BAB IV

PEMBAHASAN

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

Alvin Toffler menjelaskan tentang tiga hal perubahan kebudayaan sosial masyarakat yang mengubah peradaban manusia secara umum, yang pertama berkembangnya masyarakat agraris yang menghapus kebudayaan masyarakat nomaden yang hanya mengandalkan sumber daya alam untuk hidup, yang kedua dimulai sejak revolusi industri yang dimulai pada akhir abad 17 sampai dengan pertengahan abad 20, masa ini ditandai dengan standardinasi, spesialisasi, konsentrasi keuangan, energy, dan kekuasaan, serta produksi, distribusi dan konsumsi yang di lakukan secara masal; pada era ini muncul teknologi-teknologi yang menggantikan tenaga manusia. Ketiga disebut dengan *post-industrial society* yang dimulai sejak akhir yahun 1950an menekankan pada informasi dan bukan tenaga, era ini disebut juga dengan era informasi atau pengetahuan yang bergantung pada komputer. Era ini ditandai dengan berkembangnya ilmu pengetahuan seperti teori informasi serta teori ruang, dan teknologi-teknologi seperti *biology molecular,* dan *electronic quantum.* Selain itu, peningkatan produktivitas dimungkinkan melalui komputer dan proses data.[31]

Berdasarkan ulasan tentang perkembangan peradaban manusia di atas diketahui bahwa seiring perkembangan jaman ilmu teknologi

[31] The Third Wave (1980) dalam buku: Joshua Sitompul, ***Cyberspace, Cybercrime, Cyberlaw,*** Tatanusa,Jakarta,2012 hlm. 13

berkembang dengan pesat. Perkembangan teknologi komputer dan internet memberikan dampak terhadap pengaturan atau dan regulasi dalam hukum siber serta terhadap perkembangan kejahatan dalam *cyberspace* (ruang siber). **Howard F Lipson** berpendapat bahwa internet pada awalnya tidak pernah dirancang untuk *tracking* dan *tracing user behavior*, tetapi dirancang untuk kebutuhan militer dalam menghadapi perang dunia selain itu pada awal dibentuknya internet berada dalam satu control administrator. Sistem kontrol administrator ini mengatur secara penuh sistem perangkat lunak jaringan dan sistem perangkat keras komputer. Pengguna awal internet adalah anggota komunitas yang dapat diidentifikasi sehingga dalam hal pengguna melakukan penyalahgunaan jaringan atau perangkat, sistem administrator dapat segera mengetahuinya. Akan tetapi saat internet dilepas ke publik dan bisa diakses semua masyarakat maka bermunculan bermacam sistem administrator baik berupa organisasi maupun individu dari berbagai domain internet. Pola sistem administrasi sentral telah diubah dengan sistem administrasi dan desentralisasi. Hal ini berakibat aparat penegak hukum kesulitan dalam menangani pelaku tindak pidana.[32]

Disamping berbagai kemudahan dan manfaat yang diberikan teknologi internet dan komputer, internet juga menimbulkan dampak dan berbagai permasalahan hukum seperti transaksi online yang mudah dapat menimbulkan keraguan terhadap keamanan informasi, karena teknologi

---

[32] Howard F. Lipson, ***Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues***, November 2002, Special Report CMU0SEI-2002-SR-009, *Carnwgie Mellon University, United State. Dalam buku: Joshua Sitompul, Cyberspace Cybercrime Cyberlaw*, Tatanusa,Jakarta,2012 Hlm. 27

informasi yang bisa diakses orang lain tanpa diketahui para pihak, semakin berkurangnya saksi yang melihat secara langsung suatu kejadian dalam internet serta kebebasan anonimitas yang diterapkan dalam transaksi elektronik juga mengakibatkan sulitnya aparat penegak hukum dalam mencari dan menemukan pelaku tindak kejahatan siber (*cybercrime)*.[33]

Membicarakan tindak kejahatan *cybercrime* tentunya tidak lepas dari penegakan hukum yang mengaturnya. Hukum pada dasarnya merupakan pengaturan yang dibuat untuk mengatur perilaku seseorang di dalam masyarakat terhadap suatu pelanggaran dan dikenakan sanksi oleh negara. Meskipun dunia siber ialah dunia maya, hukum tetap diperlukan untuk mengatur sikap masyarakat, karena masyarakat yang ada di dunia maya adalah masyarakat yang hidup di dunia nyata yang memilki nilai dan kepentingan baik secara sendiri-sendiri maupun secara bersama-sama yang harus dilindungi dan hal yang terjadi di dunia maya kerap kali berhubungan dengan dunia nyata dan berakibat langsung bagi masyarakat seperti, transaksi yang dilakukan oleh masyarakat memiliki pengaruh dalam dunia nyata, baik secara ekonomis maupun non ekonomis.[34]

Di dalam dunia siber kejahatan bisa bertambah semakin kompleks dan beraneka ragam jenisnya dibanding di dunia nyata karena jutaan orang mengunjunginya tanpa batasan ruang dan waktu. Membicarakan tentang urgensi tata cara pembuktian tindak pidana siber *(cybercrime)* berarti membicarakan mengenai seberapa pentingnya tata cara pembuktian tersebut harus ada.

---

[33] Joshua Sitompul, **Cyberspace *Cybercrime* Cyberlaw**, Tatanusa,Jakarta,2012 Hlm29
[34] *idid*, Hlm 39

1. Alat Bukti Elektronik Mempunyai Sifat Mudah Rusak

Menurut **Alan M Gahtan** bukti elektronik adalah informasi yang tersimpan secara elektronik dalam setiap bentuk computer yang dapat digunakan sebagai bukti dalam suatu tindakan hukum.[35] Penjelasan tersebut menerangkan bahwa untuk kepentingan tindakan hukum 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*[36]*, source code, object code,* data yang tersimpan dalam file komputer, data yang tersimpan dalam metode penyimpanan elektronik seperti *flashdisk*, CD atau alat lain. Karakteristik bukti elektronik berbeda dengan bukti konvensional, bukti elektronik berupa bukti perangkat lunak *(shoftware).* Sesuai dengan pasal 1 ayat 1 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UUITE)[37] dan juga pasal 1 ayat 4 UUITE.[38] Bukti

---

[35]Alan M Gahtan, Elektronik Evidence(Toronto :Carswell:1999 Dalam: Siti Setiasari Hadiwinoto, 2012, **Perbandingan Alat Bukti Dan Beban Pembuktian Pada Kegiatan Transfer Dana Pada UU No.3 Tahun 2011 Tentang Transaksi Dana Dengan Elektronik Fund Transfer Act Di Amerika Serikat**(*online*), Fakultas Hukum UI, http://lib.ui.ac.id/file?file=digital/20311357-S42947-Perbandingan%20alat.pdf, Hl\m 116 (4 Oktober 2017)

[36] *Data base* menurut penjelasan pasal 12 ayat (1) Undang-Undang No 19 Tahun 2002 tentang hak cipta adalah kompilasi data dalam bentuk apapun yang dapat dibaca oleh mesin *(computer*) atau dalam bentuk lain yang karena alasan pemilihan atau pengaturan atas isi data itu merupakan kreasi intelektual.

[37]Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbataspada 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.

[38]Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal,

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.[39]

Salah satu karakteristik khusus bukti elektronik bentuknya yang disimpan dalam media elektronik, disamping itu bukti elektronik dapat dengan mudah direkayasa sehingga sering diragukan validitasnya.[40] Salah satu contohnya Seperti halnya dengan salah satu aplikasi chat saat ini yang dapat diunduh bebas di perangkat handphone yaitu line dari Line Corporation, pada fiture terbarunya line menyajikan fiture khusus untuk control obrolan dalam durasi tertentu yakni pada durasi satu jam, enam jam, dan dua puluh empat jam, jadi bukti elektronik bisa hapus dengan sendirinya, dimana apabila dikaitkan pada proses pembuktian hal ini menjadi kelehaman juga untuk obrolan *chating* yang digunakan sebagai alat bukti karena dengan mudahnya secara otomatis di hapus oleh aplikasi line itu sendiri, jadi hilangnya alat bukti tidak harus dari pelaku secara manual karena bisa diatur secara otomatis.

2. Sebagai Acuan Penyidik Dalam Memperlakukan Barang Bukti Elektronik

---

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

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

[40] *ibid*

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. Penyidik harus memiliki panduan tentang cara memperkenalkan bukti komputer ke pengadilan dengan menggunakan standart yang berlaku sesuai dengan undang-undang. Adanya peraturan mengenai tata cara melakukan pembuktian tindak pidana siber *(cybercrime)* dapat melindungi data yang telah diamankan dan juga berguna untuk mengamankan jaringan komputer, menangkap suatu informasi penting yang berguna untuk menangkap tersangka yang berkelompok.

Kejahatan yang melibatkan perangkat elektronik beraneka ragam mulai dari pornografi, terorisme, hingga pencurian data pribadi bahkan data suatu pemerintahan. Penyidik harus memiliki keahlian di bidang teknologi informasi dan perangkat elektronik yang memadai yang tepat untuk digunakan mengungkap suatu kejahatan. Suatu file komputer mungkin telah dihapus, rusak dan hilang akan tetapi hal tersebut bisa dipulihkan kembali dengan keahlian khusus.

Dalam prakteknya pejabat yang berwenang melakukan autentifikasi untuk memperkuat validitas bukti elektronik, untuk mempermudahnya Suatu arsip elektronik akan meliputi :

1. Validitas substansi informasi ditentukan oleh proses pengolahan informasi dan identitas hukum para pihak (*legal identity*).

2. Format formasi akan ditentukan oleh kepentingan para pihak dan/atau sesuai dengan konteks komunikasi yang terjadi, khususnya kepada siapa informasi itu ditujukan.
3. Tanggung jawab para pihak, baik sebagai si penyampai informasi (*originators*) dan si penerima/tujuan infomasi (*recipient*), sebenarnya dipengaruhi oleh kaedah-kaedah hukum yang berlaku, baik secara etis maupun berdasarkan peraturan perundang-undangan.
4. Validitas informasi sebagai *output*, secara teknis dan yuridis semestinya ditentukan oleh validitas sistem informasi dan komunikasi yang ada.[41]

Autentifikasi adalah melakukan sebuah proses untuk menjamin keaslian dokumen elektronik, karena bukti elektronik mudah dipalsukan dan dihapus. Autentikasi bukti elektronik dapat ditampilkan dalam bentuk cetak *hard copy* dari komputer atau alat penyimpanan data elektronik yang di salin langsung dari alat penyimpanan asli (*original*). Dalam kejahatan *cybercrime* seringkali aparat penegak hukum penyidik, penuntut umum, hakim dan pengacara dihadapkan pada kesulitan menentukan kebenaran bukti-bukti elektronik ketika menangani hal tersebut. Hal ini disebabkan katena mayoritas bukti elektronik yang ada berupa catatan-catatan elektronik yang tersimpan dalam alat penyimpanan data maupun yang dicetak dari komputer tersebut. Dan tidak semua orang bisa membaca data dalam komputer hanya sebagian orang tertentu seperti ahli dibidang teknologi informasi saja, oleh karena itu aparat penegak hukum seperti penyidik, pengacara, penuntut umum, dan

[41]Edmon Makarim, 2004:.211dalam Muhamad Jodi S dan Edy Herdyanto, **alat bukti elektronik sebagai alat bukti di persidangn dalam hukum acara pidana***(online)*http://jurnal.hukum.uns.ac.id/index.php/verstek/article/viewFile/703/657 (4 april 2017)

hakim harus mempunyai keahlian khusus dibidang teknologi informasi dan juga mempunuai acuan dasar di dalam undang-undang untuk melakukan pembuktian yang baik dan benar.

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, dikatakan sebagai alat bukti yang sah apabila telah memenuhi aspek keaslian sebagai alat bukti, dalam pengadilan hakim akan bertanya kepada terdakwa atau korban tentang surat elektronik tersebut, apakah terdapat perbedaan dari bentuk aslinya atau tidak, jika terdakwa atau korban mengakui bahwa surat elektronik tersebut sama dengan aslinya atau tidak terdapat perbedaan maka surat elektronik tersebut sah.

Apabila salah satu pihak tidak mengakui maka diperlukan keterangan ahli untuk menentukan sah atau tidaknya hasil cetak dari surat elektronik tersebut, dan keterangan ahli tersebut akan menjadi dasar pertimbangan hakim dalam menentukan sah atau tidaknya hasil cetak (*printout*) surat elektronik sebagai alat bukti dalam persidangan.[42] Adapun tata cara pembuktian tindak pidana siber *(cybercrime)* di indonesia selama ini dengan cara melakukan digital forensic dengan menggunakan bantuan ahli komputer. Karena permasalahan yang ada di dalam komputer sangat komplek oleh sebab itu dibutuhkan

[42]Muhamad Jodi S dan Edy Herdyanto, **alat bukti elektronik sebagai alat bukti di persidangan dalam hukum acara pidana***(online)*http://jurnal.hukum.uns.ac.id/index.php/verstek/article/viewFile/703/657 (4 april 2017

ahli dibidang komputer untuk memeriksa data rahasia, data yang sudah dihapus dan diubah.

Dalam jurnal international U.S. Departemnt of Justice yang berjudul Electronik Crime Scene Investigation :[43]

1. *Actions taken to secure and collect electronic evidence should not change that evidence.*
2. *Persons conducting examination of electronic evidence should be trained for the purpose.*
3. *Activity relating to the seizure, examination, storage, or transfer of electronic evidence should be fully documented, preserved, and available for review.*

Yang artinya:

1. Tindakan yang diambil untuk mengamankan dan mengumpulkan bukti elektronik seharusnya tidak mengubah bukti.
2. Orang yang melakukan pemeriksaan bukti elektronik harus dilatih untuk tujuan itu
3. Aktivitas yang berkaitan dengan perampasan, pemeriksaan, penyimpanan, atau pengalihan bukti elektronik harus didokumentasikan, diawetkan, dan tersedia untuk ditinjau.

Dari jurnal di atas dapat dimengerti bahwa untuk mengambil dan mengamankan barang bukti hingga sampai ke pengadilan tidak boleh mengubah barang bukti asli, oleh sebab itu penyidik dalam menangani kasus tersebut harus mempunyai keahlian khusus dibidang teknologi komunikasi.

[43] *National Institute of Justice U.S. Departement of Justice,* ***Electronic Crime Scene Investigation*****,** https://www.ncjrs.gov/pdffiles1/nij/219941.pdf, diakses 17 Mei 2017

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. Didalam istilah hukum Indonesia forensik artinya suatu ilmu pengetahuan yang menggunakan multi disiplin ilmu yaitu dengan menerapkan ilmu pengetahuan alam seperti kimia, fisika, biologi, psikologi, kedokteran, psikologi dan kriminologi yang bertujuan membuat terang suatu perkara pidana dan membuktikan ada tidaknya kejahatan atau pelanggaran dengan memeriksa barang bukti fisik dalam perkara tersebut.[44] Menurut jurnal internasional yang berjudul computer forensics, digital forensic adalah :[45]

> *"Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts. (The word forensics means "to bring to the court.") Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive".*
>
> Yang artinya :
>
> "Forensik adalah proses menggunakan pengetahuan ilmiah untuk mengumpulkan, menganalisis, dan menyajikan bukti ke pengadilan. (Kata forensik berarti "membawa ke pengadilan.") Forensik terutama berkaitan dengan

[44] Marwan, kamus hukum, rality publisher, Surabaya, 2009 hlm 211

[45] US-Cert, Computer Forensic, 2008, https://www.us-cert.gov/sites/default/files/publications/forensics.pdf, diakses 17 Mei 2017

> pemulihan dan analisis bukti ynag tidak terlihat (laten). Bukti laten dapat mengambil banyak bentuk, dari sidik jari yang tertinggal di jendela sampai bukti DNA pulih dari noda darah ke file pada hard drive".

Digital forensik juga bisa diartikan sebagai:

> *"Computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law".*

Yang artinya:

> "Forensik komputer sebagai disiplin yang menggabungkan unsur hukum dan ilmu komputer untuk mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan dengan cara yang dapat diterima sebagai bukti di pengadilan".

Itu sebabnya mengapa hasil analisa dari digital forensik harus bisa dipertanggungjawabkan di sidang pengadilan. Digital forensik tidak hanya diperlukan untuk menganalisa kasus tindak pidana siber *(cybercrime)* tetapi juga di perlukan untuk semua kasus tindak pidana karena saat ini semua kasus memiliki bukti digital karena di akibatkan dari pengaruh perkembangan zaman yang modern. Digital forensik sangat diperlukan didalam semua kasus tindak pidana karena mampu menemukan data yang sulit dicari sekalipun. Dan saat melakukan digital forensik seharusnya menerapkan prosedur untuk mengunpulkan dan mengamankan bukti digital.

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. 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
2. Analisa
3. Presentasi

Sesuai yang telah dijelaskan dalam jurnal internasional yang berjudul *Open Source Digital Forensics Tools* yang menjelaskan sebagai berikut :

> *"The Acquisition Phase saves the state of a digital system so that it can be later analyzed.This is analogous to taking photographs, fingerprints, blood samples, or tire patterns from a crime scene. As in the physical world, it is unknown which data will be used as digital evidence so the goal of this phase is to save all digital values. At a minimum, the allocated and unallocated areas of a hard disk are copied, which is commonly called an image.Tools are used in the acquisition phase to copy data from the suspect storage device to a trusted device. These tools must modify the suspect device as little as possible and copy all data. The*

Analysis Phase takes the acquired data and examines it to identify pieces of evidence. There are three major categories of evidence we are looking for":

1. Inculpatory Evidence: That which supports a given theory

2. Exculpatory Evidence: That which contradicts a given theory

3. Evidence of tampering: That which can not be related to any theory, but shows that the system was tampered with to avoid identification

This phase includes examining file and directory contents and recovering deleted content. The scientific method is used in this phase to draw conclusions based on the evidence that was found.Tools in this phase will analyze a file system to list directory contents and names of deleted files, perform deleted file recovery, and present data in a format that is most useful. This phase should use an exact copy of the original, which can be verified by calculating an MD5 checksum. It is important that these tools show all data that exists in an image.

Regardless of the investigation setting (corporate, federal, or military), the steps performed in the acquisition and analysis phases are similar because they are dominated by technical issues, rather than legal. The Presentation Phase though is based entirely on policy and law, which are different for each setting. This phase presents the conclusions and corresponding evidence from the investigation.

Yang artinya :

"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. Paling tidak, area yang dialokasikan dan tidak terisi dari hard disk disalin, yang biasanya disebut gambar. Alat digunakan dalam tahap akuisisi untuk menyalin data dari perangkat penyimpanan tersangka ke perangkat tepercaya. Alat ini harus memodifikasi perangkat tersangka sesedikit mungkin dan menyalin semua data. Fase Analisis mengambil data yang diperoleh dan memeriksanya untuk mengidentifikasi beberapa bukti. Ada tiga kategori utama bukti yang kami cari":

1. Bukti Dakwaan: Itu yang mendukung teori yang diberikan
2. Bukti eksepsi: Itu yang bertentangan dengan teori yang diberikan
3. Bukti gangguan: Hal yang tidak dapat dikaitkan dengan teori apapun namun menunjukkan bahwa sistem tersebut dirusak untuk menghindari identifikasi

Fase ini mencakup pemeriksaan isi file dan direktori dan memulihkan konten yang terhapus. Metode ilmiah digunakan pada tahap ini untuk menarik kesimpulan berdasarkan bukti yang ditemukan. Alat dalam tahap ini akan menganalisa sistem berkas untuk mencantumkan isi direktori dan nama file yang terhapus, melakukan recovery file yang terhapus, dan menyajikan data dalam format yang paling berguna. Fase ini harus menggunakan salinan asli yang sebenarnya, yang dapat diverifikasi dengan menghitung checksum MD5. Adalah penting bahwa alat ini menunjukkan semua data yang ada pada gambar.

Terlepas dari pengaturan investigasi (korporat, federal, atau militer), langkah-langkah yang dilakukan dalam fase akuisisi dan analisis serupa karena didominasi oleh masalah teknis, dan bukan legal. Tahap Presentasi meskipun didasarkan sepenuhnya pada kebijakan dan undang-undang, yang berbeda untuk setiap setting. Fase ini menyajikan kesimpulan dan bukti yang sesuai dari penyelidikan.

Dari keterangan di atas ketiga tahap tersebut saling berkaitan, akuisisi adalah tahap penyimpanan bukti digitas sebelum dianalisis, gunanya menganalisa bukti digital untuk mengembalikan file yang terhapus, membuat salinan dll, selanjutnya yang terakhir tahap presentasi untuk memberi kesimpulan pada data yang telah periksa. Adapun di Indonesia sendiri untuk memperoleh dan memperlakukan bukti elektronik aparat penegak hukum juga melakukan digital forensik dengan tahapan-tahapan sebagai berikut :

1. Pengambilan Bukti Digital

Mengingat sifatnya yang dapat diubah, dirusak, atau dihilangkan apabila tidak ditangani dengan tepat, pengambilan informasi atau dokumen

elektronik harus dilakukan dengan menjaga dan melindungi keutuhan atau integritasnya. Tahap ini dimaksudkan untuk mengambil dan mengamankan alat bukti elektronik *(original).* Cara atau prosedur pengambilan alat bukti elektronikoriginal dapat didasarkan pada kondisi awal ditemukannya alat bukti elektronik atau alatperangkat yang menyimpan alat bukti elektronik tersebut. Alat penyimpanan yang bisa dijadikan sebagai barang bukti mencakup sebuah sistem komputer, media penyimpanan seperti *handphone, flash disk, hard disk, pen drive, smart card,* atau *CD-ROM), PDA, e-mail, sms, cookies, source code, windows registry, , document, web browser bookmark, chat loglog file*, atau bahkan sederetan paket yang berpindah dalam jaringan komputer. Untuk memberikan gambaran, sebagai contoh, *ACPO assosiation of chief police officers* memberikan prosedur penanganan terhadap computer yang ditemukan dalam keadaan menyala dan dalam keadaan mati.

2. Kewajiban menyimpan dokumen elektronik.

   Ada kalanya hukum mengharuskan pihak tertentu untuk menyimpan data atau dokumen untuk jangka waktu tertentu, misalnya untuk keperluan akuntansi atau pajak. Akan tetapi, suatu data elektronik tidak selamanya dapat diharapkan disimpan dalam bentuknya yang asli mengingat tidak jarang data tersebut disimpan dalam bentuk yang sudah dipendekkan, atau diubah bentuk dan format dan sebagainya.

   Oleh karena itu, jika data atau dokumen tersebut merupakan data elektronik, maka kewajiban data atau dokumen tersebut harus dianggap telah memenuhi persyaratan hukum jika:

a. Informasi dalam dokumen elektronik tersebut masih dapat diakses untuk masa selanjutnya;
b. Informasi tersebut disimpan tetapi masih dapat diidentifikasi keasliannya dan tujuannya, dan dapat pula ditentukan waktu data tersebut diterima atau dikirim
c. Informasi disimpan dalam format asli ketika disimpan, dikirim, atau diterima, atau dalam format yang dapat ditunjukkan bahwa data tersebut merepresentasikan secara akurat terhadap informasi yang disimpan, dikirim, atau diterima tersebut.

Namun demikian, kewajiban menyimpan data tersebut tentunya tidak berlaku terhadap data atau informasi yang mempunyai tujuan hanya untuk dikirim atau diterima;[46] Penyimpanan dan penyiapan bukti-bukti yang ada, termasuk melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu. Bukti harus benar-benar steril artinya belum mengalami proses apapun ketika diserahkan kepada ahli digital forensik untuk diteliti. Karena bukti digital bersifat sementara (volatile), mudah rusak, berubah dan hilang, maka pengetahuan yang mendalam dari seorang ahli digital forensik mutlak diperlukan. Kesalahan kecil pada penanganan bukti digital dapat membuat barang bukti digital tidak diakui di pengadilan. Bahkan menghidupkan dan mematikan komputer dengan tidak hati-hati bisa saja merusak/merubah barang bukti tersebut. Karena saatkomputer dihidupkan terjadi beberapa perubahan pada temporari file, waktu akses, dan seterusnya. Sekali file-file ini telah

[46] *ibid*

berubah ketika komputer dihidupkan dan tidak ada cara untuk mengembalikan *(recover)* file-file tersebut kepada keadaan semula. Karena komputer dalam kondisi hidup juga tidak bisa sembarangan dimatikan, sebab jika komputer dimatikan data-data yang ada bisa terhapus oleh program komputer. Oleh sebab itu seorang ahli digital forensik harus menguasai langkah-langkah tertentu dalam mematikan/menghidupkan komputer agar tidak merusak/menghilangkan barang bukti yang ada di dalamnya.

Aturan utama pada tahap ini adalah bukti asli tidak boleh di ikutkan dalam penydikan karena dikhawatirkan akan dapat merubah isi dan struktur yang ada didalamnya. Untuk mengatasi hal ini maka dilakukan penyalinan *copy* data secara *Bitstream Image*[47] dari bukti asli ke media penyimpanan lainnya. Dengan kata lain, setiap biner digit demi digit di-copy secara utuh dalam media baru. Teknik ini umumnya diistilahkan dengan cloning atau imaging.Data hasil cloning inilah yang selanjutnya menjadi objek penelitian dan penyelidikan.[48]

3. Pemeriksaan alat bukti

Pemeriksaan terhadap alat bukti elektronik original umumnya menggunakan perangkat keras dan perangkat lunak ynag khusus dibuat untuk kepentingan digital forensic.Pada tahap ini, pemeriksa melakukan ekstraksi, yaitu mengambil seluruh data dari media dimana data tersebut

[47] *Bitstream image* adalah metode penyimpanan digital dengan mengkopi setiap bit demi bit dari data orisinil, termasuk file yang tersembunyi *(hidden files*), file temporer (*temporary file*), file yang terdefrag (*defragmented file*), dan file yang belum teroverwrite

[48] Asrizal, DigitalForensik *(online),* http://edokumen.kemenag.go.id/files/VQ2Hv7uT1339506324.pdf(11,April 2017)

mengambil seluruh data dari media dimana data tersebut tersimpan, termasuk data yang telah terhapus sebelumnya. Pemeriksa juga perlu menggunakan *write blocker,* yaitu alat yang digunakan untuk mencegah penulisan terhadap data original. Selain itu, dalam melakukan pengambilan data, pemeriksa juga perlu menentukan nilai dari keseluruhan data ynag diambil *(hash)*. Nilai *(hash)* dari data original akan sama dengan nilai dari hasil ekstraksi. Sehingga, apabila diperlukan pemeriksaan ulang oleh pemeriksa yang berbeda (misalnya pemeriksa dari advikat tersangka), nilai dari alat bukti elektronik tersebut akan sama. Setelah alat bukti elektronik harus dilakukan dengan membuat salinan dari informasi atau dokumen elektronik yang asli. Pengambilan informasi atau dokumen elektronik dilakukan, tahap selanjutnya ialah pemeriksaan dan analisa terhadap alat selanjutnya ialah pemeriksaan dan analisa terhadap alat bukti elektronik.pemeriksaan dilakukanterhadap salinan dari alat bukti elektronik yang asli.

Pemeriksa juga dapat membuat salinan dari alinan alat bukti elektronik sebagibahan kerja.Pada tahap ini, pemeriksa juga melakukan analisa, yaitu adalah mengintepretasikan informasi yang telah diekstraksi dan menentukan informasi atau data yang relevan dengan tindak pidana. Tergantung dari jenis tindak pidana, dalam tahap ini, pemeriksa mencari informasi elektronik atau dokumen elektronik yang menunjukan adanya tindak pidana atau menunjukan pelaku tindak pidana. Misalnya, dalam tindak pidana penyebaran pornografi, pemeriksa harus menemukan adanya file-file pornografi dalam computer, laptop, atau USB pelaku. Untuk

membuktikan adanya penyebaran, pemeriksa dapat mencari rekaman email yang masih tersimpan dalam computer pelaku; dari rekaman email tersebut, pemeriksa dapat mengetahui penerima email. Dalam tindak pidana akses illegal, pemeriksa harus menemukan adanya rekaman aktivitas transaksi elektronik *log file* yang menunjukan bahwa pelaku, dengan menggunakan IP tertentu, berhasil mengakses sesuatu website secara illegal.

4. Dokumentasi dan presentasi;

Setiap tindakan yang dilakukan dalam pengumpulan dan pemeriksaan alat bukti elektronik harus didokumentasikan secara akurat dan menyuluruh. Tindak hanya tindakan dalam melakukan digital forensk, tetapi juga tindakan yang terkait dengannya, misalnya serah terima computer dari petugas ynag mengambil barang di tempat kejadian perkara kepada pemeriksa forensik. Laporan dapat memuat proses dan tahapan yang dilakukan dalam pemeriksaan, termasuk alat dan perangkat yang digunakan. Selain itu, laporan juga perlu memuat informasi mengenai keseluruhan data yang diperoleh serta yang relevan dengan tindak pidana.

Penanganan yang tidak tepat terhadap komputer yang menyala dapat menghilangkan informasi elektronik yang sifatnya *volatile*. Tindak diberikannya label terhadap komponen serta kabel atau port dari alat dan perangkat yang telah dipreteli di tempat kejadian perkara dapat menyulitkan analisis digital forensik untuk menyusun kembali perangkat tersebut di laboratorium forensik. Demikian juga pencatatan yang tidak

lengkap dapat menimbulkan keraguan hakim atau pengacara terhadap hasil forensik yang dilakukan.

Dalam pengumpulan alat bukti elektronik, penyidik akan menemukan berbagai informasi, baik yang relevan dengan tindak pidana, maupun yang tidak relevan. Terkait dengan hal ini, penyidik harus menjaga kerahasiaan informasi, khususnya informasi terkait privasi seseorang yang tidak relevan dengan tindak pidana. Semua informasi yang tidak relevan tidak boleh diungkap di pengadilan.

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

Sistem peradilan pidana dibentuk untuk menanggulangi kejahatan di masyarakat yaitu terdapat serangkaian subsistem pendukung yang saling berkaitan yakni kepolisian, kejaksaan, pengadilan dan lembaga pemasyarakatan yang secara keseluruhan membentuk kesatuan lembaga penegak hukum. Tugas dan wewenang lembaga penegak hukum masing-masing secara garis besar adalah sebagai berikut:[49]

1. Kepolisian

Tugas kepolisian di bidang penyidikan, melakukan penyidikan tambahan, berperan sebagai koordinator dan pengawas Penyidik Pegawai Negeri Sipil adalah kewenangan kepolisian. KUHAP ini mengatur cara mengenai dapat atau tidaknya dilakukan penyidikan dgn mencari tau dan

[49] *Opcid* hlm 14

menemukan suatu peristiwa yang diduga sebagai tindak pidana yg merupakan ruang lingkup penyelidikan.[50]

2. Kejaksaan

Lembaga kejaksaan bertugas melakukan penuntutan terhadap suatu tindak pidana.Kejaksaan bertugas sebagai lembaga penuntut dan pelaksana dari putusan pengadilan pidana dari semua tingkat pengadilan.Tugas-tugasnya adalah melaksanakan putusan-putusan pengadilan pidana mempertahankan ketentuan undang-undang, melakukan penuntutan tindak-tindak pidana pelanggaran dan kejahatan melakukan penyidikan dan penyidikan lanjutan. Di dalam Undang-undang Nomor 16 tahun 2004 Tentang Kejaksana Republik Indonesia pasal 2 menyatakan bahwa Kejaksaan adalah lembaga pemerintahan yang melaksanakan kekuasaan negara di bidang penuntutan serta kewenangan lain berdasarkan undang-undang.[51]

3. Pengadilan

Lembaga pengadilan adalah pelaksanaan atau penerapan hukum terhadap suatu perkara dengan suatu putusan hakim yang bersifat melihat, putusan mana dapat berupa pemidanaan, pembebasan maupun pelepasan dari hukuman terhadap pelaku tindak pidana.

Di sini lembaga pengadilan adalah lembaga penegak hukum yang paling penting dikarenakan untuk menentukan terdakwa tersebut bersalah atau tidak. Hakim memiliki peranan yang sangat besar untuk menentukan

[50] UU Nomor 26 tahun 2000, pasal 1 angka 5

[51] Di dalam Undang-undang Nomor 16 tahun 2004 Tentang Kejaksana Republik Indonesia pasal 2

pelaksanaan sistem peradilan pidana hakim tidak boleh pandang bulu dalam melaksanakan putusan.

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, beberapa sistem pembuktian sebagai berikut :

a. sistem atau teori pembuktian berdasarkan undang-undang secara positif (*positive wettelijk bewijstheorie*)
b. sistem atau teori pembuktian berdasarkan keyakinan hakim melulu
c. sistem atau teori pembuktian berdasar keyakinan atas alasan yang logis (*laconviction raisonnee*)
d. teori pembuktian berdasarkan undang-undang secara negative (*negatief wettelijk*)

Pembuktian yang dianut oleh Indonesia adalah pembuktian menurut undang-undang secara negative (*negatief wettelijk*), Sistem pembuktian ini merupakan gabungan dari sistem pembutian menurut undang-undang secara positif dan sistem pembuktian berdasarkan keyakinan hakim melulu

(*conviction intime)*. Dari gabungan antara kedua sistem pembuktian yang saling bertabrakan ini terwujudlah suatu sistem hukum dimana seorang terdakwa baru dapat dinyatakan bersalah apabila terbukti dari keyakinan hakim berdasarkan cara pembuktian dan alat bukti menurut undang-undang. Hal ini sesuai pasal 183 KUHAP yang berbunyi :

> "hakim tidak boleh menjatuhkan pidana kepada seseorang, kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya."[52]

Dengan demikian, pembuktian harus di dasarkan pada ketentuan dan cara pembuktian yang ditentukan di dalam KUHAP berdasarkan keyakinan hakim. Namun dalam sistem pembuktian ini juga mempunyai titik kelemahan yaitu apabila di dalam undang-undang semua unsur terpenuhi namun hakim tidak yakin akan bukti tersebut terdakwa harus dibebaskan dari tuntutan hukum. Dalam pembuktian tindak pidana elektronik hakim akan mempertanyakan keaslian alat bukti elektronik, jika alat bukti tersebut dinyatakan asli maka sah menurut undang-undang namun jika tidak maka diperlukan bantuan dari ahli untuk membuktikan keaslian alat bukti untuk menjadi dasar pertimbangan hakim. Dalam menggunakan bukti elektronik pada suatu perkara yang terjadi dalam transaksi elektronik terdapat tiga hal yang dapat dijadikan panduan antara lain adalah:

a. Dalam melakukan tindak pidana siber (*cybercrime)* adanya pola (modus operandi) yang relatif sama dengan menggunakan komputer;

---

[52] Pasal 183 KUHAP

b. Antara satu peristiwa dengan peristiwa yang lain terdapat kesesuaian;

c. Adanya motif (alasan melakukan tindak pidana).

Agar suatu transaksi elektronik dalam pengadilan pidana dapat diterima menjadi bukti terdapat beberapa cara, antara lain:[53]

1. *The real evidence route.*

   Bukti elektronik sebagai suatu alat bukti yang sah dan yang berdiri sendiri (*real evidencce*) tentunya suatu rekaman/salinan data(*data recording*) harus dapat memberikan jaminan berjalan sesuai dengan prosedur yang berlaku (telah diprogram) sedemikian rupa sehingga dalam pembuktian suatu kasus hasil *print out* suatu data dapat diterima;

2. *The statutory route.*

   Suatu bukti elektronik dapat diterima sebagai alat bukti di pengadilan jika suatu data (*statutory route*) sudah di tetapkan dan dikatakan sah.Contohnya dalam suatu kasus dengan mempertimbangakan suatu dokumen merupakan dokumen publik maka mengedepankan salinan dokumen berupa ijazah. Dokumen atau data tersebut disahkan oleh negara atau pengadilan yang merupakan pihak yang memiliki kewenangan dan dalam hal pembuktian suatu kasus, keabsahan data/dokumen tidak harus tercetak di atas kertas tapi juga termasuk data atau informasi yang ada dalam sebuah disket, dokumen yang diterima dengan menggunakan komputer melalui fasilitas telekomunikasi (*fax,e-mail*) sepanjang dapat

[53]Naskah Akademik Rancangan Undang-Undang tentang Tanda Tangan Elektronik danTransaksi Elektronik Lembaga Kajian Hukum Teknologi, Fakultas Hukum Universitas Indonesia(lkht-fhui), Depok, 2001, dalam: Sahuri Lasmadi, **Pengaturan Alat Bukti Dalam Tindak Pidana Dunia Maya,**2014, hlm 5

dibuktikan data/informasi itu asli (*original*) atau hasil *photocopy* yang otentik, kemungkinan data atau informasi tersebut dapat diterima. Pada kategorisasi ini yang ditetapkan adalah data atau informasi yang ada di dalamnya, atau data tersebut dinyatakan otentik.

3. *The expert witness.*

Selanjutnya dalam peranan saksi ahli (*the expert witness*) adalah bahwa keterangan seorang ahli dapat dijadikan alat bukti terhadap suatu kasus, dimana keterangan yang diberikan berdasarkan pada pengetahuan dan pengalaman. Hakin akan mempertimbangkan kesaksian seorang ahli terutama mengenai kekuatan pembuktian suatu alat bukti dan memberikan suatu standar keakuratan dan keobjektifan bekerjanya suatu sistem komputer. Seorang ahli dapat dipanggil jika terjadi suatu kasus penggunaan komputer secara ilegal maka di dalam suatu persidangan kemudian saksi tersebut memberikan keterangan mengenai cara kerja dan sistem kompuer.

Ketentuan hukum pidana materil yang mengatur tindak pidana *cyber* dapat dilaksanakan hanya berdasarkan hukum pidana formil atau hukum acara pidana.Dalam konteks penegakan hukum, kriminalisasi tindak pidana mempunyai kaitan langsung dengan hukum acara pidana. Sebagaimana yang terdapat pada Pasal 44 yang menentukan bahwa alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

a. Alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan;

b. Alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

Kejahatan siber memiliki karakter yang berbeda dengan tindak pidana umum yang diatur dalam KUHAP sehingga butuh penanganan dan pengaturan khusus di luar KUHAP, seperti bukti elektronik yang belum diatur secara khusus dalam KUHAP. KUHAP yang merupakan payung hukum pidana formil di Indonesia diketahui merupakan hukum acara untuk melaksanakan hukum pidana materil yang utamanya diatur dalam KUHP dimana dalam KUHP memuat aturan-aturan untuk melaksanakan proses peradilan pidana, mulai tahap penyidikan, penuntutan, persidangan, sampai pelaksanaan putusan pengadilan. Dalam perkembangannya terdapat undang-undang baru yang lahir yang khusus mengatur pidana materil, seperti halnya UU ITE. Dari penjelasan tersebut dapat dipahami antara UU ITE dan KUHAP adalah dua peraturan yang saling berkaitan mengatur tentang tindak pidana siber.

Menurut hukum telematika (*cybercrime)* adalah kejahatan yang di lakukan di internet terkait *cyberlaw*.[54] *Cybercrime* merupakan suatu tindak kejahatan yang dilakukan di dunia maya dan teknologi komputer sebagai alat kejahatan utamanya.*Cybercrime* memanfaatkan perkembangan teknologi komputer khususnya internet.Secara umum yang dimaksud dengan kejahatan komputer atau kejahatan didunia *cyber* adalah upaya untuk memasuki dan/atau menggunakan fasilitas komputer atau jaringan

[54]Marwan,Op. cit hlm142

komputer tanpa izin dan melawan hukum dengan atau tanpa menyebabkan perubahan dan/atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut.[55]

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 penegcualian untuk sementara mengenai ketentuan khusus acara pidana (hukum pidana formil) diberlakukan undang-undang tertentu sebelum ditinjau kembali, diubah atau dinyatakan tidak berlaku lagi terhadapnya.

Sehubungan dengan hal pembuktian, hukum sebenarnya sudah lama mencoba memperluas penafsiran asas dan norma ketika menghadapi persoalan yang tidak berwujud, seperti kasus yang penah terjaid di Indonesia yakni pencurian listrik yang kemudian dikualifikasikan sebagai tindak pidana. Pembuktian menjadi hal yang sangat penting mengingat informasi elektronik bukan saja belum terakomodasikan di dalam hukum acara pidana Indonesia

[55]Josua Sitompul, ***Cyberspace Cybercrime Cyberlaw*** **tinjauan Aspek Hukum Pidana**, (Tatanusa, Jakarta: 2012), hlm 35

secara komprehensif karena sangat rentannya alat bukti yang mudah untuk diubah, disadap, dipalsukan dan dikirim ke berbagai penjuru dunia dalam waktu hitungan kurang dari seperdetik saja.[56] Yang menjadi pertanyaan saat ini apakah system pembuktian konvensional yang dianut KUHAP dapat diterapkan untuk membuktikan perbuatan pidana sesuai ketentuan pasal 30 ayat (3) Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transkasi Elektronik maka hal tersebut yang akan menjadi focus penulis dalam sub bab ini. Pembuktian merupakan factor penting dalam proses pemeriksaan di persidangan.

Dari pembuktian tersebut menentukan nasib seseorang dengan status sebagai terdakwa. Jika kesalahan yang didakwakan kepada seseorang tidak dapat dibuktikan berdasarkan alat-alat bukti yang ditentukan Undang-Undang, maka terdakwa harus dibebaskan dari hukuman/ pidana yang menjadi ancaman perbuatannya. Sebaliknya, apabila alat bukti yang sah menurut ketentuan Undang-Undang yang berlaku dapat membuktikan kesalahan terdakwa, maka terdakwa harus dinyatakan bersalah dan harus dijatuhi pidana untuk mempertanggungjawabkan perbuatan/ tindak pidana yang telah dilakukannya. Jika ketentuan Pasal 183 KUHAP dihubungkan dengan jenis alat bukti in casu yang diatur KUHAP maupun Undang-Undang tentang Informasi dan Transaksi Elektronik, maka terhadap terdakwa dapat dijatuhi pidana apabila kesalahannya dapat dibuktikan paling sedikit dengan dua jenis alat bukti yang disebutkan dalam Pasal 184 ayat (1) juncto Pasal 5 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[56] Maskun, **Kejahatan Siber Cyber Crime**, Pranada Media Grup,Jakarta, 2013, hlm. 31

Yang untuk lebih jelasnya, untuk membuktikan kesalahan terdakwa harus merupakan:

a. Penjumlahan dari sekurang-kurangnya seorang saksi ditambah dengan seorang ahli, atau informasi dan/ atau dokumen elektronik maupun petunjuk, dengan ketentuan penjumlahan kedua alat bukti tersebut harus "saling bersesuaian", "saling menguatkan", dan tidak saling bertentangan antara satu dengan yang lain;
b. Penjumlahan dua alat bukti itu berupa keterangan dua orang saksi yang saling bersesuaian dan saling menguatkan, maupun penggabungan antara keterangan seorang saksi dengan keterangan terdakwa, asal memiliki persesuaian dengan jelas antara keterangan saksi dengan keterangan terdakwa.

Selain ketentuan *bewijs minimum* menurut pasal 183 KUHAP sebagai aturan umum pembuktian, ketentuan pasal 185 ayat (2) KUHAP dan pasal 189 ayat (4) KUHAP juga mengandung prinsip minimal pembuktian antara lain untuk pasal 185 ayat (2) mengandung prinsip *unus testis nullus testis* atau satu saksi bukan saksi; dan untuk pasal 189 ayat (4) mengandung prinsip pengakuan atau keterangan terdakwa saja tidak cukup untuk membuktikan kesalahannya. Penulis berpendapat bahwa meskipun delik ini adalah delik khusus dalam ruang lingkup kejahatan siber (*cyber crime*) namun penggunaan prinsip *bewijs minimum* tetap dipertahankan dengan tentunya berdasarkan pula pada keyakinan hakim sebagaimana system pembuktian *Negatief WettelijkStelsel* yang dianut oleh KUHAP.

Di dalam pasal ini masih terlihat tidak jelas mengenai ketentuan yang mengatur tentang Informasi dan Transaksi Elektronik dianggap sah sepanjang informasi tersebut dapat diakses, ditampilkan,dijamin keutuhannya, dan dapat dipertanggungjawabkan. Kejahatan siber *(cybercrime)* memiliki karakter yang berbeda dengan tindak pidana umum yang di atur dalam KUHAP sehingga butuh penanganan dan pengaturan khusus di luar KUHAP, seperti bukti elektronik yang belum di atur secara khusus dalam KUHAP. Perkembangan teknologi informasi yang demikian pesatnya haruslah di antisipasi dengan hukum yang mengaturnya, Kendala yuridis dalam Undang-undang ini juga belum sepenuhnya mengatur mengenai pembuktian *cybercrime,* padahal pembuktian adalah faktor terpenting dalam persidangan salah satunya tidak mengatur secara khusus seperti pasal mengenai pembuktian tindak pidanasiber (*cybercrime)* belum dapat mencangkup secara keseluruhan mengenai tata cara pembuktian yang seperti apa yang bisa diterapkan dalam hukum Indonesia agar lebih mudah aparat hukum dalam menangani kasus tersebut, keterbatasan aturan hukum tersebut mengakibatkan kekosongan peraturan. Undang-undang Informasi dan Transaksi Elektronik haruslah fleksibel agar sesuai dengan perkembangan jaman, karena teknologi akan semakin berkembang pada masa ke masa maka hukum juga harus menyesuaikan perkembangan teknologi dengan mengisi kekosongan peratutan.

Demikian pula halnya dengan pengaturan tindak pidana siber (*cybercrime)* dalam perundang-undangan Indonesia, khususnya UU ITE dapat dijalankan dengan berdasarkan ketentuan mengenai hukum acara

pidananya.sebagaimana diatur dalam Undang-Undang Nomor 8 Tahun 1981. Namun karena tindak pidana siber (*cybercrime)* memiliki karakteristik teknologi informasi dan komunikasi, mudah dan cepat, *anonymity, borderless,* mempunyai efek yang masif, dan transnasional yang berbeda dengan tindak pidana tradisional maka ketentuan dalam KUHAP tidak dapat dilaksanakan sepenuhnya.

Ketentuan mengenai penyelidikan dan penyidikan serta alat bukti dalam pemberantasan tindak pidana siber (*cybercrime)* yang tercantum pada pasal 183 dan 184 mengenai pembuktian Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP) memiliki perbedaan dalam pemberantasan tindak pidana tradisional. Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP) dibentuk pada era berkembangnya kejahatan komputer yang kemudian pada tahun 1990 mengalami transformasi menjadi tindak pidana *cyber*, belum mengatur berbagai aspek mengenai teknologi informasi dan komunikasi termasuk sistem computer atau sitem elektronik dalam ketentuan-ketentuan hukum acara pidananya sehingga terdapat masalah hukum ketika digunakan dalam pemberantasan tindak pidana siber (*cybercrime)*.[57]

Di dalam KUHAP banyak peraturan yang sudah tidak sesuai dengan masa sekarang yang sudah jauh berubah seperti keadaan sosial, budaya, ekonomi, dan teknologi.Sebagaian rumusan KUHAP ada yang sudah tidak sesuai dengan permasalahan yang dihadapi masyarakat saat ini.

---

[57]Sigid Suseno, **Yurisdiksi Tindak Pidana Siber**, Refika Aditama, Bandung, 2012, hlm 220

Perkembangan globalisasi saat ini telah membuat masyarakat Indoneisa menjadi masyarakat yang modern, globalisasi masuk dalam segala aspek kehidupan termasuk teknologi informasi, oleh sebab itu Indonesia membutuhkan peraturan baru yang bisa seimbang dengan perkembangan saat ini seperti proses penegakan hukum yang cepat, pembuktian tindak pidana yang efektif dan lain sebagainya.

Berdasarkan uraian di atas dengan semakin maraknya penggunaan internet pada dunia siber (*cyberspace*) tidak hanya dimanfaatkan secara positif saja tetapi juga secara negative demi menguntungkan salah satu pihak yakni pelakunya sendiri.Meskipun hal tersebut dilakukan di dunia maya namun pelakunya berada di dunia nyata.Sehingga ketika terjadi suatu tindak pidana tentunya tidak lepas dari penegakan hukumnya. Melihat beberapa kasus yang sering terjadi mengenai tindak pidana siber (*cybercrime*), sudah seharusnya menjadi perhatian juga oleh aparat penegak hukum. Meskipun tindak pidana siber dilakukan di dunia maya namun dampaknya dirasakan di dunia nyata. Tentunya hal ini sudah bisa menjadi alasan mengapa tindak pidana siber *(cybercrime)* perlu diatur secara khusus di dalam peraturan perundang-undangan di Indonesia yakni Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sifatnya yang berbeda dan memerlukan pembuktian secara khusus mengingat alat bukti yang bersifat perangkat lunak (*software*) berupa data elektronik yang sangat mudah untuk diubah dan dirusak dan dengan bahkan perusakan tersebut dapat ditutupi menjadikan tindak pidana siber tidak dapat disamakan dengan tindak pidana pada umumnya seperti yang pencurian, pembunuhan dan tindak pidana yang lain

yang alat buktinya didapati di dunia nyata. Tata cara pembuktian yang begitu rumit tampaknya belum menjadi fokus pembuat undang-undang untuk mengatur. 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

1. Proses Analisa Bukti Elektronik

Amerika Serikat adalah negara federal yang tersusun dari negara-negara bagian yang sistem hukumnya berdiri sendiri-sendiri dengan berbagai otoritas dan Konstitusi Federal tidak diserahkan kepada organ-organ Federal. Antara pemerintahan negara bagian dengan pemerintah federal dalam hal terdapat beberapa bidang yang memiliki yuridiksi yang sama, maka hukum federal lah yang dianggap lebih kuat dari hukum negara bagian. Oleh karena itu 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*. Sistem hukum acara pidana di Amerika Serikat terdapat beberapa tahap proses penanganan perkara pidana dimulai dari penyidikan, penuntutan, pemeriksaan dalam sidang, penetapan hukuman dan pelaksanaan hukumannya.

Sistem pembuktian dalam perkara pidana di Amerika Serikat menganut sistem peradilan juri, yang mana mereka dari masyarakat sipil dan bukan dari praktisi hukum yang ditunjuk oleh negara pihak yang tidak memiliki hubungan terhadap terdakwa.Juri disini bertugas untuk menilai alat bukti yang di ajukan dan untuk menentukan bersalah atau tidaknya seorang terdakwa. Alat bukti tersebut sebelum masuk tahap perentasi harus di evaluasi terlebih dahulu oleh pengacara agar dapat diterima oleh hukum Amerika Serikat, bukti ilmiah harus lulus uji yang disebut dengan *daubert,*[58] yang berasal dari *A.S. Supreme* Keputusan pengadilan di *Daubert* vs *Merrell Dow Pharmaceuticals* (1993) [17]. Makalah ini akan membahas persyaratan Uji *Daubert.*[59] Agar analisa bukti elektronik dapat diterima di pengadilan Amerika Serikat, bukti harus relevan dan dapat diandalkan. Kenadalan bukti ilmiah dari digital forensik ditentukan oleh hakim. Seperti yang dijelaskan dalam jurnal internasional yang berjudul *Open Source Digital Forensics Tools* sebagai berikut:[60]

---

[58]Daubert adalah sebuat standart yang ditetapkan di sebuah negara, di amerika pengertian 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.

[59] Brian Carrier, **Open Source Digital Forensics Tools**, http://www.digital-evidence.org/papers/opensrc_legal.pdf, diakses pada 17 mei 2017

[60] *ibid*

To be admissible in a United States court, evidence must be both relevant and reliable.
The reliability of scientific evidence, such as the output from a digital forensics tool, is determined by the judge (as opposed to a jury) in a pre-trial "Daubert Hearing". The judge's responsibility in the Daubert Hearing is to determine whether the underlying methodology and technique used to identify the evidence was sound, and whether as a result, the evidence is reliable. The Daubert process identifies four general categories that are used as guidelines when assessing a procedure:
*- **Testing:** Can and has the procedure been tested?s*
*- **Error Rate:** Is there a known error rate of the procedure?*
*- **Publication:** Has the procedure been published and subject to peer review?*
*- **Acceptance:** Is the procedure generally accepted in the relevant scientific*
community?
The Daubert Test is an expansion of the Court's prior approach to the admissibility of scientific evidence. Previously, under the "Frye Test", courts placed responsibility of identifying acceptable procedures on the scientific community using peer-reviewed journals. However, as not every field has peer-reviewed journals, the Daubert Test offered additional methods of testing the quality of evidence.
Each guideline will now be addressed in more detail with respect to digital forensics. The guidelines will be examined for both data acquisition tools and analysis tools. Currently, the majority of digital forensics involves the acquisition of hard disks and analysis of file systems.

Yang artinya:
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:
- Pengujian: Bisa dan prosedurnya sudah teruji?

> - Error Rate: Apakah ada tingkat kesalahan prosedur yang diketahui?
> - Publikasi: Apakah prosedur telah dipublikasikan dan tunduk pada peer review?
> - Penerimaan: Apakah prosedurnya berlaku umum di bidang ilmiah yang relevan
> masyarakat?
> 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.

Di dalam *Federal Rule of Evidence* data *daubert* diatur dalam *Rule* 901(b)(9)[4] yang menggambarkan bahwa suatu proses dapat diatutentikasi dengan bukti yang menjelaskan proses atau sistem yang digunakan untuk menghasilkan suatu hasil dan menunjukan bahwa proses atau sistem menghasilkan hasil yang akurat.[61]

2. 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

[61] *Ibid*, hlm 7

untuk menentukan kualitas bukti dengan mengguankan forensik digital. Adapun prosedurnya sebagai berikut :[62]

1. Testing

Adalah sebuah pedoman untuk menguji dan mengidentifikasi suatu prosedur untuk memperoleh hasil yang akurat, ada dua kategori testing yang harus dilakukan pada alat output yaitu:

a. False Negatives

Tujuannya untuk memastikan bahwa alat tersebut menyediakan semua data yang tersedia dari input. Sebagai contoh, ketika sebuah alat mencantumkan isi sebuah direktori maka semua file harus ditampilkan. Demikian pula, jika alat ini mampu menampilkan nama file yang dihapus, semua nama yang dihapus harus ditampilkan. Alat akuisisi harus menyalin semua data ke tujuan. Dengan alat forensik digital, kategori ini adalah yang paling mudah untuk diuji dan pengujian yang paling formal adalah tipe ini. Data yang diketahui ditanam pada sistem, diperoleh, dianalisis, dan diverifikasi bahwa data dapat ditemukan.

b. False Negatives

Untuk memastikan bahwa alat tersebut tidak memasukan data baru pada hasil. Sebagai contoh, ketika sebuah alat mencantumkan isi sebuah direktori maka file tersebut tidak menambahkan nama file baru. Kategori ini lebih sulit untuk diuji. Teknik yang umum digunakan untuk memverifikasi

[62] *Opcid,* hlm. 5

bahwa alat yang tidak mengenalkan data adalah memvalidasi hasilnya dengan alat kedua.

2. Error Rates

Error rate diartikan sebagai tingkat kesalahan yaitu pedoman untuk mengidentifikasi tingkat kesalahan yang diketahui dari prosedur. Alat forensik digital memproses data melalui serangkaian aturan. Error rater juga seperti tes ilmiah pada umumnya seperti halnya tes DNA atau tes sidik jari yang mempunyai tingkat kesalahan yang didasarkan pada bagaimana pengujian dilakukan. Untuk menghitung tingkat kesalahan pertama-tama kita harus mengembangkan metodologi pengujian yang dibutuhkan oleh pedoman pertama. Alat open source (atau closed source / documented design) memungkinkan metodologi pengujian dibuat lebih mudah. Selain itu, jauh lebih sulit untuk aplikasi open source untuk menyembunyikan asal kesalahan dan kerusakan.

3. Publikasi

Publikasi adalah prosedur yang dilakukan untuk menampilkan hasil dari proses forensic digital agar penyidik dapat mengidentifikasi bagaimana prosedur di lakukan. Pedoman publikasi sangat penting dan salah satu yang paling kurang dalam analisis forensik digital. Sedikit yang telah diterbitkan tentang pemulihan file yang dihapus dan analisis sistem berkas. Minimal, alat tertutup harus mempublikasikan spesifikasi desain yang mendokumentasikan prosedur dan rincian analisis mereka. Alat sumber terbuka mengungkapkan semua prosedur mereka melalui sumber kode dan memungkinkan seseorang

untuk memverifikasi bahwa alat tersebut memang mengikuti proses penerbitan dan tidak hanya menerbitkan minimum yang diperlukan. Selain itu, alat sumber terbuka harus mempublikasikan rincian prosedural dalam bahasa selain

4. Acceptance

Pedoman penerimaan adalah kerangka kerja bagi komunitas ilmuwan terkait untuk mengevaluasi prosedur yang diterbitkan. Agar pedoman ini dapat dinilai, prosedur yang diterbitkan diperlukan. Alat sumber tertutup sebelumnya telah menanggapi pedoman ini dengan mengutip sejumlah besar pengguna yang mereka miliki. Penerimaan alat berbeda dari penerimaan prosedur. Jika ada beberapa pilihan alat yang melakukan prosedur dan tidak ada satupun yang mempublikasikan rincian prosedur atau kekurangan utama, maka pilihan pilihan kemungkinan didasarkan pada faktor non-prosedural seperti antarmuka dan dukungan. Sampai rincian prosedural dipublikasikan dan menjadi faktor saat membeli alat analisis forensik digital, ukuran komunitas pengguna bukanlah ukuran penerimaan prosedural yang valid. Alat sumber terbuka mendokumentasikan prosedur yang mereka gunakan dengan menyediakan kode sumber, sehingga memungkinkan masyarakat untuk menerima atau menolaknya.

3. 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 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),* antara lain yaitu*:*

> *Article X. Contents Of Writings, Recordings, And Photographs*
> *Rule 1001. Definitions That Apply to This Article In this article:*
>
> *(a) A "writing" consists of letters, words, numbers, or their equivalent set down in any form.*
>
> *(b) A "recording" consists of letters, words, numbers, or their equivalent recorded in any manner.*
>
> *(c) A "photograph" means a photographic image or its equivalent stored in any form.*
>
> *(d) An "original" of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, "original" means any printout — or other output readable by sight — if it accurately reflects the information. An "original" of a photograph includes the negative or a print from it.*
>
> *(e) A "duplicate" means a counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent process or technique that accurately reproduces the original.*

Yang artinya:

> 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 seterusnya 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 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 yang secara akurat mereproduksi yang asli.

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*

Wire communication adalah komunikasi nirkabel yang artinya transfer aural yang dilakukan secara keseluruhan atau sebagian melalui penggunaan fasilitas untuk transmisi komunikasi dengan bantuan nirkabel, kabel, atau sambungan sejenis lainnya antara titik asal dan titik penerimaan (Termasuk penggunaan koneksi semacam itu di stasiun *switching*) yang dilengkapi atau dioperasikan oleh siapa saja yang terlibat dalam penyediaan atau pengoperasian fasilitas semacam itu untuk transmisi komunikasi atau komunikasi antarnegara bagian atau asing yang mempengaruhi perdagangan antarnegara atau luar negeri.

1. *Wire And Electronic Communications Interception And Interception Of Oral Communications* mengatur mengenai :[63]

    1) Intersepsi dan pengungkapan komunikasi nirkabel, lisan, atau elektronik dilarang
    2) Pembuatan, pendistribusian, kepemilikan, dan periklanan alat penyadapan komunikasi kabel, lisan, atau elektronik dilarang
    3) Penyitaan perangkat interepsi, komunikasi lisan, atau komunikasi elektronik
    4) Larangan penggunaan sebagai bukti kawat yang disadap atau komunikasi lisan
    5) Otorisasi untuk intersepsi komunikasi kawat, lisan, atau elektronik
    6) Otorisasi untuk pengungkapan dan penggunaan kabel yang disadap, komunikasi lisan atau elektronik
    7) Prosedur untuk intersepsi komunikasi kawat, lisan, atau elektronik
    8) Laporan tentang komunikasi kawat, komunikasi lisan, atau elektronik yang disadap
    9) Pemulihan kerusakan sipil yang diotorisasi
    10) Tindakan melawan intersepsi ilegal
    11) Penegakan Bantuan Komunikasi untuk Penegakan Hukum

2. *Pen Registers and Trap and Trace Devices* mengatur mengenai:[64]

    1) Larangan umum pendaftar dan perangkap dan penggunaan perangkat; pengecualian

[63] *18 U.S.Code Chapter 119 Rule 2510-22*
[64] *18 U.S.Code Chapter 206*

2) Aplikasi untuk pemesanan register pena atau perangkap dan perangkat jejak
3) Penerbitan pesanan untuk register pena atau perangkap dan perangkat jejak
4) Bantuan dalam pemasangan dan penggunaan register pena atau perangkat perangkap dan jejak
5) Register register darurat dan perangkap dan peranti penginstalan
6) Laporan tentang register pena dan perangkat perangkap dan jejak

3. *Stored Wire And Electronic Communications And Transactional Records Access* mengatur mengenai:[65]

1) Akses yang tidak sah ke komunikasi yang tersimpan
2) Pengungkapan komunikasi pelanggan secara sukarela atau catatan
3) Diperlukan pengungkapan komunikasi pelanggan atau catatan
4) Pelestarian cadangan
5) Pemberitahuan tertunda
6) Penggantian biaya
7) Tindakan sipil
8) Eksklusivitas pengobatan
9) Akses kontraintelijen ke pulsa telepon dan catatan transaksional
10) Salah pengungkapan rekaman video tape atau catatan penjualan
11) Definisi untuk bab

[65] *18 U.S.Code Chapter 121 Rule 2701-120)*

12) Tindakan sipil melawan Amerika Serikat

Menurut Mohammed Chawki dari Computer Research Center mengklasifikasi bukti elektronik menjadi tiga kategori, yaitu:[66]

1. *Real Evidence atau Physical Evidence*

   Real evidence merupakan bukti nyata yang berupa sesuatu yang berwujud dan bisa di sentuh. *Real evidence* di dalam bukti elektronik dapat berupa file, dokumen atau rekaman yang tersimpan di dalam komputer.

2. *Testamentary evidence*

   Alat bukti ynag berupa keterangna saksi maupun ahli yang diberikan selama persidangan, berdasarkan apa yang dialami dan berdasarkan pengamatan masing-masing. Kedudukan para ahli sedikit banyak mempengaruhi keyakinan hakim dalam memberi putusan karena dapat memperjelas bukti elektronik.

3. *Circumstantial evidence*

   Bukti yang diperoleh dari pengamatan dan kejadian sebenarnya untuk mendorong suatu kesimpulan dan merupakan percampuran dari real evidence dan hearsay evidence.

Berdasarkan uraian di atas *Federal Rule Of Evidenve Article IX* juga menyebutkan tentang barang bukti bahwa :

Rule 901. Authenticating or Identifying Evidence

> *"(a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is".*

[66] *Ibid*, hlm.126

Yang artinya :

(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.

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	Federal Rule of Evidence 2015 Pasal X. Isi dari tulisan, rekaman, dan foto Untuk alat bukti berupa tulisan, rekaman dan

		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 b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.	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 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

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

1. Pengaturan Pembuktian Tindak Pidana di Indonesia

Menurut **Sudikno Mertokusumo,** membuktikan mempunyai beberapa pengertian, yaitu arti logis, konvensional, dan yuridis.[67]Dalam konteks ini pembuktian dalam hukum pidana adalah inti persidangan jadi harus memberikkan kepastian yang nantinya bisa diterima masyarakat.Pembuktain ialah ketentuan yang membatasi sidang pengadilan dalam usaha mencari dan mempertahankan kebenaran, baik oleh hakim, penuntut umum, terdakwa maupun penasihat hukum, yang sudah tercantum dalam undang-undang.[68]

Di dalam suatu sistem peradilan pidana, setelah melalui proses penyelidikan, penyidikan dan penuntutan, akan tiba pada proses yang selanjutnya akan masuk pada proses persidangan yang mana sebagai inti dari rangkaian pemeriksaan perkara di sidang pengadilacertn. Pemeriksaan persidangan ini hasil penyidikan yang berbentuk surat dakwaan di tingkat penuntutan akan diuji untuk memperoleh kebenaran materiil. Inti proses

[67] Eddy O.S**, Teori Dan Hukum Pembuktian, Yogyakarta**, 2012, hlm 6
[68] *Opcit* hlm 7

pemeriksaan persidangan adalah pembuktian, dimana alat bukti tersebut akan di nilai oleh majelis hakim untuk memperoleh kesimpulan, apakah terdakwa bersalah atau tidak bersalah melakukan tindak pidana sebagaimana didakwakan oleh penuntut umum.[69]

Pembuktian adalah ketentuan-ketentuan yang berisi pedoman tentang cara-cara yang dibenarkan undang-undang untuk membuktikan kesalahan yang di dakwakan kepada terdakwa. Pembuktian merupakan ketentuan yang mengatur mengenai alat-alat bukti yang dibenarkan undang-undang dan boleh dipergunakan hakim untuk membuktikan kesalahan terdakwa.[70] Oleh sebab itu pembuktian merupakan proses untuk mengolah alat bukti dan menggunakannya sesuai undang-undang yang berlaku.

Sistem atau teori pembuktian yang dianut Indonesia adalah teori pembuktian berdasarkan undang-undang secara negative yaitu keyakinan hakim yang didasarkan pada undang-undang. Undang-Undang secara negatif artinya bahwa walaupun dalam suatu perkara terdapat cukup bukti sesuai dengan undang-undang, akan tetapi hakim belum boleh menjatuhkan hukuman, sebelum yakin akan kesalahan terdakwa. Alat bukti yang sah menurut pasal 184 KUHAP adalah Keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Dalam kasus *cyber crime*, proses penegakan hukum tidak dapat dilepaskan begitu saja dengan alasan pada proses pembuktian mengalami kendala dan kesulitan. Apalagi jika perbuatan *cyber crime* tersebut telah dapat dikenakan delik-delik konvensional yang ketentuannya jelas dan tegas.Upaya yang dapat

---

[69] Tolib Effendi, **Dasar Dasar Hukum Acara Pidana**, Setara Press, Surabaya, 2014,hlm 150

[70] *Ibid.*

ditempuh adalah penelusuran bukti-bukti yang berkaitan dengan perbuatan pelaku *cyber crime* dengan tetap mengacu pada undang-undang yang berlaku. Artinya, bahwa tetap menggunakan alat-alat bukti berupa keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Minimalnya, kesalahan pelaku dapat terbukti dengan sekurang-kurangnya 2 (dua) alat bukti yang sah.Alat-alat bukti ini harus mampu membuktikan telah terjadi suatu perbuatan dan membuktikan adanya akibat dari perbuatan *cyber crime*.

Berdasarkan uraian tersebut di atas dapat dianalisis bahwa cara yang harus ditempuh oleh pihak kepolisian dan Kejaksaan apabila terjadi suatu tindak pidana *cyber crime* adalah melakukan investigasi kasus untuk mengumpulkan alat bukti, bisa juga dengan cara mencari alamat ip address web terlebih dahulu dan mencari bukti elektronik yang bersangkutan. Karena ip address web adalah bukti pertama yang kuat didalam pengungkapan kasus tindak pidana siber *(cybercrime)*. Secara umum pembuktian mengenai *cybercrime* di Indonesia di atur dalam pasal 5 dan 6 Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Pasal 5

(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

> b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta
>
> **Pasal 6**
>
> Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.[71]

Jadi selain alat bukti yang terdapat dalam KUHAP alat bukti elektronik juga termasuk alat bukti yang sah yang dapat dijadikan bahan pertimbangan di pengadilan. Alat-alat bukti ialah upaya pembuktian melalui alat-alat yang diperkenankan untuk dipakai membuktikan dalil-dalil atau dalam perkara pidana dakwaan di sidang pengadilan.[72]Alat-alat bukti didalam KUHAP dipergunakan untuk memperkuat dakwaan, gugatan atau tuntutan dan juga untuk melawan hal tersebut. Alat bukti adalah hal yang penting didalam pembuktian karena berfungsi sebagai pemberi kepastian tentang suatu kebenaran. Dalam tindak pidana tradisional alat bukti fisik memegang peranan penting untuk mengungkap terjadinya tindak pidana berdasarkan fakta hukum yang ada. Alat bukti hukum pidana diatur dalam Pasal 184 KUHAP yang terdiri dari keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Di dalam KUHAP tidak dicantumkan mengenai alat bukti elektronik, sehingga tidak bisa diketahui pembuktian kasus tindak pidana elektronik menggunakan alat bukti seperti apa, apa termasuk dalam alat bukti surat atau petunjuk, karena yang kita ketahui alat bukti elektronik adalah surat

---

[71]Pasal 5 dan 6 Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

[72] Bambang Waluyo, **Sistem Pembuktian Dalam Peradilan Indonesia**, Sinar Grafika, Jakarta, 1991, hlm. 2

atau tulisan dalam bentuk digital, sehingga untuk mengetahuinya dibutuhkan undang-undang yang mengatur secara khusus mengenai alat bukti dalam kasus *cybercrime.*

Alat-alat bukti elektronik yang berupa *software*, data *elektronik*, sebelum adanya undang-undang tentang Informasi dan Transaksi Elektronik belum dapat diterima sebagai alat bukti yang sah .Sementara berdasarkan Pasal 28 Ayat (1) Undang-Undang Republik Indonesia Nomor 4 Tahun 2004 tentang Kekuasaan Kehakiman, hakim wajib menggali, mengikuti, dan memahami nilai-nilai hukum dan rasa keadilan yang hidup dalam masyarakat. Dengan demikian, maka hakim diwajibkan untuk memahami nilai-nilai hukum dan rasa keadilan yang hidup dalam masyarakat, oleh karena itu menyangkut juga eksistensi alat bukti elektronik dalam menjalankan praktik pembuktian tindak pidana siber (*cybercrime)*.Sehingga alat bukti elektronik harus diakui keberadaannya dan kekuatan hukumnya.[73]

Dalam tindak pidana siber (*cybercrime)* yang dilakukan dengan menggunakan komputer atau teknologi informasi dan komunikasi menempatkan peran alat bukti baru, yaitu alat bukti digital atau alat bukti elektronik disamping alat-alat bukti yang sudah diatur dalam Pasal 184 KUHAP, alat bukti elektronik inilah yang memegang peran penting dalam melakukan pembuktian tindak pidana siber (*cybercrime)*

[73]Sahuri Lasmadi, **Pengaturan Alat Bukti Dalam Tindak Pidana Dunia Maya**, Jurnal Imu Hukum, 2014, hlm. 2

2. Alternatif Pengaturan Untuk Pembuktian Tindak Pidana Siber *(cybercrime)* Di Indonesia

BAB I

KETENTUAN UMUM

Dalam undang-undang ini yang dimaksud dengan :

1. Tulisan adalah terdiri dari huruf, kata, angka, atau seterusnya yang setara dalam bentuk catatan atau informasi.
2. Foto adalah gambar fotografis baik berwarna maupun hitam putih yang menunjukan suaku kejadian atau keaadaan pada suatu waktu.
3. Rekaman adalah alat penyimpanan yang menyimpan objek baik berupa foto, grafik, angka, maupun tulisan, yang berada di dalam komputer atau di luar komputer.
4. Asli adalah hasil cetakan - atau masih berupa rekaman file komputer yang dapat dibaca oleh penglihatan dan benar-benar mencerminkanInformasi sesuai dengan yang dibutuhkan.
5. Duplikat adalah objek yang diproduksi oleh mekanik, fotografi, kimia, elektronik, atau proses atau teknik setara lainnya yang secara akurat mereproduksi sesuai dengan yang asli.

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.

PENJELASAN

Pasal …

Tata Cara Pembuktian

(1) Yang dimaksud dengan rekaman yaitu berisi angka, atau catatan informasi yang tersimpan secara elektronik.

(2) Yang dimaksud "asli" dari suatu tulisan atau rekaman berarti penulisan atau rekaman itu sendiri.

(3) Yang dimaksud duplikat dengan syarat tertentu yaitu yang dapat diterima untuk dijadikan alat bukti adalah duplikat dapat diterima sampai batas tertentu seperti aslinya kecuali jika ada pertanyaan asli yang diajukan mengenai hal itu. Keaslian asli atau keadaan membuatnya tidak adil untuk mengakui duplikatnya. Hal ini berarti alat bukti yang diduplikat kejaksaan agar dapat diterima maka benar-benar dipastikan diduplikat dari yang asli dengan pemberian batas waktu tertentu, pemberian batas waktu tertentu kemudian diharapkan agar dapat menjamin keorisinalitasan alat bukti dan mendukung peradilan cepat, sederhana dan biaya ringan untuk kemudian dimasukkan pada proses peradilan.

(4) Yang dimaksud lembaga yang berwenang adalah Penyidik dapat menggunakan salinan untuk membuktikan isi file resmi - atau dokumen yang ada. Dicatat atau diajukan di kantor publik yang diberi wewenang oleh undang-undang - jika persyaratan ini terpenuhi: catatan atau dokumen. Jika tidak bisa diterima; Dan salinannya telah disertifikasi sebagaimana mestinya sesuai dengan Peraturan 902 (4) atauBersaksi akan benar oleh saksi yang telah membandingkannya dengan yang asli. Jika tidak ada salinan tersebut dapat diperolehDengan ketekunan yang wajar, maka pemrakarsa dapat menggunakan bukti lain untuk membuktikan isinya.

(5) Penyidik harus membuat dokumen asli atau salinanyang tersedia untuk pemeriksaan atau penyalinan, atau keduanya, oleh pihak lain pada waktu dan tempat yang bisa diterima. Dan pengadilan dapat memerintahkan pemrakarsa untuk memproduksinya di pengadilan. (untuk membuktikan kebenaran tulisan-tulisan, fotografi dan rekaman penyidik harus membuktian dengan ringkasan, grafik, atau perhitungan.

(6) Yang dimaksud faktual adalah tulisan, rekaman, atau foto yang ditegaskan yang pernah adayang lain diproduksi di persidangan atau pendengaran adalah sesuai dengan yang asli; atau bukti konten lainnya secara akurat mencerminkan isinya. Di dalam pengadilan untuk menentukan apakah pemrakarsa membuktikan apakah alat bukti dari isi tulisan, rekaman, atau foto tersebut asli hakim menentukan sesuai dengan undang-undang bahwa:Tulisan, rekaman, atau foto yang ditampilkan di persidangan adalah asli dan pernah ada bukti adalah secara akurat mencerminkan isinya.Tulisan, rekaman, atau foto yang ditegaskan yang pernah ada. Yang lain diproduksi di persidangan atau pendengaran adalah sesuai dengan yang asli; atau bukti konten lainnya secara akurat mencerminkan isinya.

Hal tersebut dapat menjadi acuan bagi aparat penegak hukum untuk mempergunakan UU ITE tentunya dalam mengambil upaya penegakan hukum sehingga dapat memenuhi kepastian hukum untuk tindak pidana siber (*cybercrime*) karena tidak menutup kemungkinan akan ditemui isu hukum yang memerlukan penanganan secara khusus terkait tindak pidana siber di masa mendatang.