ketentuan perundang-undangan.

2. Setiap orang;

   Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.

3. Melakukan tindakan apa pun;

   Dengan menghalalkan segala cara termasuk cara melalui pemanfaatan teknologi.

4. Berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya;

   Yang dapat menyebabkan suatu akibat negatif terhadap sistem elektronik (kerusakan/tidak berjalan sebagaimana mestinya). Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

Perbuatan tersangka yang melakukan tindak pidana *cracking* melalui *botnet* telah memenuhi unsur subjektif dan unsur objektif Pasal 32 ayat (1) dan Pasal 32, maka berdasarkan Pasal 48 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak

Rp2.000.000.000,00 (dua miliar rupiah). Berdasarkan Pasal 49 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

## B. Upaya Pembuktian Atas Tindak Pidana *Cracking* Menggunakan *Botnet* Terhadap Sistem Komputer Dihubungkan Dengan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Pembuktian dalam hukum pidana merupakan sub sistem kebijakan kriminal sebagai *science of response* yang mencakup berbagai disiplin ilmu. Hal ini disebabkan oleh luasnya kausa dan motif berkembangnya jenis kejahatan berbasis teknologi informasi dewasa ini. Penggunaan transaksi elektronik tidak menggunakan kertas (*paperless transaction*) dalam sistem pembayaran menimbulkan permasalahan khususnya terkait dengan ketentuan pembuktian sebagaimana diatur dalam pasal dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Pembuktian adalam suatu upaya yang dilakukan dalam persidangan untuk meyakinkan hakim atas benar tidaknya tindak pidana yang dilakukan oleh terdakwa.

Hambatan yang klasik adalah sulitnya menghukum pelaku mengingat belum lengkapnya ketentuan pidana yang mengatur tentang kejahatan komputer, internet dan teknologi informasi (*cybercrime*) dan belum diterimanya dokumen elektonik (misalnya *file* komputer) sebagai alat bukti oleh konsep

KUHAP. Berhadapan dengan kasus *cybercrime*, pembuktian menjadi masalah yang pelik. Seringkali penegak hukum di Indonesia mengalami kesulitan saat menjerat pelaku *cybercrime* karena masalah pembuktian (*documentary evidence*) yang tidak memenuhi ketentuan sistem hukum pidana Indonesia. Sementara upaya penjeratan terhadap pelaku-pelaku *cybercrime* harus tetap dilakukan, upaya perluasan menjadi solusi untuk menegakan hukum.

Hukum pembuktian merupakan sebagian dari hukum pidana yang mengatur tentang alat-alat bukti yang sah menurut hukum, barang-barang bukti, sistem pembuktian yang dianut, syarat dan tata cara pembuktian yang dilakukan, serta kewenangan hakim untuk menerima, menolak dan menilai suatu pembuktian. Sumber hukum pembuktian adalah undang-undang, doktrin dan yurisprudensi. Oleh karena itu, Undang-Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana (selanjutnya disebut KUHAP) menjadi salah satu sumber hukum dalam proses pembuktian. Pembuktian merupakan titik sentral pemeriksaan perkara dalam sidang pengadilan. Pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang untuk membuktikan kesalahan yang didakwakan kepada terdakwa. Pembuktian juga merupakan ketentuan yang mengatur alat-alat bukti yang dibenarkan undang-undang yang dapat dipergunakan hakim dalam membuktikan kesalahan terdakwa. Oleh karena itu, hakim tidak dapat mempergunakan alat bukti yang bertentangan dengan undang-undang. Kebenaran atas suatu putusan harus teruji dengan alat bukti yang sah secara

hukum serta memiliki kekuatan pembuktian yang melekat pada setiap alat bukti yang ditemukan.

Secara umum terdapat beberapa teori mengenai sistem pembuktian yakni:

1. *Conviction In Time Theory*, yaitu sistem pembuktian yang menyatakan bahwa salah tidaknya seorang terdakwa semata-mata ditentukan oleh penilaian keyakinan hakim. Keyakinan hakim ini dapat diperoleh melalui alat-alat bukti yang diajukan dalam persidangan.
2. *Conviction Rsisonee Theory*, merupakan sistem pembuktian berdasarkan keyakinan hakim untuk menentukan salah tidaknya terdakwa, namun dalam sistem ini keyakinan hakim dibatasi dan harus didasari dengan alasan-alasan yang jelas dan dapat diterima yang wajib diuraikan dalam putusannya.
3. Teori Pembuktian Menurut Undang-Undang Secara Positif, merupakan pembuktian yang berlatar belakang sistem pembuktian berdasarkan keyakinan atau *conviction in time theory*. Pembuktian pada sistem ini didasari dengan alat-alat bukti yang sah yang telah ditetapkan oleh undang-undang disertai keyakinan hakim dalam menentukan salah tidaknya terdakwa.
4. Teori Pembuktian Menurut Undang-Undang Secara Negatif (*Negatief Wettelijke Stelsel*), merupakan sistem pembuktian yang menggunakan teori perpaduan antara sistem pembuktian menurut undang-undang secara positif dengan sistem pembuktian menurut

keyakinan atau *conviction in time theory*. Rumusan teori ini adalah bahwa salah tidaknya seorang terdakwa ditentukan oleh keyakinan hakim yang didasarkan pada cara dan dengan alat-alat bukti yang sah menurut undang-undang.

Sistem pembuktian yang dianut oleh KUHAP adalah sistem pembuktian menurut undang undang secara negatif, karena merupakan perpaduan antara sistem pembuktian menurut undang-undang secara positif dengan sistem pembuktian menurut keyakinan atau *conviction in time theory*. Hal ini terlihat ketentuan Pasal 183 KUHAP yang menegaskan bahwa hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah diperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya.

Proses pebuktian tidak terlepas dari pembahasan mengenai alat bukti yaitu segala sesuatu yang berhubungan dengan perbuatan, yang mana alat bukti tersebut digunakan hakim memutuskan suatu perkara. Dengan demikian, alat bukti yang digunakan hakim untuk menjatuhkan putusan, harus sesuai dengan ketentuan undang-undang yang secara limitatif telah diatur dalam Pasal 184 KUHAP.

Dalam KUHAP, dikenal 5 (lima) alat bukti yang sah sebagaimana diatur dalam Pasal 184 ayat 1 KUHAP. Berdasakan Pasal 183 KUHAP, bahwa sekurang-kurangnya terdapat dua alat bukti yang sah. Alat bukti ini harus

mampu membuktikan telah terjadi suatu perbuatan dan membuktikan adanya akibat dari perbuatan tersebut. Alat-alat bukti dalam Pasal 184 ayat 1 KUHAP dimaksud adalah:

1. Keterangan saksi

   Dalam Pasal 185 KUHAP ayat 1 disebutkan bahwa keterangan saksi sebagaimana alat bukti ialah apa yang saksi nyatakan di sidang pengadilan. Dalam penjelasan KUHAP dinyatakan bahwa dalam keterangan saksi tidak termasuk keterangan yang diperoleh dari orang lain atau *testimonium de auditu*. Pasal 1 angka 27 KUHAP menyatakan bahwa keterangan saksi adalah salah satu alat bukti dalam perkara pidana yang berupa keterangan dari saksi mengenai suatu peristiwa pidana yang ia dengar sendiri, ia lihat sendiri dan ia alami sendiri dengan menyebut alasan dari pengetahuanya itu.

   Yang dapat dijadikan keterangan saksi dalam kasus cybercrime ialah melalui hasil interaksi di dalam dunia cyber seperti chatting dan e-mail antara pengguna internet, atau juga dapat melalui keterangan seorang administrator sistem komputer yang telah disertifikasi.

2. Keterangan ahli

   Pasal 186 KUHAP menyatakan bahwa keterangan seorang ahli ialah apa yang seorang ahli nyatakan di persidangan. Selanjutnya penjelasan Pasal 186 KUHAP menyatakan bahwa keterangan ahli ini dapat juga sudah diberikan pada waktu pemeriksaan oleh penyidik atau penuntut umum yang dituangkan dalam bentuk laporan dan

dibuat dengan mengingat sumpah pada waktu ia menerima jabatan atau pekerjaan. Menurut teori hukum pidana yang dimaksud dengan keterangan ahli adalah keterangan yang diberikan seseorang berdasarkan ilmu dan pengetahuan yang dikuasainya. Dalam kasus ini adalah keterangan dari seorang ahli teknologi informasi dan yang segala hal berhubungan dengan teknologi informasi.

3. Surat

   Dalam *cybercrime* contohnya adalah surat yang bersifat *online* atau hasil *print out* dan *recipt* hasil transaksi elektronik.

4. Petunjuk

   Pasal 188 ayat 1 KUHAP memberi definisi petunjuk sebagai, kejadian atau keadaan, yang karena penyesuaiannya, baik antara yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya.

5. Keterangan terdakwa

   Dalam pasal 189 ayat 1 KUHAP ditentukan bahwa keterangan terdakwa adalah apa yang terdakwa lakukan, ketahui dan alami sendiri. Dalam kasus *cybercrime*, keterangan terdakwa yang dibutuhkan terutama mengenai cara-cara pelaku melakukan perbuatannya, akibat yang ditimbulkan, informasi jaringan serta motivasinya.

Ketentuan mengenai alat bukti di atas merupakan ketentuan hukum acara pidana yang bersifat memaksa (*dwingen recht*), artinya semua jenis alat bukti yang telah diatur dalam pasal tersebut tidak dapat ditambah atau dikurangi.

Dalam *cybercrime*, pengumpulan alat bukti secara fisik akan sulit dipenuhi. Yang paling mudah dalam melakukan pengumpulan bukti-bukti adalah mencari petunjuk-petunjuk yang mengindikasikan telah adanya suatu niat jahat berupa akses secara tidak sah atau juga penyembunyian data.

Proses pembuktian dalam kasus-kasus *cybercrime* khususnya kasus tindak pidana *cracking* menggunakan *botnet* didasari ketentuan Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi:

> "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah".

Sementara itu, Pasal 5 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juga menegaskan:

> "Informasi Elektronik dan/atau Dokumen 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".

Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan perluasan dari alat bukti petunjuk.

Apa yang dimaksud dengan bukti petunjuk menurut Pasal 188 ayat (1) KUHAP Petunjuk adalah perbuatan, kejadian atau keadaan, yang karena persesuaiannya, baik antara yang yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya.

Selanjutnya dalam Pasal 188 ayat (2) mengariskan bahwa petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (1) hanya dapat diperoleh dari tiga komponen yaitu:

1. Keterangan saksi;
2. Surat;
3. Keterangan terdakwa.

Pasal 188 ayat (3), penilaian atas kekuatan pembuktian dari suatu petunjuk dalam setiap keadaan tertentu dilakukan oleh hakim dengan bijaksana setelah ia mengadakan pemeriksaan dengan penuh kecermatan dan kesaksian berdasarkan hati nuraninya.

Sesuai dengan ketentuan tersebut disimpulkan bahwa bukti petunjuk akan ditemukan dari kandungan alat bukti lain, dari tiga komponen alat bukti masing-masing keterangan saksi, surat dan keterangan terdakwa. Oleh karena itu bukti petunjuk memiliki sifat interdependensi dengan substansi alat bukti lainya karena hal-hal sebagai berikut:

1. Selamanya tergantung dan bersumber pada substansi dari alat lain.

2. Bukti petunjuk baru akan diperlukan dalam pembuktian, apabila alat bukti lain belum dianggap cukup oleh hakim, untuk membuktikan kesalahan terdakwa.
3. Bukti petunjuk baru dianggap sangat diperlukan apabila upaya pembuktian dengan alat bukti lain belum mencapai batas minimum pembuktian.
4. Hakim harus terlebih dulu berupaya mencukupi pembuktian dengan alat bukti yang lain, sebelum mempergunakan alat bukti petunjuk.
5. Dengan kata lain maka upaya menggali dan mencari alat bukti petunjuk baru dilakukan pada tingkatan keadaan tertentu yakni, pencarian alat bukti lain sudah tidak mungkin ditemukan lagi dan dalam keadaan demikian itulah maka hakim mengupayakan penemuan/penggalian alat bukti petunjuk

Bukti petunjuk memiliki nilai pembuktian bebas lagi pula tidak dapat berdiri sendiri untukmembuktikan kesalahan terdakwa. Ia tetap terikat pada prinsip batas minimum pembuktian, oleh karena demikian maka agar petunjuk memiliki nilai kekuatan pembuktian yang cukup harus didukung oleh sekurang-kurangnya satu alat bukti lain.

Berdasarkan hal diatas, alat bukti petunjuk hanya dapat diambil dari ketiga alat bukti diatas. Pada umumnya, alat bukti petunjuk baru diperlukan apabila alat bukti lainya belum mencukupi batas minimum pembuktian yang diatur dalam Pasal 183 KUHAP di atas. Dengan demikian, alat bukti petunjuk

merupakan alat bukti yang bergantung pada alat bukti lainya yakni saksi, surat, dan keterangan terdakwa. Alat bukti petunjuk memiliki kekuatan pembuktian yang sama dengan alat bukti lain, namun hakim tidak terikat atas kebenaran persesuaian yang diwujudkan oleh petunjuk, sehingga hakim bebas untuk menilai dan mempergunakannya dalam upaya pembuktian. Selain itu, petunjuk sebagai alat bukti tidak dapat berdiri sendiri membuktikan kesalahan terdakwa, karena hakim tetap terikat pada batas minimum pembuktian sesuai ketentuan Pasal 183 KUHAP.

Pada kasus tindak pidana *cracking* melaui *botnet*, tersangka menanamkan *payload* yang ditanam dan diinstruksikan untuk penyebaran virus/*worm*, *spam*, *phising*, *spyware* untuk pencurian data, dan bahkan secara serentak menyerang kesuatu target D-DOS (*Distributed Denial of Service*) melalui *search bot* dan mengumpulkan data, membuat data basenya dan melakukan *hacking online*, meninggalkan informasi elekronik berupa dokumen elektronik yang tersimpan dalam memori (*log.*) atau hasil cetak yang dapat dijadikan alat bukti yang sah sesuai dengan pasal 5 ayat 1 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang kemudian dapat diambil bukti petunjuk berdasarkan keterangan terdakwa.