URGENSI PENGATURAN TATA CARA PEMBUKTIAN TINDAK PIDANA SIBER (*CYBERCRIME)*

Novita Maharani, Dr. Yuliati. SH.,LLM, Alfons Zakaria, SH.,LLM

Fakultas Hukum Universitas Brawijaya

Email : novitamaharani.nm@gmail.com

ABSTRAKSI

Kejahatan berkembang seiring berkembangnya teknologi yang semakin maju. Karena banyaknya kejahatan yang menggunakan teknologi komputer. Maka dibutuhkan peraturan yang jelas. Meskipun dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sudah mengatur mengenai tindak pidana siber (*cybercrime)* dan di dalam Kitab Undang-Undang Hukum Acara Pidana sudah mengatur mengenai pembuktian tindak pidana akan tetapi peraturan tersebut masih lemah dan tidak efektif, kekosongan peraturan mengenai tata cara pembuktian tindak pidana siber yang menggunakan bukti elektronik menyulitkan aparat penegak hukum dalam melakukan pembuktian karena Undang-Undang saat ini tidak cukup sebagai acuan. Dan karena komputer adalah masalah yang sangat kompleks dan dibutuhkan keahlian khusus dalam menganalisa kasus tersebut untuk itu Penulis mengusulkan pengaturan terkait tata cara pembuktian tindak pidana siber.

Kata Kunci :pembuktian, *cybercrime*

Abstract

Crime develops as technology advances. Because of the many crimes that use computer technology. It needs clear rules. Although in Law (Undang-undang) No. 11 of 2008 on Information and Electronic Transactions has regulated the crime of

cybercrime and *in the Criminal Procedure Code already regulate the proving of criminal act but the regulation is still weak and ineffective, the void of the regulation on the procedure for the proof of criminal acts of cyber that uses electronic evidence makes it difficult for law enforcement officials to prove because the current law is not enough as a reference. And because the computer is a very complex problem and it takes a special skill in analyzing the case. Therefore the author proposes arrangements related to the procedure for the proof of cyber crime.*

PENDAHULUAN

A. Latar Belakang

Manusia adalah makhluk sosial, sebagai makhluk sosial manusia hidup dalam suatu kelompok masyarakat yang saling berinteraksi untuk memenuhi kebutuhan satu sama lain terlebih lagi.[1] Jadi manusia disamping mempunyai kebutuhan mendasar berupa kebutuhan primer maupun sekunder, juga memiliki kebutuhan yang berupa hubungan sosial dengan manusia lain, seiring perkembangan jaman interaksi manusia juga berkembang yang awalnya hanya meliputi wilayah kecil dan interaksi bisa di lakukan dengan sederhana hingga interaksi manusia tak terbatas oleh jarak dan waktu, untuk memangkas perbedaan jarak, waktu dan wilayah manusia menciptakan sebuah dimensi baru bernama teknologi informasi dan komunikasi.

Hubungan manusia untuk bersosialisasi dimudahkan dengan perkembangan teknologi dan informasi yang secara tidak langsung merubah pola pikir manusia dari sederhana menjadi tak terbatas. Teknologi informasi dan komunikasi yang beraneka ragam jenisnya seperti radio, telephone dan televisi munculah teknologi informasi baru yaitu internet. Pengguna internet dipermudah untuk mencari informasi yang di butuhkan, saling berinteraksi sesama pengguna maupun bertukar pendapat, berbagi komentar, mengirim file, dan lain sebagainya.

[1]Sudikno Mertokusumo, **Mengenal Hukum Suatu Pengantar**, Liberty, Yogyakarta, 2003, Hlm 1

Hadirnya internet saat ini telah membuka ruang dan dunia baru dalam kehidupan manusia. Internet adalah alat elektronik yang dapat menembus batas antarnegara dan mempercepat penyebaran segala bidang informasi. Akan tetapi *cyberspace* selain banyak memberikan kemudahan bagi masyarakat juga memiliki dampak negative. Kejahatan-kejahatan yang dulunya sederhana saat ini mulai menjadi lebih rumit karena bisa dilakukan di dunia maya, kejahatan di internet dinamakan *cybercrime* macam-macamnya seperti perjudian *online*, prostitusi *online*, penyadapan data, *spamming* (mengirim pesan atau iklan yang tidak di kehendaki), *carding, hacking, cyberstalking* atau *cyber harassment* dan lain sebagainya.

Cybercrime di Indonesia terjadi sejak tahun 1983, terutama di bidang perbankan. Dalam tahun-tahun berikutnya sampai saat ini, di Indonesia banyak terjadi tindak pidana siber (*cybercrime),* misalnya pembajakan program computer, *cracking,* penggunaan kartu kredit pihak lain secara tidak sah (*carding*), pembobolan bank (*bank fraud*), pornografi, termasuk kejahatan terhadap nama domain (*domain name).* Selain itu, kasus kejahatan lain yang menggunakan komputer di Indonesia antara lain penyelundupan gambar-gambar porno melalui internet *(cyber smuggling), pagejacking (mousetrapping), spam (junk mail), intercepting, cybersquatting, typosquatting.* Sedangkan kasus kejahatan terhadap sistem atau jaringan komputer antara lain*cracking, defacting, Denial ofservice Attack (DoS) Distributed Denial of Service Attack (DDoS)* penyebaran virus *(worm),* dan pemasangan *logic bomb*.[2]

Pembuktian merupakan inti persidangan perkara pidana karena dicari dalam hukum pidana adalah kebenaran materiil. Pembuktian dalam perkara pidana sudah dimulai sejak tahap penyelidikan untuk mencari dan menemukan peristiwa yang diduga sebagai tindak pidana guna dapat atau tidaknya dilakukan penyidikan. Pembuktian dilihat dari prespektif hukum acara pidana, yakni ketentuan yang membatasi sidang pengadilan dalam usaha mencari dan mempertahankan kebenaran, baik oleh hakim, penuntut umum, terdakwa maupun penasehat hukum, semua terikat pada ketentuan dan tata cara, serta penilaian alat bukti yang ditentukan oleh undang-undang.[3]

---

[2]Widodo, **Sistem Pemidanaan Dalam Cyber Crime**, Laksbang Mediatama, Malang, 2009, hlm 29

[3] Edie O.S. Hiariej, **Teori dan Hukum Pembuktian**, Erlangga, Yogyakarta, 2012, hlm. 07

Bukti elektronik menurut Undang–Undang Informasi dan Transaksi Elektronik adalah informasi elektronik dan dokumen elektronik. Informasi elektronik dan dokumen elektronik diatur dalam bab III pasal 5 dan pasal 6 Undang–Undang Informasi dan Transaksi Elektronik, akan tetapi tidak ada peratutan yang menyebutkan tentang tata cara apa yang bisa digunakan dalam melakukan tindak pidana siber (*cybercrime)* yang membuat aparat penegak hukum kesulitan dalam menangani kasus *cybercrime.*

Peraturan mengenai tindak pidana siber (*cybercrime)* dan cara penanganan pembuktianpun menjadikan lemahnya lembaga hukum dan pengadilan dalam memecahkan kasus *cybercrime.* Selama ini yang menjadi acuan dalam pembukain tindak pidana siber (*cybercrime)* adalah pasal 5 dan pasal 6 Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik saja karena tidak adanya pasal yang menyatakan bagaimana cara melakukan pembuktian secara merinci sehingga terdapat kekosongan hukum.

Sulitnya pembuktian tindak pidana siber (*cybercrime)* disebabkan karena bukti elektronik yang mudah dihapus, mudah diganti dan diakses banyak orang. Indonesia menempati posisi tertinggi sebagai negara yang pengguna internetnya menjadi korban kejahatan siber di antara 26 negara lain, posisi kedua ditempati oleh Vietnam dan India dengan masing-masing 25% dan 24% pengguna internet jadi target kejahatan. Survei ini juga menemukan, 48% konsumen menjadi target aksi penipuan yang dirancang untuk menipu dan mendapatkan informasi sensitif dan data keuangan untuk tindak criminal.[4] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik secara umum mengacu pada KUHP sedangkan dalam KUHP tidak diatur mengenai pembuktian tindak pidana siber (*cybercrime)*sehingga menimbulkan kekosongan peratutan.

B. MASALAH/ISU HUKUM

Dari latar belakang yang telah diuraikan, maka dapat diperoleh rumusan masalah yait apa urgensi pengaturan tata cara pembuktian tindak pidana siber *(cybercrime)*?; dan

[4] Liputan6.com, **Orang Indonesia Rentan Menjadi Korban Kejahatan Online**, http://tekno.liputan6.com/read/2519790/orang-indonesia-paling-banyak-jadi-korban-penipuan-online, diakses tanggal 11/15/1016

bagaimanakah alternatif pengaturan yang tepat terhadap tata cara pembuktian tindak pidana siber (*cybercrime)*?

C. METODE PENELITIAN

1. Jenis Penelitian

   Untuk menjawab isu hukum yang dihadapi penulis menggunakan jenis penelitian yuridis normatif, yaitu merupakan suatu penelitian hukum yang bertujuan untuk menemukan asas hukum atau doktrin hukum positif yang berlaku.

2. Jenis pendekatan

   Penulisan ini menggunakan pendekatan perbandingan dan pendekatan perundang-undangan, yaitu dilakukan dengan membandingkan peraturan suatu negara dengan peraturan negara lain mengenai suatu hal yang sama. Pendekatan perundang-undangan dilakukan dengan menelaah semua undang-undang yang bersangkutan dengan masalah yang sedang di teliti.

D. PEMBAHASAN

a. Urgensi Pengaturan Tata Cara Pembuktian Tindak Pidana Siber (*Cibercrime)*

1. Alat Bukti Elektronik Mempunyai Sifat Mudah Rusak

Alat bukti elektronik sangat penting untuk kepentingan pembuktian di pengadilan, bukti elektronik yang didapat berasal dari data elektronik, dan disebut bukti elektronik apabila bukti tersebut tersimpan secara elektronik dalam suatu mesin penyimpanan data. Data elektronik komputer adalah data yang dapat dibaca menggunakan bantuan mesin elektronik yang dapat berupa *data base, source code, object code,* data yang tersimpan dalam file komputer, data yang tersimpan dalam metode penyimpanan elektronik seperti *flashdisk,* CD atau alat lain. Bukti elektronik tidak terbatas pada tulisan, gambar, atau foto tetapi juga berupa kode, symbol dan grafik yang diolah melalui computer, oleh sebab itu bukti elektronik bisa dikatakan khusus dan bersifat mudah rusak karena sifatnya yang tidak tetap yang tak terbatas. Karakteristik tersebut adalah yang pertama data elektronik mudah untuk menyimpannya serta mudah untuk dibawa dan dihilangkan. Serta data

elektronik mudah untuk diubah dan dirusak dan dengan bahkan perusakan tersebut dapat ditutupi.[5]

2. Sebagai Acuan Penyidik Dalam Memperlakukan Barang Bukti Elektronik

Dalam memperlakukan barang bukti elektronik penyidik tidak boleh sembarangan dalam melakukan penyidikan, oleh sebab itu harus ada acuannya karena data elektronik mempunyai resiko mudah hancur. Dalam proses pembuktian di persidangan, yang diperlukan hanya hasil cetakannya (*print out*) alat bukti surat elektronik dan tidak diperlukan bentuk aslinya (*soft copy*). Hal ini mengacu kepada Pasal 5 ayat (1) Undang-Undang No.11 Tahun 2008. Mengenai aspek keaslian dari hasil cetakan (*printout*) surat elektronik, hakim akan menanyakan kepada terdakwa atau korban mengenai surat elektronik tersebut apakah terdapat perbedaan dari bentuk aslinya, jika terdakwa atau korban mengakui bahwa surat elektronik tersebut sama dengan aslinya atau tidak terdapat perbedaan maka surat elektronik tersebut telah memenuhi aspek keaslian sebagai alat bukti dan menjadi alat bukti yang sah.

3. Agar Kredibilitas Barang Bukti Elektronik Dapat Dipertanggungjawabkan di Persidangan.

` Untuk mencari dan menangani bukti elektronik dengan baik dan benar digunakan metode penanganan khusus yaitu dengan melakukan digital forensik, Secara garis besar, digital forensik adalah salah satu cabang ilmu Informatika untuk menganalisa barang bukti elektronik yang disebut juga digital forensik yang memiliki pemahaman yang sama dengan forensik pada umumnya. Terdapat dua jenis data dasar yang dapat dikumpulkan dalam komputer forensik. Data yang *persisten* adalah data yang tersimpan pada *hard drive* lokal (atau media lain) dan dipelihara saat komputer dimatikan. Data *volatil* adalah data yang tersimpan dalam memori, atau ada dalam *transit*, yang akan hilang saat komputer kehilangan daya atau dimatikan. Data volatil berada *pada register, cache,* dan *random access memory* (RAM). Karena data *volatil* bersifat sementara, sangat penting penyidik mengetahui cara yang andal untuk menangkapnya.

[5]*what is cyber crime investigation*,www.cyber/ASCL%20Certified%20Cyber%20Crime%Investigation

Administrator sistem dan petugas keamanan juga harus memiliki pemahaman dasar tentang bagaimana tugas rutin komputer dan jaringan dapat mempengaruhi proses forensik (kemungkinan diterimanya bukti di pengadilan) dan kemampuan untuk memulihkan data yang mungkin penting untuk identifikasi dan analisis. Pada dasarnya tujuan digital forensik untuk mengidentifikasi bukti elektronik dengan menggunakan metode ilmiah untuk membuat kesimpulan. Dan kesimpulan tersebut untuk membuat terang suatu perkara. Tahap tahap melakukan digital forensik yang paling mendasar ada tiga tahap yaitu:

1. Akuisisi

   Tahap Akuisisi menyimpan keadaan sistem digital sehingga dapat dianalisis kemudian. Ini serupa dengan pengambilan foto, sidik jari, contoh darah, atau pola ban dari TKP. Seperti di dunia fisik, tidak diketahui data mana yang akan dijadikan bukti digital sehingga tujuan dari tahap ini adalah untuk menyelamatkan semua nilai digital.
2. Analisa

   Fase Analisis mengambil data yang diperoleh dan memeriksanya untuk mengidentifikasi beberapa bukti. Alat bukti dianalisa menggunakan metode ilmiah untuk menarik kesimpulan berdasarkan bukti yang di temukan.
3. Presentasi

Presentasi adalah tahap dimana hasil analisa di disajikan untuk ditarik kesimpulan sesuai dengan undang-undang.

4. Menghindari Kekosongan Yuridis mengenai Pengaturan Tata Cara Pembuktian Tindak Pidana Siber *(Cybercrime)*

   Dalam hal pembuktain tindak pidana siber (*cybercrime)* dibutuhkan penelitian lebih lanjut mengenai pengaturan pembuktian tindak pidana siber (*cybercrime)* secara konvensional di Indonesia. *Cybercrime* merupakan perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. *Cybercrime* di sisi lain, bukan hanya menggunakan kecanggihan teknologi komputer, akan tetapi juga melibatkan teknologi

telekomunikasi di dalam pengoperasiannya. Pembuktian bertujuan untuk mengetahui tentang cara meletakkan hasil pembuktian terhadap perkara yang sedang diperiksa. Pembuktian yang dianut oleh Indonesia adalah pembuktian menurut undang-undang secara negatif (*negatief wettelijk*), Sistem pembuktian ini merupakan gabungan dari sistem pembutian menurut undang-undang secara positif dan sistem pembuktian berdasarkan keyakinan hakim melulu (*conviction intime).*

Tindak pidana *cyber* diatur dalam UU ITE yang terdiri dari 13 bab dan 54 pasal yang mengatur secara terperinci tentang bagaimana aturan di dunia maya dan transaksi yang terjadi di dalamnya. Merujuk Pasal 42 UU ITE yang berkaitan dengan tahap penyidikan yang juga dikenal dalam KUHAP, dimana semua aturan yang ada dalam KUHAP berlaku sebagai ketentuan umum (*lex generalis*) kecuali yang disimpangi oleh UU ITE yang posisinya sebagai ketentuan yang khusus (lex *specialis*). Yakni dengan kata lain, ketentuan yang tidak diatur dalam UU ITE maka yang menjadi acuannya adalah KUHAP. Seperti yang telah tercantum pada Pasal 284 ayat (2) KUHAP yang menyatakan bahwa terhadap semua perkara diberlakukan ketentuan KUHAP, dengan pengecualian untuk sementara mengenai ketentuan khusus acara pidana (hukum pidana formil) diberlakukan undang-undang tertentu sebelum ditinjau kembali, diubah atau dinyatakan tidak berlaku lagi terhadapnya. Di dalam KUHAP banyak peraturan yang sudah tidak sesuai dengan masa sekarang.

Sejauh ini aparat penegak hukum dalam membuktikan tindak pidana siber (*cybercrime*) hanya mengacu pada Kitab Undang-Undang Hukum Acara Pidana yakni pada pasal 138 sampai 184 KUHAP. Sedangkan saat ini Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik belum mengatur secara jelas bagaimana tata cara pembuktian tindak pidana siber. Sehingga penulis berpendapat aparat penegak hukum memerlukan pengaturan tentang tata cara melakukan pembuktian yang benar tentang tindak pidana siber (*cybercrime*) untuk mempermudah dalam rangka melakukan pembuktian.

b. Pengaturan Pembuktian Tindak Pidana Siber *(Cybercrime)* di Amerika

a. Proses Analisa Bukti Elektronik

Amerika memiliki banyak sistem hukum yang saling berkaitan. Proses pembuktian pada sistem *common law* tidak terbatas hanya kepada apa yang disebut didalam undang-undang. Akan tetapi, menggunakan hukum yang berlaku umum, kebiasaan-kebiasaan yang hidup di tengah-tengah masyarakat, dan adanya asas *the binding of presedent*.

Untuk dapat diterima di pengadilan Amerika Serikat, bukti harus relevan dan dapat diandalkan. Keandalan bukti ilmiah, seperti hasil dari alat forensik digital, ditentukan oleh hakim (berlawanan dengan juri) dalam sebuah peradilan "Daubert Hearing".Tanggung jawab hakim dalam Daubert Hearing adalah untuk menentukan apakah metodologi dan teknik yang mendasari yang digunakan untuk mengidentifikasi bukti itu masuk akal, dan apakah hasilnya bisa diandalkan, buktinya dapat diandalkan. Proses Daubert mengidentifikasi empat kategori umum

Yang digunakan sebagai pedoman saat menilai sebuah prosedur:

1. Pengujian: Bisa dan prosedurnya sudah teruji?
2. Error Rate: Apakah ada tingkat kesalahan prosedur yang diketahui?
3. Publikasi: Apakah prosedur telah dipublikasikan dan tunduk pada peer review?
4. Penerimaan: Apakah prosedurnya berlaku umum di bidang ilmiah yang relevan?

Tes Daubert adalah perluasan pendekatan Pengadilan sebelum diterimanya bukti ilmiah.Sebelumnya, di bawah "Frye Test", pengadilan menempatkan tanggung jawab untuk mengidentifikasi prosedur yang dapat diterima pada komunitas ilmiah menggunakan jurnal peer-review.Namun, karena tidak semua bidang memiliki jurnal peer-review, Uji Daubert menawarkan metode pengujian kualitas bukti tambahan.Setiap pedoman sekarang akan dibahas secara lebih rinci berkenaan dengan forensik digital. Pedoman tersebut akan

diperiksa untuk alat akuisisi data dan alat analisis. Saat ini, mayoritas forensik digital melibatkan perolehan hard disk dan analisis sistem file.

b. Prosedur yang Digunakan dalam Suatu Peradilan Pidana di Amerika Serikat

Di Amerika Serikat prosedur yang digunakan dalam suatu peradilan pidana untuk menganalisis bukti elektronik menggunakan sebuah metodologi dan tekniknik yang bernama tes daubert yang artinya adalah pendekatan pengadilan sebelum diterima bukti ilmiah, yaitu suatu metode kajian ilmiah untuk menentukan kualitas bukti dengan mengguankan forensik digital. Adapun prosedurnya sebagai berikut :[6]

1. *Testing*

   Adalah sebuah pedoman untuk menguji dan mengidentifikasi suatu prosedur untuk memperoleh hasil yang akurat.

2. *Error Rates*

   Error rate diartikan sebagai tingkat kesalahan yaitu pedoman untuk mengidentifikasi tingkat kesalahan yang diketahui dari prosedur

3. Publikasi

   Publikasi adalah prosedur yang dilakukan untuk menampilkan hasil dari proses forensic digital agar penyidik dapat mengidentifikasi bagaimana prosedur di lakukan.

4. *Acceptance*

   Pedoman penerimaan adalah kerangka kerja bagi komunitas ilmuwan terkait untuk mengevaluasi prosedur yang diterbitkan.

c. Undang-Undang Amerika yang Mengatur Transaksi Elektronik

Undang-undang Amerika yang mengatur mengenai *cybercrime* adalah Cybercrime Laws of the United States yang secara umum mengatur mengenai larangan pencurian identitas secara online, pengacauan sistem komputer, pencabulan visual, pornografi anak, judi online, perlindungan hak kekayaan intelektual. Selain itu Amerika juga mengatur mengenai transaksi

[6] *Opcid*, hlm. 5

elektronik dalam *Criminal Procedure* code dan bukti elektronik diatur dalam *Federal Rule Of Evidence* 2015 yang menjelaskan mengenai bukti berupa foto, video, rekaman didalam alat penyimpanan perangkat lunak *(shoftware).*

Di dalam *Criminal Procedure Code* terdapat peraturan mengenai keamanan komputer dan digital forensik antara lain :

1. Wire And Electronic Communications Interception And Interception Of Oral Communications.

2. Pen Registers and Trap and Trace Devices

3. Stored Wire And Electronic Communications And Transactional Records Access

Tabel 2 Perbandingan pengaturan pembuktian tindak pidana siber *(cybercrime)* antara Indonesia dan Amerika

No	Materi yang dibandingkan	Pengat`uran konvensional	*Electronic Evidenc* America
1.	Pengaturan pembuktian	Pasal 183 KUHAP menyatakan bahwa hakim menjatuhkan pidana ekurang-kurangnya du alat bukti yang sah dengan keyakinan bahwa suatu tindak pidana benar-benar terjadi dan terdakwalah yang bersalah melakukannya. Penjelasan pasal 183: ketentuan ini adalah untuk menjamin tegaknya kebenaran, keadilan, dan kepastian humum bagi seseorang.	Federal Rules Of Evidence 2015 Didalam aturan nomor 1005 menjelaskan bahwa untuk melakukan pembuktian dibutuhkan salinan untuk membuktikan alat bukti asli di persidangan. Barang bukti diatur dalam federal rule of evidence IX. Rule 901(a) secara umum. Untuk memenuhi persyaratan otentikasi atau identifikasi barang bukti, pemrakarsa harus menghasilkan bukti yang cukup untuk mendukung temuan bahwa barang bukti tersebut adalah apa yang diyakini oleh pemrakarsa tersebut
2.	Sistem peradilan pidana	Common law	Anglo Saxon

3.	Beban Pembuktian	*Presumption of innocence*	*Presumption of guilty* (Sistem Beban Pembuktian Biasa dan Sistem Pembuktian Terbalik)
5	Alat bukti pada tindak pidana siber *(cybercrime)*	Sesuai dengan Pasal 184 KUHAP a. Keterangan saksi b. Keterangan ahli c. Surat d. Petunjuk e. Keterangan terdakwa Dan pasal 5 UUITE (1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. (2) 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. (3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini. (4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk: a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan	Federal Rule of Evidence 2015 Pasal X. Isi dari tulisan, rekaman, dan foto Untuk alat bukti berupa tulisan, rekaman dan foto maka Aturan 1001. Definisi yang Berlaku untuk Artikel Ini Dalam artikel ini: (A) "Tulisan" terdiri dari huruf, kata, angka, atau seterunya yang setara dalam bentuk apapun. (B) "rekaman" terdiri dari huruf, kata, angka, atau catatan ekuivalennya dengan cara apapun. (C) "Foto" berarti gambar fotografis atau ekuivalennya yang tersimpan dalam bentuk apapun. (D) "asli" dari suatu tulisan atau rekaman berarti penulisan atau rekaman itu sendiri atau rekan lainnya Hal ini Dimaksudkan untuk memiliki efek yang sama oleh orang yang mengeksekusi atau mengeluarkannya. Lalu khusus Untuk informasi yang tersimpan secara elektronik, "Asli" disini berarti hasil cetakan - atau keluaran lain yang dapat

		b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.	dibaca oleh penglihatan - jika benar-benar mencerminkanInformasi sesuai dengan yang dibutuhkan. Yang dimaksud "Yang asli" dari sebuah foto termasuk yang negatif atau yang dicetak darinya. (E) "duplikat" berarti mitra yang diproduksi oleh mekanik, fotografi, kimia, elektronik, Atau proses atau teknik setara lainnya secara akurat mereproduksi yang asli

A. Alternatif Pengaturan Untuk Pembuktian Tindak Pidana Siber (*Cybercrime)*

Pasal X

Tata Cara Pembuktian

(1) Setiap barang bukti berupa tulisan, rekaman, dan foto harus asli dan dapat dibuktikan keorisinalitasnya pada saat proses persidangan.

(2) Untuk kepentingan penyelidikan barang bukti dapat diduplikat dari aslinya dengan syarat tertentu.

(3) Salinan barang bukti tersebut salinan harus dicatat atau diajukan di kantor publik yang diberi wewenang oleh undang-undang untuk kemudian disertfiikasi secara legal.

(4) Penyidik, dapat melakukan serangkaian proses digital forensik untuk menganalisa dan mengolah data komputer dan file-file yang tidak bisa diperiksa dengan mudah di pengadilan dengan kesaksian atau pernyataan pihak untuk membuktikan konten di hadapan pejabat yang diberi wewenang oleh undang-undang.

(5) Pada proses di pengadilan majelis hakim menentukan apakah penyidik telah memenuhi persyaratan faktual untuk mengakui bukti lain dari isi tulisan, rekaman, atau foto dengan sumber yang asli.

PENUTUP

A. Kesimpulan

Berdasarkan hasil penelitian diatas maka dapat diambil kesimpulan sebagai berikut:

1. Adanya kekosongan peraturan yang terdapat pada Undang-Undang Nomor 11 Tahun 2008 Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 ynag terkait tidak adanya pengaturan yang pasti mengenai tata cara pembuktian tindak pidana siber *(cybercrime).* Dalam proses pembuktian tindak pidana siber (*cybercrime*), dibutuhkan tata cara pembuktian yang benar dan merinci yang di atur dalam Undang-undang karena untuk membantu penyidik, penuntut umum ataupun hakim dalam mengungkapkan suatu kasus kejahatan siber(*Cybercrime*). Berkaitan dengan permasalahan yang dibahas mengenai pembuktian tindak pidana siber (*cybercrime)* yang menggunakan sarana *internet* aparat penegak hukum baik polisi, jaksa dan hakim masih mengacu pada Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan TransaksiElektronik untuk mengungkapkan suatu kejahatan siber *(cybercrime).*
2. Alat bukti kejahatan siber *(cybercrime)* mempunyai karakteristik yang berbeda dari alat bukti yang di atur dalam KUHAP karena bentuknya yang berupa perangkat lunak *(shofware)* oleh sebab itu pembuktian tindak pidana siber *(cybercrime)* harus diatur secara khusus dalam Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

B. Saran

1. Bagi aparat penegak hukum untuk memiliki kemampuan dalam melakukan digital forensic untuk mempermudah dalam melakukan pembuktian yang berhubungan dengan barang bukti elektronik.
2. Bagi pemerintah untuk memperhatikan mengenai pengaturan tata cara pembuktian tindak pidana siber *(cybercrime)* karena sangat penting sebagai acuan dalam menyelidiki kasus tersebut.

Daftar Pustaka

Buku

Sudikno Mertokusumo, **Mengenal Hukum Suatu Pengantar**, Liberty, Yogyakarta, 2003

Widodo, **Sistem Pemidanaan Dalam Cyber Crime**, Laksbang Mediatama, Malang, 2009, hlm 29

Edie O.S. Hiariej, **Teori dan Hukum Pembuktian**, Erlangga, Yogyakarta, 2012,

internet

Liputan6.com, **Orang Indonesia Rentan Menjadi Korban Kejahatan Online**, http://tekno.liputan6.com/read/2519790/orang-indonesia-paling-banyak-jadi-korban-penipuan-online, diakses tanggal 11/15/1016

*what is cyber crime investigation,*www.cyber/ASCL%20Certified%20Cyber%20Crime%Investigation

Undang-undang :

Undang-Undang Nomor11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Kitab Undang-Undang Hukum Acara Pidana

Criminal Procedure Code

Federal Rule Of Evidence 2015