BAB IV

HASIL PENELITIAN DAN ANALISIS

A. Penentuan Keabsahan Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana *Cybercrime*

Pembuktian Tindak Pidana *Cybercrime* memegang peranan yang penting dalam proses pemeriksaan sidang pengadilan. Pembuktian inilah yang menentukan bersalah atau tidaknya seseorang yang diajukan di muka pengadilan. Proses pembuktian pada tindak pidana *cybercrime* pada dasarnya tidak berbeda dengan pembuktian pada tindak pidana yang lain, hanya saja digunakannya alat bukti elektronik menjadi hal utama dalam pembuktian tindak pidana *cybercrime*. Sehingga agar alat bukti elektronik dapat membuktikan suatu tindak pidana *cybercrime*, pengupayaan keabsahan alat bukti elektronik juga menjadi hal yang penting dan pokok.

Pengupayaan keabsahan alat bukti elektronik menjadi hal yang penting dikarenakan meningkatnya khasus *cybercrime* tiap tahunya dan berkembangnya modus operandi dari tindak pidana ini memerlukan penanganan yang serius terhadap penegakan hukumnya dan pembuktiannya.

Berdasarkan data dari Rekapitulasi Laporan Polisi akan Tindak Pidana *Cybercrime* yang disidik DIRESKRIMSUS POLDA DIY pada tahun 2016 masih meningkat dan justru mengalami peningkatan modus operandinya.

TABEL II

REKAPITULASI LAPORAN POLISI TINDAK PIDANA *CYBERCRIME* YANG DILIDIK/ DISIDIK DIREKRIMSUS POLDA DIY PADA TAHUN 2016

No	Jenis Tindak Pidana *Cybercrime*	Jumlah	Bulan		Keterangan
			Januari	Febuari	
1.	Penipuan/ Beli barang Online melalui Toko Online, BBM, Website	45 LP	29 LP	16 LP	LP menurun sebanyak 13 LP
2.	Penipuan tawaran beasiswa melalui internet	-	-	-	Tidak ada LP
3.	Penipuan melalui telepon bahwa anak/keluarga/teman terkena musibah/ disandera/ membutuhkan bantuan dan meminta uang/pulsa	7 LP	2 LP	5 LP	LP meningkat sebanyak 3 LP
3.	Penipuan SMS/ Telepon mendapat hadiah	2 LP	1 LP	1 LP	Tidak ada peningkatan maupun penurunan
5.	Penipuan SMS tawaran lelang barang	-	-	-	Tidak ada LP
6.	Penipuan tawaran lowongan pekerjaan melalui internet	3 LP	1 LP	2 LP	Terdapat peningkatan 1 LP

7.	Penipuan tawaran investasi melalui media sosial	4 LP	3 LP	1 LP	Terdapat penurunan 2 LP
8.	Pencurian saldo modus ATM tertelan/ ATM tidak bisa masuk	1 LP	-	1 LP	Terdapat LP yang sebelumnya tidak ada
9.	Pencurian melalui internet banking	-	-	-	Tidak ada LP
10.	Pencemaran nama baik melalui facebook, BBM, dan sosial media lainnya	12 LP	5 LP	7 LP	Terjadi peningkatan 2 LP
11.	Pencemaran nama baik/ penghinaan melalui SMS	2 LP	-	2 LP	Terdapat LP yang sebelumnya tidak ada
12.	Pornografi/ Asusila melalui facebook, BBM, dan sosial media lainnnya	-	-	-	Tidak ada LP
13.	Menggunakan webs orang lain tanpa ijin	-	-	-	Tidak Ada LP
JUMLAH		76 LP	41 LP	35 LP	-

Sumber: *Laporan Polisi Tindak Pidana Cybercrime yang Dilidik/ Disidik DIREKRIMSUS POLDA DIY pada Tahun 2016 pada 5 Januari 2017*

Dari data tersebut, tindak pidana *cybercrime* dalam bentuk Penipuan online sangat banyak yakni sebanyak 62 Laporan Polisi yang bermodus berbeda-beda, setelah itu tindak pidana yang banyak setelah penipuan *online* adalah Pencemaran nama baik lewat media sosial yakni sebanyak 14 Laporan Polisi. Hal ini menunjukan bahwa bentuk dan jenis tindak pidana *cybercrime* di Yogyakrta yang berkembang adalah Tindak Pidana *Cyberrime* dalam bentuk penipuan melalui lewat media sosial.

TABEL III

DATA TINDAK PIDANA PELANGGARAN UU ITE TAHUN 2013-2016

DITRESKRIMSUS POLDA DIY

NO	JENIS	TAHUN								KET
		2013		2014		2015		2016		
		L	S	L	S	L	S	L	S	
1	Penipuan Online	244	9	209	163	204	4	202	4	-
2	Pornografi Online	5	4	6	1	2	-	12	5	-
3	Pembobolan Account	17	-	7	1	22	1	4	1	-
4	Pencemaran Nama Baik	15	12	24	5	35	10	12	1	--
5	Pencurian Online	1	1	3	1	3	1	4	1	-

6	Pemerasaan/ Pengancaman Online	-	-	1	1	5	-	1	-	-
7	SARA/ITE	-	-	1	-	1	-	2	-	-
JUMLAH		**282**	**26**	**251**	**172**	**272**	**16**	**237**	**12**	**-**

Sumber: *Laporan Polisi Tindak Pidana Cybercrime yang Dilidik/ Disidik DIREKRIMSUS POLDA DIY pada Tahun 2013-2016*

Berdasarkan dari tabel diatas dapat diketahui bahwa adanya sejumlah dari tindak pidana *cybercrime* sejak tahun 2013 hingga tahun 2016. Perkara yang diindikasi sebagai tindak pidana *cybercrime* dari tahun ke tahun telah mengalami perubahan yang cukup signifikan. Namun pada tabel tersebut terdapat kolom yang menjelaskan penyelesaian kasus tersebut, telah selesai sampai proses peradilan. Dapat diketahui dalam tabel proses selesai terdapat data yang tidak berimbang, dimana tidak semua tindak pidana *cybercrime* yang dilaporkan terjadi tidak selesai sampai proses pengadilan. Menurut Wawancara dengan Bripkan Dion Agung, S. H penyidik pada direskrimsus Polda DIY, tidak terselesaikannya kasus karena laporan sudah dicabut, dan alat bukti tidak cukup membuktikan unsur pidana. Penyidik akan mencari pemenuhan unsur pidana berdasarkan alat-alat bukti yang diatur dalam perundang-undangan. Dari data diatas kurangnya alat-alat bukti menyebabkan hanya sedikit laporan yang selesai diproses. Sehingga penggunaan alat bukti elektronik sangat dibutuhkan dalam proses pembuktian tindak pidana

cybercrime hal ini jika tidak diperhatikan kasus akan semakin banyak dan meningkat.[1]

Peningkatan tindak pidana *cybercrime* tersebut juga berimpikasi pada peningkatan jumlah alat bukti elektronik. Hal ini dikarenakan Objek atau sarana prasarana yang digunakan dalam tindak pidana *cybercrime* menggunakan barang barang elektronik, dan hampir semua menggunakan alat bukti elektronik, sehingga penanganan dan bentuknya atau ragamnya berbeda-beda dari alat bukti elektronik yang satu dengan yang lain dikarenakan berkembangnya globalisasi dan bertambahnya jumlah sesuai tindak pidana yang dilakukanya.[2] Sehingga diperlukannya pengklasifikasian barang bukti elektronik tersebut. Klasifikasi barang bukti elektronik pada laboratorium forensic terbagi atas:

1. Barang Bukti Elektronik

   Barang bukti ini bersifat fisik dan dapat dikenali secara visual, oleh karena itu penyidik dan pemeriksa harus sudah memahami untuk kemudian dapat mengenali masing-masing barang bukti elekronik ini ketika sedang melakukan proses pencarian barang bukti di tempat kejadian perkara. Jenis-jenis barang bukti elektronik adalah sebagai berikut:

   a. *Personal Computer*, laptop/*notebook*, *netbook* dan tablet;

   b. *Handphone* dan *smartphone*;

[1] Wawancara Bripka Dion Agung, Penyidik pada Direskrimsus POLDA DIY, pada hari Kamis, 5 Januari 2017, pukul 11.32 WIB

[2] Wawancara Bapak M. Ismet Karnawa, Jaksa Penuntut Umum pada Kejaksaan Negeri Sleman, pada hari Selasa, 17 Januari 2017, pukul 11. 30 WIB

c. *Flashdisk/thumb drive*;

d. *Harddisk*;

e. *Compact Disk/DVD*;

f. *Rauter, Switch, hub*;

g. Kamera Video dan cctv;

h. Kamera digital;

i. Digital *recorder;*

j. Music/Video *player.*

k. Kamera

l. Memory *Card*

m. Sim *Card*

2. Informasi elektronik atau dokumen elektronik

Barang bukti ini bersifat digital yang di dapat dari barang bukti elektronik. Jenis barang bukti inilah yang harus dicari oleh pemeriksaan laboratorium forensic untuk kemudian dianalisis secara teliti keterkaitan masing-masing *file* (berkas data) dalam rangka mengungkap tindak pidana yang berkaitan dengan barang bukti elektronik. Berikut adalah jenis-jenis informasi elektronik, adalah sebagai berikut:

a. *Logical file*, yaitu *file-file* yang masih ada dan tercatat di *file system* yang sedang berjalan (*running*) di suatu partisi. *File-file* tersebut bias berupa *file-file* aplikasi, *library*, *office*, *logs*, multimedia dan lain-lain.

b. *Deleted file*, dikenal juga dengan istilah *unallocated cluster* yang merujuk pada *cluster* dan sektor tempat penyimpanan *file* yang sudah terhapus dan tidak teralokasikan lagi untuk *file* tersebut dengan ditandai dalam *file system* sebagai area yang dapat digunakan lagi untuk penyimpanan *file-file* baru. Artinya *file* yang sudah terhapus tersebut masih tetap berada di *cluster* atau sektor tempat penyimpanannya sampai tertimpa (*overwritten*) oleh *file-file* yang baru pada *cluster* atau sektor tersebut. Pada kondisi dimana *deleted file* tersebut belum tertimpa, maka proses *recovery* secara utuh terhadap *file* tersebut sangat memungkinkan terjadi.

c. *Lost file*, yaitu *file* yang sudah tidak tercatat lagi di *file system* yang sedang berjalan (*running*) dari suatu partisi, namun *file* tersebut masih ada di sektor penyimpanannya. Ini bisa terjadi ketika misalnya suatu *flashdisk* atau *harddisk* maupun partisinya dilakukan proses re-*format* yang menghasilkan *file system* yang baru, sehingga *file-file* yang sudah ada sebelumnya menjadi tidak tercatat lagi di *file system* yang baru. Untuk proses *recovery*-nya didasarkan pada *signature* dari *header* maupun *footer* yang tergantung pada jenis format *file* tersebut.

d. *File slack*, yaitu sektor penyimpanan yang berada di antara *End of File* (EoF) dengan *End of Cluster* (EoC). Wilayah ini

sangat memungkinkan terdapat informasi yang mungkin penting dari *file-file* yang sebelumnya sudah dihapus (*deleted*).

e. *Log file*, yaitu *file-file* yang merekam aktivitas (*logging*) dari suatu keadaan tertentu, misalnya *log* dari sistem operasi, *internet browser*, aplikasi, *internet traffic* dan lain-lain.

f. *Encrypted file*, yaitu *file* yang isinya sudah dilakukan enkripsi dengan menggunakan algoritma kriptografi yang kompleks, sehingga tidak bisa dibaca atau dilihat secara normal. Satu-satunya cara untuk membaca atau melihatnya kembali adalah dengan melakukan dekripsi terhadap *file* tersebut menggunakan algoritma yang sama. Ini biasa digunakan dalam dunia *digital information security* untuk mengamankan informasi yang penting. Ini juga merupakan salah satu bentuk dari *anti-forensic*, yaitu suatu metode untuk mempersulit analis forensik atau investigator mendapatkan informasi mengenai jejak-jejak kejahatan.

g. *Steganography file*, yaitu *file* yang berisikan informasi rahasia yang disisipkan ke *file* lain, biasanya berbentuk file gambar, video atau audio, sehingga *file-file* yang bersifat *carrier* (pembawa pesan rahasia) tersebut terlihat normal dan wajar bagi orang lain, namun bagi orang yang tahu

metodologinya, *file-file* tersebut memiliki makna yang dalam dari informasi rahasianya tersebut. Ini juga dianggap sebagai salah satu bentuk *anti-forensic*.

h. *Office file*, yaitu *file-file* yang merupakan produk dari aplikasi *Office*, seperti *Microsoft Office*, *Open Office* dan sebagainya. Ini biasanya berbentuk *file-file* dokumen, *spreadsheet*, *database*, teks dan presentasi.

i. *Audio file*, yaitu *file* yang berisikan suara, musik dan lain-lain, yang biasanya berformat wav, mp3 dan sebagainya. *File* audio yang berisikan rekaman suara percakapan orang ini biasanya menjadi penting dalam investigasi ketika suara di dalam *file* audio tersebut perlu diperiksa dan di analisis secara *audio forensic* untuk memastikan suara tersebut apakah sama dengan suara pelaku kejahatan.

j. *Video file*, yaitu *file* yang memuat rekaman video, baik dari kamera digital, *handphone, handycam* maupun CCTV. *File* video ini sangat memungkinkan memuat wajah pelaku kejahatan sehingga *file* ini perlu dianalisis secara detail untuk memastikan bahwa yang ada di *file* tersebut adalah pelaku kejahatan.

k. *Image file*, yaitu *file* gambar digital yang sangat memungkinkan memuat informasi-informasi yang penting yang berkaitan dengan kamera dan waktu pembuatannya

(*time stamps*). Data-data ini dikenal dengan istial metadata exif (*exchangeable imege file*). Meskipun begitu, metadata exif ini bisa dimanipulasi, sehingga analis forensic atau investigator harus hati-hati ketika memeriksa dan menganalisis metadata dari *file* tersebut.

l. *E-mail* (*electronic mail*), yaitu surat berbasis sistem elektronik yang menggunakan sistem jaringan *online* untuk mengirimkannya atau menerimanya. *E-mail* menjadi penting di dalam investigasi khususnya *phishing* (yaitu, kejahatan yang menggunakan *e-mail* palsu dilengkapi dengan identitas palsu utnuk menipu si penerima). *E-mail* berisikan *header* yang memuat informasi penting jalur distribusi pengiriman email mulai dari pengirim (*sender*) sampai di penerima (*recipient*). Oleh karena itu, data di *header* inilah yang sering dianalisis secara teliti untuk memastikan lokasi si pengirim yang didasarkan pada alamat IP. Meskipun begitu, data-data di *header* juga sangat dimungkinkan untuk dimanipulasi. Dengan demikian pemeriksaan *header* dari *e-mail* harus dilakukan secara hati-hati dan komprehensif.

m. *User* ID dan *password*, merupakan syarat untuk masuk ke suatu *account* secara *online*. Jika salah satunya salah, maka akses untuk masuk ke *account* tersebut akan ditolak.

n. *Short Message Service* (SMS), yaitu layanan pengiriman dan penerimaan pesan pendek yang diberikan oleh operator seluler terhadap pelanggannya SMS-SMS yang bisa berupa SMS masuk (*inbox*), keluar (*sent*) dan rancangan (*draft*) dapat menjadi petunjuk dalam investigasi untuk mengetahui keterkaitan antara pelaku yang satu dengan yang lain.

o. *Multimedia Message Service* (MMS), merupakan jasa layanan yang diberikan oleh operator seluler berupa pengiriman dan penerimaan pesan multimedia yang bisa berbentuk suara, gambar atau video.

p. *Call logs*, yaitu catatan penggilan yang terekam pada suatu nomor panggil seluler. Panggilan ini bisa berupa *incoming* (panggilan masuk), *outgoing* (panggilan keluar) dan *missed* (panggilan tak terjawab).

Dengan diberlakukanya UU ITE maka terdapat suatu pengaturan yang baru mengenai alat-alat bukti elektronik. Berdasarkan ketentuan Pasal 5 ayat 1 UU ITE ditentukan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Selanjutnya di dalam Pasal 5 ayat 2 UU ITE ditentukan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan perluasan alat bukti yang sah dan sesuai dengan hukum acara yang berlaku di Indonesia. Dengan demikian, bahwa UU ITE telah menentukan bahwa alat bukti elektronik merupakan alat bukti yang sah

sesuai dengan hukum acara sehingga dapat digunakan sebagai alat bukti di muka persidangan.

Pembuktian tindak pidana *cybercrime* seperti yang telah dijelaskan sebelumnya tetap menganut sistem pembuktian negatif, yakni kesalahan terdakwa ditentukan oleh minimal dua alat bukti yang sah dan keyakinan hakim. Hanya saja alat bukti elektronik menjadi penting karena mengingat tindak pidana *cybercrime* untuk melakukan tindak pidana tentu bersingungan dengan elektronik. Sama halnya dengan persyaratan dan ketentuan alat bukti yang diatur dalam KUHAP, alat bukti elektronik harus memenuhi persyaratan baik secara formil dan materil sehingga alat bukti tersebut dinyatakan sah dan dapat dipergunakan di persidangan. Ketentuan dan persyaratan tersebut adalah untuk menjamin kepastian hukum dan berfungsi sebagai alat penguji dalam menentukan keabsahan alat bukti sehingga hakim dapat yakin dengan fakta-fakta hukum yang dihadirkan melalui alat bukti elektronik.

Keabsahan alat bukti didasarkan pada pemenuhan syarat dan ketentuan baik segi formil maupun materil. Prinsip ini juga berlaku terhadap pengumpulan dan penyajian alat bukti elektronik baik yang dalam bentuk original maupun hasil cetaknya, yang diperoleh baik melalui penyitaan maupun intersepsi. KUHAP telah memberikan pengaturan yang jelas mengenai upaya paksa penggledahan dan penyitaan secara umum, tetapi belum terhadap Sistem Elektronik. Akan terapi, hal ini diatur di dalam berbagai undang-undang yang lebih spesifik. Oleh karena itu,

ketentuan dan persyartan formil dan meteril mengenai alat bukti elektronik tersebut. Penelitian ini membatasi hanya kepada ketentuan dan persyaratan yang di atur dalam UU ITE saja.

Persyaratan materiil ialah ketentuan dan persyaratan untuk menjamin keutuhan data (*integrity*), ketersediaan (*availability*), keamanan (*security*), keotentikan (*authenticity*) dan keteraksesan (*accessbilty*) informasi dan dokumen elektronik dalam proses pengumpulan atau penyimanan dalam proses penyidikan dan penuntutan, serta penyampaiannya di sidang pengadilan. Karena itu menurut Josua Sitompul, dibutuhkan suatu cabang disiplin ilmu di bidang forensic komputer (*computer forensic*) atau forensic digital (*digital forensic*).[3]

Persyaratan materil alat bukti elektronik diatur dalam Pasal 5 ayat (3) UU ITE, yaitu informasi atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam UU ITE. Lebih lanjut, sistem elektronik diatur dalam Pasal 15 dan 16 UU ITE, yamh menyebutkan persyaratan yang lebih rinci, yaitu:

1. Andal, aman, dan bertanggungjawab.

   Penjelasan pasal 15 ayat (1) UU ITE menyatakan bahwa "andal" artinya sistem elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunaannya. "Aman" artinya sistem elektronik terlindungi secara fisik dan nonfisik,

[3] Josua Sitompul, *Op. Cit.*, hlm. 283

"Bertanggungjawab" artinya beroperasi sebagaimana mestinya maksudnya bahwa sistem elektronik memiliki kemampuan sesuai dengan spesifikasinya;

2. Dapat menampilkan kembali informasi atau dokumen secara utuh, utuh artinya tidak ada yang dihilangkan dan sesuai dengan pada awalnya.
3. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elketronik;
4. Dilengkapi dengan prosedur atau petunjuk dan dapat beroperasi sesuai prosedur atau petunjuk yang telah ditetapkan tersebut.[4]

Pasal 6 Undang-undang ITE juga memberikan persyartan materill mengenai keabsahan alat buti elektronik, yaitu bahwa informasi atau dokumen elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilakn, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Maksud nya adalah bahwa:

1. dapat diakses, yaitu data digital yang ditemukan dapat diakses oleh sistem elektronik;
2. dapat ditampilkan, yaitu data digital tersebut dapat ditampikan oleh sistem elektronik;
3. dijamin keutuhannya, yaitu bukti digital yang dihasilkan proses pemeriksaan dan analisis harus utuh isinya. Tidak hanya di

[4] Josua Sitompul, *Op. Cit.,* hlm 284

kedua proses tersebut, namun ketika suatu barang bukti elektronik diakses pertama kali untuk proses akuisisi yang menghasilkan *image file*, isi dari barang bukti elektronik dan *image file* tersebut harus utuh, tidak boleh berubah. Sekalipun ada perubahan selama proses digital forensik dan invesitagor harus bisa menjelaskan apa yang berubah, dan tindakan apa yang dilakukan hingga itu berubah, termasuk alasan teknisnya. Keutuhan barang bukti elektronik, *image file*, dan bukti digital dapat diukur dengan nilai *hash*, misalnya MD5 atau SHA1 yang diperoleh dari proses *hashing*. Disamping nilai *hash*, juga dibutuhkan adanya *time stamps* (*created* dan *modified date*) dari bukti digital untuk memastikan ada tidaknya modifikasi dan kapan pembuatannya pertama kali;

4. dapat dipertanggungjawabkan, yaitu apa yang dihasilkan mulai dari proses akuisisi hingga analisis di dalam kegiatan digital forensik dapat dipertanggungjawabkan, baik secara keilmiahnya, maupun secara hukum. Dapat dipertanggungjawabkan secara teknis keilmiahan artinya harus ada SOP yang disebutkan dalam laporan pemeriksaan yang memuat tahapan-tahapan yang dikerjakan sehingga ketika hasil yang ada di laporan tersebut dipertanyakan dan diuji ulang oleh pihak ketiga yang independen, seharusnya diperoleh hasil yang sama dengan menggunakan SOP yang sama. Dapat

dipertanggungjawabkan secara hukum artinya, harus jelas tingkat kompetensi dari analis forensik dan investigator yang melakukan kegiatan digital forensik tersebut, sehingga bukti digital yang diperoleh dapat dianggap sebagai informasi elektronik dan/atau dokumen elektronik yang nantinya dapat diterima di depan pengadilan.

Pada penjelasan Pasal 6 dinyatakan: "selama ini bentuk tertulis identik dengan informasi dan/atau dokumen yang tertuang di atas kertas semata, padahal pada hakikatnya informasi dan/atau dokumen dapat dituangkan ke dalam media apa saja, termasuk media elektronik". Dalam lingkup Sistem Elektronik, informasi yang asli dengan salinannya tidak relevan lagi untuk dibedakan sebab Sistem Elektronik pada dasarnya beroperasi dengan cara penggandaan yang mengakibatkan informasi yang asli tidak dapat dibedakan lagi dari salinannya.

Sedangkan persyaratan formil alat bukti elektronik diatur dalam Pasal 5 ayat (4) dan Pasal 43 Undangan-undangan No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu:

1. Informasi atau dokumen elektronik tersebut bukanlah:
    a. Surat yang menurut undang-undang harus dibuat dalam bentuk tertulis;
    b. Surat beserta dokumennya yang menurut undang-undnag harus dibuat dalam bentuk akata notaril atau akata yang dibuat oleh pejabat pembuat akta.

2. Penggeledahan atau penyitaan terhadap sistem elektronik harus dilakukan atas izin ketua pengadilan negeri setempat;
3. Penggeladahan atau penyitaan dalam angka (2) tetap menjaga terpeliharanya kepentingan pelayanan umum.

Apabila sistem elektronik yang digunakan telah memenuhi persyaratan tersebut, maka kualitas alat bukti elektronik dalam bentuk originalnya (informasi elektronik atau dokumen elektronik) dan hasil cetaknya dari informasi atau dokumen elektronik adalah bernilai sama. Dalam mencari serta menemukan informasi elektronik dan dokumen elektronik yang akan menjadi alat bukti elektronik diperlukan barang bukti elektronik, yang dalam hal proses penangannya memerlukan syarat formil dan syarat materiil. Syarat formil dan syarat materiil tersebut harus dipenuhi dalam proses penyidikan sehingga alat bukti elektronik menjadi sah ketika dihadirkan di pengadilan.

Bukti elektronik dapat diklasifikasikan sebagai bukti elektronik asli (*original digital evidence*) yang berarti bahwa barang secara fisik dan obyek data yang berkaitan dengan barang-barang tersebut pada saat bukti disita, bukti elektronik duplikat (*duplicate digital evidence*) yang merujuk pada reproduksi digital yang akurat dari seluruh obyek data yang tersimpan di dalam benda mati yang asli.

Suatu tindak pidana *cybercrime* yang otomatis dilakukan dengan menggunakan fasilitas atau jaringan internet dan elektronik, membutuhkan penangan yang lebih serius, karena pada tahap pembuktian untuk kejahtan

seperti ini membutuhkan bukti elektronik agar proses pembuktiannya lebih terjamin. Dalam kejahatan-kejahatan yang menggunakan komputer, bukti yang akan lebih mengarahkan kepada kejhatan dari peristiwa pidana tersebut yaitu berupa data-data elektronik. Data elektronik tersebut dapat berada di dalam komputer itu sendiri (*hard disk/floppy disk*) atau yang merupakan hasil *print out*, atau dalam bentuk lain berupa (*path)* atau jejak dari suaau aktivitas penggunakan komputer atau alat elektronik lainnya.

Ada dua hal yang dapat dijadikan panduan untuk menggunakan alat bukti elektronik dalam mengungkapkan kejahatan komputer, yaitu:

1. Adanya pola (modus operandi) yang relative sama dalam melakukan tindak pidana dengan menggunakan komputer.
2. Adanya persesuaian antara satu peristiwa dengan peristiwa lain.

Praktiknya agar setiap bukti elektronik terjamin keasliannya perlu dilakukan suatu autentifikasi, yang merupakan cara atau proses yang dilakukan dengan tujuan agar keaslian dari suatu dokumen dapat terjamin. Autentifikasi terhadap suatu bukti elektronik dapat dilakukan terhadap dua hal, yaitu:

1. Alat bukti elektronik yang ditampilkan dalam bentuk *hard copy* yang dicetak langsung dari alat penyimpanan;
2. Atas bukti elektronik yang dibuat dalam bentuk media penyimpanan seperti *CD Room,* kaset atau sarana penyimpanan lainnya yang di *copy* langsung dari media penyimpanan yang orisinil

3. Dilakukanya *digital forensic* dalam *laboratorium forensic* dengan memberikan berita acara hasil dari pemeriksaan pada *laboratorium forensic*.[5]

Hal tersebut sejalan dengan pendapat Edmon Makarim yang menyatakan bahwa persyartan secara umum keotentikan suatu alat bukti elektronik, yaitu:[6]

1. Keotentikan secara materiil yaitu kejelasan syarat subyektif dan obyektif, terkhusus, kecakapan bersikap tindak; jelas waktu dan tempat; *Confidentiality;* dapat ditelusuri kembali; Terjamin Keutuhan data atau keamanan informasi; Aslinya harus sesuai dengan *copynya*, yaitu salinan data.
2. Keotentikan secara formil yaitu ; sesuai bentuk yang ditentukan oleh undang-undang, termasuk media dan format tertentu; Pembacaan, yaitu apakah yang menjadi bukti telah dilakukanya suatu pembacaan; Pencantuman waktu, yaitu apakah jaminan waktu yang dituliskan dengan benar (*time-stamping*); Keamanan dokumen informasi beserta substansinya, yaitu apakah *historical data* terhadap dokumen elektronik sudah jelas; Pemeliharaan *Log* atau catatan, yaitu apakah benar telah terpelihara dengan baik. Keabsahan suatu alat bukti elektronik juga tergantung dalam pengupayan alat bukti tersebut jelas waktu dan kapannya.

[5] Wawancara dengan Bripka Dion Agung, Penyidik pada Disrekrimsus Polda DIY, pada hari Kamis, 5 Januari 2017, pukul 11.12

[6] Edmon Makarim, *Op. Cit.,* hlm 126

Kasus

Tindak Pidana *Cybercrime* pernah terjadi di wilayah hukum Pengadilan Negeri Sleman dan telah diputus serta memiliki kekuatan hukum tetap (*inkrach*). Putusan tersebut berakhir di Pengadilan Negeri Sleman sesuai dengan Putusan Nomor 535/Pid. Sus/2016/PN. Smn dalam perkara terdakwa:

Nama : ADIDIYA INDRA WIBIHARSO Alias ADIT;

Tempat lahir : Klaten;

Umur/tanggal lahir : 25 tahun / 03 Juni 1991;

Jenis Kelamin : Laki-laki;

Kebangsaan : Indonesia;

Tempat tinggal : Birit RT 001/001 Sukorejo Kecamatan Wedi Kabupaten Klaten Jawa Tengah

Agama : Islam;

Pekerjaan : Swasta (mantan karyawan Otazen Home);

Pendidikan : D3

Kronologi Kasus:

Sekitar pertengahan bulan Januari 2016 ADIDIYA INDRA WIBIHASONO bertemu dengan DWI RINANTI di warung dekat Otazen Home di Jalan Gejayan Condangcatur Depok Sleman, kemudian Adidya dengan DWI RIANTI dimana Dwi Rianti sekarang bekerja setelah keluar dari Otazen Home adalah sekarang DWI RINANTI bekerja sebagai marketing di Angel Interior yang beralamat di Jalan Kaliurang km. 10,2 Ngaglik Sleman Yogyakarta selanjutnya DWI RINANTI juga menjelaskan bahwa bisa dianggarkan fee untuk orang ketiga

(penghubung) apabila ada project deal dengan perusahaan Dwi dan beberapa waktu kemudian Adidya juga mendapat telephone dari Dwi Rinanti sehingga Adidya tertarik untuk mencarikan atau memberikan data custumer kepada Dwi Riananti.

Pada hari Rabu tanggal 27 Januari 2016 sekitar pukul 20.10 WIB bertempat di kantor Otazen Home di Jalan Gejayan No. 1 Condongcatur Depok Sleman, ADIDYA INDRA WIBIHARSO alias ADIT yang merupakan karyawan bagian marketing PT OTA Indonesia yang merupakan perusahaan di bidang furniture, membuka file dokomen berformat Microsoft Office (Word) yang berisi data customer/pelanggan yang ada dalam komputer Otazen Home kemudian Adidya memilih dan mengambil 7 (tujuh) data customer yaitu 1. Bapak Candra, 2. Bapak Wawan, 3. Ibu Yesi, 4. Ibu Tika Ramli, 5. Ibu Ida, 6. Ibu Sari dan 7. Bapak Tanto yang memuat nama custumer, alamat, phone/e-mail, kebutuhan dan keterangan/estinimasi harga, selanjutnya data custumer tersebut terdakwa kirim atau transfer melalui email terdakwa adidyaindra@gmail.com kepada sistem elektronik orang lain yaitu saksi DWI RINANTI yang merupakan karyawan marketing dari perusahaan furniture Angel Interior atau perusahaan lain pesaing dari Otazen Home dengan email duwi.harmonia@yahoo.com, dengan isi sebagai berikut:

TABEL IV

DATA COSTUMER OTAZEN HOME

No	Nama Customer	Alamat	Phone/email	Kebutuhan	Keterangan
1	Bapak	Yogya	08122694232	Lantai kayu, kayu sono	Estimasi

	Candra			keeling	Harga
2	Bapak Wawan	Yogya	081802771557	Project Mataram city (apartemen)	-
3	Ibu Yesi	-	081366012210	Project	-
4	Ibu Tika Ramli	-	0816877593	Project 3D WALLPANEL	-
5	Ibu Ida	-	081222229600	PROJECT WALKING CLOSET	-
6	Ibu Sari	-	085779988297 Anugerahibu.jogja@gmail.com	Custom meja resepsionis. 1. Full melamin (2X1) 2. Resepsionis Lt. 1 (2X1)	
7	Bapak Tanto	Cilicap	0818228683 T1m086@yahoo.com	Parquet lantai 3.000 m2	Estimasi

Sumber : Putusan Pengadilan Negeri Sleman Nomor 535/Pid.Sus/2016/PN.Smn.

Data customer Otazen Home tersebut merupakan data milik perusahaan sebelum deal dari sebuah project yang akan ditangani/ditindaklanjuti khusus customer domestic, yang hanya dapat/ boleh diakses dibuka oleh supervisor marketing, operasional officer dan manager reperesentative yang sifatnya rahasia, tidak boleh diketahui atau dikirim kepada pihak lain tanpa seijin dari pihak manajemen perusahaan; Aan tetapi Adidya justru mengirim atau mentransfer data costumer tersebut tanpa sepengetahuan dan seijin dari supervisor marketing,

operasional officer dan manager reperesentative Otazen Home dan hal ini Adidya lakukan dengan maksud untuk memperoleh keuntungan atau fee dari saksi DWI RINANTI apabila ada project yang deal/terjadi antara customer yang datanya diberikan oleh terdakwa tersebut dengan perusahaan tempat saksi DWI RINANTI bekerja sebagaimana yang pernah dijanjikan oleh saksi DWI RINANTI kepada Adidya;

Perbuatan terdakwa sebagaimana diatur dan diancam pidana dalam Pasal 48 ayat (2) jo Pasal 32 ayat (2) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Dari perbuatan terdakwa tersebut Hakim memutus perkara sebagai berikut:

1. Menyatakan terdakwa ADIDYA INDRA WIBIHARSO Alias ADIT telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana *"**Dengan sengaja dan tanpa hak mentransfer dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak".***
2. Menjatuhkan pidana terhadap terdakwa ADIDYA INDRA WIBIHARSO Alias ADIT dengan pidana penjara selama 6 (enam) bulan dan pidana denda sebesar Rp. 10.000.000,- (sepuluh juta rupiah), yang apabila pidana denda tersebut tidak dibayar diganti dengan pidana kurungan selama 1 (satu) bulan;
3. Menetapkan masa penahanan yang telah dijalani oleh terdakwa dikurangkan seluruhnya dari pidana yang dijatuhkan.
4. Menetapkan agar terdakwa tetap berada dalam tahanan;
5. Menetapkan barang bukti berupa :

- 1 (satu) lembar print screen forwarded message tanggal 27 Januari 2016 *email* adidyaindra@gmail.com kepada duwi.harmoni@yahoo.com
- 12 (dua belas) lembar print data costumer OTAZEN HME.
- 1 (satu) lembar print rekapan data yang dikirim adidyaindra@gmail.com kepada duwi.harmoni@yahoo.com
- 1 (satu) buah flashdisk warna hitam merk Sony 8 GB;
- Berita acara yang dibuat sdr. ADIDYA INDRA WIBIHARJO tanggal 10 Maret 2016;
- Surat permohonan maaf yang dibuat sdr. ADIDYA INDRA WIBIHARJO;
- Perjanjian kerja waktu tertentu nomor 070/OTA-HRD/PKWT/X/2015;
- Perjanjian kerja waktu tetentu nomor 003/T.1068/OTA-HRD/PKWT/I/2016;

6. Membebankan biaya perkara kepada terdakwa sebesar Rp 2.000,- (dua ribu rupiah)

Analisis Kasus:

Perkara tindak pidana *cybercrime* yang terdapat pada wilayah hukum Pengadilan Negeri Sleman dari Tahun 2015 hingga tahun 2017 yang telah diputus oleh hakim terdapat 12 perkara. Salah satu yang digunakan penulis adalah perkara Nomor 535/Pid.Sus/2016/PN.Smn, yakni tindak pidana *cybercrime* yang dilakukan Adidya Indra Wibiharso yang telah memiliki kekuatan hukum tetap

atau *Inkracht.* Berdasarkan perbuatan terdakwa, Adidya Indra Wibiharso dikenai sanksi pidana yaitu sebagaimana diancam dan dipidana dalam Pasal 48 ayat (2) jo Pasal 32 ayat (2) Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

> Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

Sanksi yang diberikan kepada Adidya Indra Wibiharso atas perbuatan terdakwa diancam dan dipidana dalam Pasal 48 ayat (2) Undang-undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang mana Pasal tersebut berbunyi:

> Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (Sembilan) tahun dan/atau denda paling banyak Rp 3.000.000.000,00 (tiga miliar rupiah).

Berdasarkan sanksi tersebut, perbuatan yang dilakukan oleh Adidya Indra Wibiharso yang mana telah mengirimkan data elektronik tanpa hak dan melawan hukum kepada orang yang tidak berhak Data elektronik yang dikirimkan adalah data *costumer* milik PT Otazen Home yang kontraknya belum deal , akan tetapi data itu dikirim ke Perusahaan lawan dari PT Otazen Home dengan dikirimkan menggunakan e-mail adidyaindra@gmail.com dikirim ke e-mail milik Dwi Rinanti yang merupakan karyawan dari Perusahaan lawan dari PT Otazen Home, Adidya mengirimkan data klien dari PT Otazen Home ke Perusahaan lawan PT Otazen Home dengan maksud agar mendapatkan *fee* dari Perusahaan Lawan PT Otazen Home, yang mana data tersebut bersifat rahasia yakni Data customer Otazen Home tersebut merupakan data milik perusahaan sebelum deal dari sebuah

project yang akan ditangani/ditindaklanjuti khusus customer domestic yang hanya dapat/ boleh diakses dibuka oleh supervisor marketing, operasional officer dan manager reperesentative yang sifatnya rahasia, tidak boleh diketahui atau dikirim kepada pihak lain tanpa seijin dari pihak manajemen perusahaan. Adidya mengirim data tersebut kepada pihak lain tanpa seijin pihak manajemen perusahaan akan tetapi dengan maksud memperoleh keuntungan. Sehingga perbuatan Adidya merupakan tindak pidana yang di kategorikan tindak pidana *cybercrime* karena perbuatan yang dilakukan Adidya tersebut merupakan perbuatan yang dilarang dan diancam dengan pidana melawan undang-undang. Adidya mentransfer data pelanggan ke Perusahan lawan dari perusahaannya . Tindakan tersebut merupakan tindak pidana karena dengan secara dengan sengaja dan melawan hukum dan sadar bahwa tindakanya dilakukan tanpa hak. Dan dikategorikan tindak pidana *cybercrime* karena objek dari tindak pidana tersebut adalah komputer maupun data elektronik, selain objek karena dalam melakukan tindak pidana menggunakan e-mail yang merupakan informasi elektronik.

Tindak Pidana yang dilakukan Adidya melanggar Pasal 32 ayat (2) UU No. 11 Tahun 2008 , rumusan pasal tersebut terdiri unsur-unsur berikut ini:

a. Kesalahan : dengan sengaja
b. Melawan hukum : tanpa hak atau melawan hukum
c. Perbuatan : memindahkan atau mentrasfer
d. Objek : Informasi Elektronik dan/atau Dokumen Elektronik
e. Tujuan : Kepada Sistem Elektronik Orang lain yang tidak berhak.

Perbuatan Adidya adalah mengirim data costumer menggunakan e-mail kepada orang yang tidak berhak. Perbuatan Adidya yang mengirimkan data customer suatu perusahaan tempatnya bekerja melalui email kepada orang lain tanpa sepengetahuan perusahaan dimana ia bekerja. Sehingga Perbuatan Adidya merupakan Tindak Pidana Cybercrime. Pembuktian Tindak Pidana *cybercrime* sama dengan tindak pidana lainnya, hanya saja data elektronik ataupun informasi elektronik disini memiliki peran yang besar dan merupakan kunci akan adanya suatu tindak pidana tersebut.

Data-data Costumer perusahaan yang disimpan di Komputer Perusahaan merupakan dokumen elektronik yang mengandung informasi elektronik berupa file dokumen berformat Microsft Office (Word). Barang bukti dalam tindak pidana tersebut adalah

1. 1(satu) lembar print screen forwaded message tanggal 27 Januari 2016 email adidyaindra@gmail.com kepada duwi.harmonia@yahoo.com
2. 12(dua belas) lembar print data custumer OTAZEN HOME
3. 1 (satu) lembar print rekapan data yang dikirim adidyaindra@gmail.com kepada duwi.harmonia@yahoo.com
4. 1 (satu) buah flashdisk warna hitam merk Sony 8 GB
5. Berita acara yang dibuat sdr. ADIDYA INDRA WIBIHARJO tanggal 10 Maret 2016
6. Surat permohonan maaf yang dibuat sdr. ADIDYA INDRA WIBIHARJO;
7. Perjanjian kerja waktu tertentu nomor 070/OTA-HRD/PKWT/X/2015;

8. Perjanjian kerja waktu tetentu nomor 003/T.1068/OTA-HRD/PKWT/I/2016

Dari barang bukti diatas , yang dikategorikan barang bukti elektronik yang selanjutnya dapat menjadi alat bukti elektronik adalah:

1. 1(satu) lembar print screen forwaded message tanggal 27 Januari 2016 email adidyaindra@gmail.com kepada duwi.harmonia@yahoo.com
2. 12(dua belas) lembar print data custumer OTAZEN HOME
3. 1 (satu) lembar print rekapan data yang dikirim adidyaindra@gmail.com kepada duwi.harmonia@yahoo.com
4. 1 (satu) buah flashdisk warna hitam merk Sony 8 GB

E-mail merupakan surat berbasis sistem elktronik yang menggunakan sistem jaringan *online* untuk mengirimkannya atau menerimanya, e-mail milik adidyaindra@gmail.com dapat dikategorikan suatu informasi elektronik dalam suatu system elektronik. Yang mana Apabila forwaded messege dalam e-mail tersebut terdapat unsur-unsur tindak pidana , maka email tersebut dapat menjadi alat bukti yang sah hal tersebut sesuai dengan Pasal 5 angka (1) UU ITE. Sehingga agar apa isi suatu informasi elektronik sah dan dapat menjadi alat bukti elektronik apabila menggunakan sistem elektronikyang sesuai dengan ketentuan yang diatur dalam UU ITE. Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik. Maka agar e-mail Adidya dapat menjadi alat bukti elektronik yang membuktikan tentang adanya perbuatan tindak pidana harus

dilakukan analisis apakah benar e-mail tersebut telah mengirimkan suatu data yang tidak seharusnya dikirim, analisi tersebut lah yang disebut *Digital Forensik*

Pasal 5 angka (2) UU ITE lain menyebutkan bahwa informasi elektronik yang telah didistribusikan atau diakses melalui jaringan telekominikasi dapat dicetak dan merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku. Dalam persidangan menjadi alat bukti petunjuk yang dapat memberikan keyakinan kepada Hakim bahwa telah terjadi suatu Tindak Pidana.

Penetuan Keabsahan suatu alat bukti elektronik menjadi penting dalam pembuktian tindak pidana *cybercrime* karena dengan diakunyai alat bukti itu sah menjadikan hakim yakin bahwa telah terjadi suatu tindak pidana. Namun dalam putusan diatas meskipun alat bukti telah diakui kedudukanya menjadi alat bukti yang sah, dalam pertimbangan hakim tidak disebutkan secara tersendiri mengenai Alat bukti elektronik yang sah. Dalam pertimbanganya hanya disebutkan berdasarkan keterangan saksi, ahli, dan barang bukti. Menurut analisi penulis tidak dicantumkannya penerangan mengenai alat bukti elektronik tersebut dikarenakan alat bukti elektronik merupakan suatu benda yang dibutuhkan seseorang ahli dalam menjelaskan suatu keadaan. Karena alat bukti tersebut meskipun telah dapat menerangkan suatu perbuatan tindak pidana, namun untuk menguatkan dibutuhkannya seorang Ahli.

Penentuan keabsahan alat bukti elektronik, tersebut dijelaskan oleh ahli yang mana Penentuan Keabsahan Alat bukti elektronik ditentukan bagaimana prosedur dalam memperoleh alat bukti tersebut dan wajib memenuhi 4(empat) syarat yang tertuang dalam Pasal 6 UU ITE yakni dapat diakses, ditampilkan,

dijamin keutuhanya, dan dapat dipertanggungjawabkan. Dalam Putusan tersebut Alat bukti elektronik telah memenuhi ke empat persyaratan tersebut. Dapat diaksesnya nya kembali e-mail tersebut dengan membuka user name dan password sehingga isi dari e-mail tersebut dapat dilihat dan ditampilkan kembali, bahwa Adidya telah mengirimkan Data Costumer yang tidak seharusnya dikirim ke sembarang orang. Jejak Path percakapan antara Adidya dengan Dewi masih tersimpan utuh dalama e-mail tersebut sehingga telah terjamin keutuhannya, untuk syarat terakahir yakni pertanggungjawaban. Hal tersebut disesuaikan dengan keterangan terdakwa itu sendiri dan persesuaian dengan keterangan para saksi.

Menurut wawancara dengan Bapak M. Ismet Karnawa, S. H., M. H. Jaksa Penuntut Umum Pada pengadilan Negeri Sleman, membenarkan bahwa kasus tersebut merupakan kasus tindak pidana *cybercrime* yang pernah terjadi di wilayah hukum PN Sleman. Bukti-bukti elektronik yang ditemukan tersebut dapat membuktikan kesalahan yang dilakukan oleh Adidiya . Cara yang ditempuh oleh pihak kepolisian dan kejaksaan Negeri Sleman untuk mensahkan bukti elektronik tersebut di hadapan pengadilan adalah dengan cara memproses bukti elektronik tersebut dari bentuk elektronik yang dihasilkan dari sistem komputer menjadi *output* yang dietak ke dalam media kertas. Penentuan keabsahan alat bukti elektronik tersebut menurut beliau ada dua hal yang menjadi parameter atau tolok mengenai keabsahan alat bukti elektronik tersebut, yakni Persesuaian dengan apa output yang di print harus sama dengan Berita Acara Pemeriksaan, hal ini dikarenakan bukti elektronik sudah sangat kuat membuktikan kesalahan terdakwa dan apa yang ada dalam sistem elektronik tersebut sulit untuk dibantah atau pun di

sangkal. Namun, apabila hal tersebut disangkal oleh terdakwa, proses digital forensik lah yang menentukan. Selain itu keotentikan dari alat bukti elektronik tersebut, dimana untuk mengupayakan ke otentikan, atau pun keaslian dari alat bukti elektronik, diperlukan proses digital forensik di Laboratorium Forensik Komputer.[7]

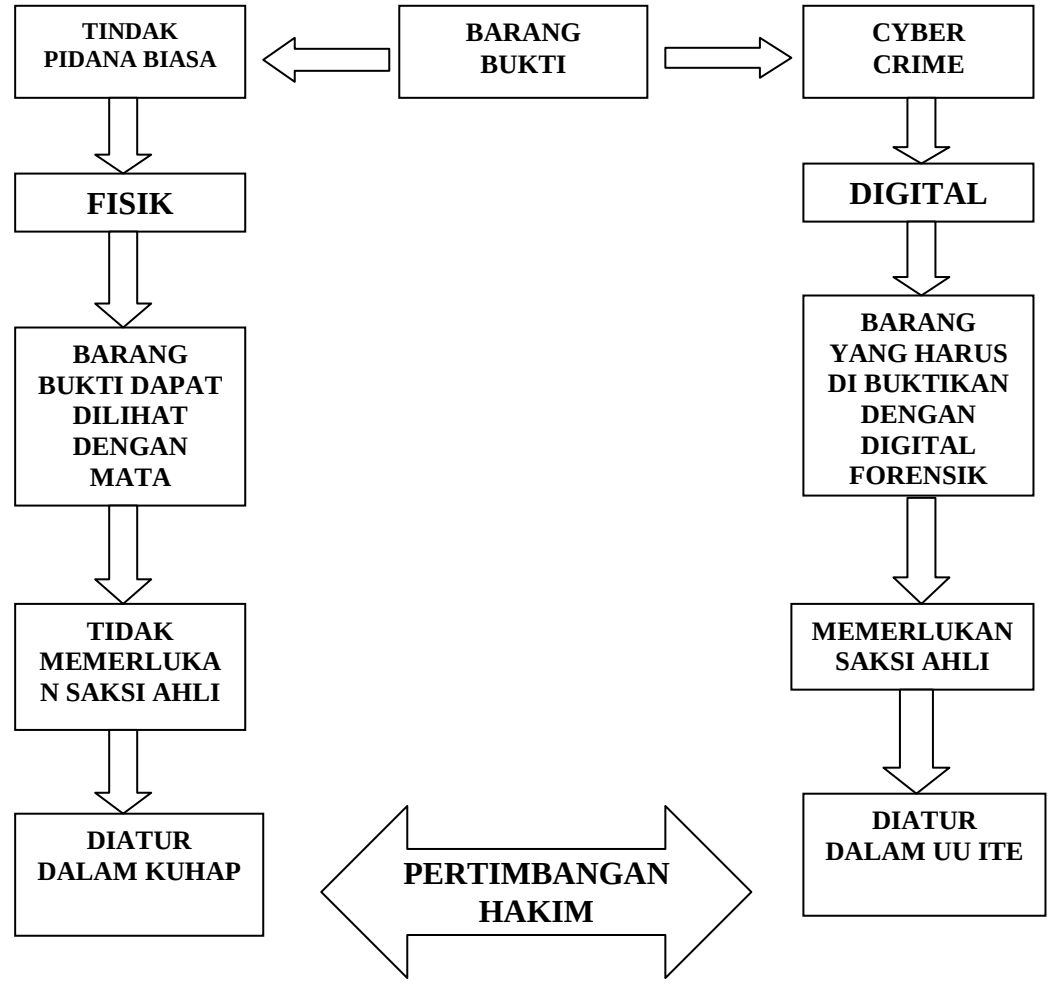
Parameter yang digunakan untuk menentukan keabsahan alat bukti elektronik dalam pembuktian tindak pidana *cybercrime* , harus berdasar pada Pasal 5 ayat (3) UU ITE, pasal 15 s.d 16 UU ITE, mengenai persyaratan materil. Dan Pasal 5 ayat (4) dan pasal 43 UU ITE, mengenaia persyaratan formil. Sehingga alat bukti elektronik tersebut dapat dikatakan sah sebagai alat bukti apabila memenuhi persyaratan tersebut. Maka Hakim dapat yakin terhadap perbuatan yang dilakukan terdakwa. Namun dari hasil penelitian penulis dan wawancara dengan para narasumber yakni Jaksa dan Penyidik masih kesulitan dalam menentukan keabsahan alat bukti elektronik tersebut, banyaknya multi tafsir dan tidak adanya keseragaman dalam menafsirkan syarat penentuan keabsahan alat bukti elektronik ini menyebabkan perbedaan antara penyidik yang satu dengan yang lain. Multi tafsir dari pemaknaan unsur dapat diakses, ditampilkan, dijamin keutuhannya dan dapat dipertanggungjawabkan dalam bisa berpengaruh terhadap keyakinan hakim dalam menafsirkan dan menilai keabsahan alat bukti elektronik tersebut, sehingga diperlukanya suatu aturan untuk menyamakan presepsi mengenai keabsahan alat bukti elektronik.

[7] Wawancara dengan M. Ismet karnawa, S. H., M. H, Jaksa Penuntut Umum pada Kejaksaan Negeri Sleman, pada hari Selasa, 17 Januari 2017, Pukul 11. 20 WIB

B. Penerapan Penggunaan Alat Bukti Elektronik dalam Pembuktian Tindak Pidana *Cybercrime*

Penggunaan Alat bukti Elektronik dalam Pembuktian tindak Pidana *Cybercrime* berbeda dengan penggunaan barang bukti non elektronik dalam pembuktian tindak pidana lain, hal ini dikarenakan adanya sifat khusus dalam elektronik, berikut skema perbedaannya,

GAMBAR IV
PERBEDAAN PENGGUNAAN BARANG BUKTI ELEKTRONIK DENGAN BARANG BUKTI NON ELEKTRONIK



Sumber: Diolah secara pribadi dari hasil penelitian

Dari skema tersebut dapat kita lihat bahwa bukti elektronik bersifat non-fisik, sehingga memerlukan saksi ahli untuk menjelaskan hal tersebut, berbeda halnya dengan bukti non-elektronik yang tidak menggunakan alat saksi ahli. Karena Barang bukti elektonik tidak dapat dilihat, diraba dengan mudah seperti barang bukti non-elektronik, maka sebelumnya digunakanlah suatu cabang keilmuan lain yakni Digital Forensik. Penanganannya pun berbeda yakni Tindak pidana *cybercrime* harus berdasar pada UU ITE.

Penanganan tindak pidana *cybercrime,* hukum acara yang digunakan yaitu hukum acara berdasarkan KUHAP. Hal tersebut memang tidak disebutkan secara jelas dalam UU ITE, tetapi karena UU ITE tidak menetukan lain maka KUHAP berlaku bagi tindak pidana yang termuat dalam UU ITE. Dalam Pasal 42 UU ITE disebutkan : "Penyidikan terhadap tindak pidana sebagimana dimaksud dalam undang-undang ini dilakukan berdasarkan ketentuan dalam Hukum Acara PIdana dan Ketentuan dalam Undang-undang ini." Berdasarkan pasal tersebut dapat ditafsirkan bahwa Hukum Acara Pidana yang diatur dalam KUHAP merupakan *lex genaralis*, sedangkan ketentuan acara dalam UU ITE ini merupakan *lex specialis*. Dengan demikian sepanjang tidak terdapat ketentuan lain maka ketentuan hukum acara yang digunakan seperti yang terdapat dalam KUHAP. Ketentran yang diatur lain dalam UU ITE ini yaitu menyangkut proses penyidikan dan penambahan satu alat bukti lain dalam penanganan tindak pidana yang diatur dalam UU ITE.

Agar suatu perkara pidana dapat sampai pada tingkat penuntutan dan persidangan, sebelumnya harus melewati tahap-tahap penyidikan yang mana dalam tahap penyidikan ini terdapat suatu tindakan-tindakan dari penyidik, namun sebelumnya dalam tahap penyelidikan yang mana harus ada bukti awal akan adanya suatu tindak pidana, maka dilanjutkan proses penyidikan. Setelah adanya bukti yang cukup, maka tugas penyidik melaklakukan pencarian dan pengumpulan barang bukti yang lebih kuat untuk membuat terang suatu tindak pidana dan untuk menemukan tersangkanya.

Dalam perkara tindak pidana *cybercrime* agar sampai dalam tahap persidangan juga harus melewati tahap-tahap tersebut, namun disini hanya saja tindak pidana *cybercrime* identik dengan kemayaan sehingga sulit sekali menemukan barang bukti yang bersifat elektronik, karenan barang tersebut tidak bisa diraba dengan indera, atau non- *paperlees*. Maka penanganan proses awal bersifat khusus. Barang bukti menjadi hal utama dalam proses penyidikan dan penyelidikan ini.

Barang bukti dalam proses pembuktian diperoleh melaui penyitaan. Penyitaan yang dilakukan oleh penyidik terhadap satu barang bukti akan memperlihatkan hubungan antara barang bukti yang ditemukan dengan tindak pidana yang dilakukan. Dalam tindak pidana *cybercrime* penyidik dapat menemukan jejak-jejak pelaku, berdasarkan informasi yang penyidik peroleh maka penyidik dapat menghubungi penyelenggara telekomunikasi yang dimaksud unrtuk memperoleh rekaman transaksi elektronik (*log file*)

dari modem yang digunakan oleh pelaku. Selain itu, penyelenggara juga dapat memberikan informasi mengenai identitas yang diberikan oleh pengguna layanan telekomunikasi pada waktu mendaftar *SIM Card* untuk pertama kalinya. Penggunaan alat bukti elektronik dalam tahap ini digunakan untuk mengetahui identitas pelaku, tempat kejadian dan barang bukti lain yang menjadi bukti awal telah terjadinya tindak pidana tersebut. Penyidik dalam menjelaskan wewenangnya untuk melakukan penggeladahan dan penyitaan terhadap sistem elektronik yang berhubungan dengan adanya dugaan terjadinya suatu tindak pidana *cybercrime*, harus telah terlebih dahulu mendapatkan izin dari Ketua Pengadilan Negeri. Hal tersebut disebutkan dalam Pasal 43 ayat (3) UU ITE. Namun, hal ini telah berubah dalam UU ITE baru yang mana menyatakan bahwa tidak memerlukan surat izin Ketua Pengadilan Apabila waktu mendesak.

Proses penyitaan barang bukti dalam tindak pidana *cybercrime* memerlukan metode, keahlian dan pengetahuan yang spesifik, berkaitan denagn adanya barang bukti elektronik atau alat bukti elektronik tersebut. Proses penyidikan dan penidakan tindak pidana *cybercrime* tidak dapat dilepaskan dari tantangan untuk menemukan, mengumpulkan, menyimpan, dan menyajikan bukti elektronik yang merupakan barang bukti yang member petunjuk atau medukung alat bukti yang digunakan

sebagai dasar penuntutan tindak pidana *cybercrime* lainnya di hadapan pengadilan.[8]

Pengakuan atas barang bukti elektronik melalui dua proses. Pertama, penyidik harus mengakui *hardware* (seperti komputer, disket, kabel jaringan) yang mengandung informasi elektronik. Kedua, penyidik harus dapat membedakan antara informasi yang tidak relevan dan data digital yang dapat digunakan memperkuat bahwa suatu tindak pidana telah dilakukan atau dapat menyediakan *link* atau menghubungkan antara tindak pidana dan korbannya atau antara tindak pidana dengan pelakunya.[9]

Pasal 43 ayat (2) Undang-undang ITE menyebutkan bahwa dalam melakukan penyidikan di bidang teknologi dan transaksi elektronik harus dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasian, kelancaran layanan publik, integritas data atau keutuhan data. Proses pemeriksaan barang bukti elektronik dilakukan oleh Pemeriksa Barang Bukti Digital Subdit IT & Cybercrime Disreskrimsus Polda Provinsi tersebut berdasarkan permintaan secara tertulis dari penyidik, dengan menyertakan :[10]

1. Laporan Polisi ;
2. Surat Perintah Tugas
3. Surat Perintah Penyidikan
4. Surat Perintah Penyitaan dan Berita Acara Penyitaan

[8] Wawancara dengan Bripka Dion Agung, Penyidik Disreskrimsus POLDA DIY, pada hari Kamis, 5 Januari 2017

[9] *Ibid.,*

[10] *Ibid.,*

5. Surat Permohonan pemeriksaan barang bukti elektronik dengan menyebutkan maksud dan tujuan dari permintaan (informasi apa saja yang dibutuhkan dari pemeriksaan).

Hambatan yang ditemui adalah apabila pada beberapa kasus yang melibatkan barang bukti dalam jumlah massif terkadang penyidik tidak dapat memberikan petunjuk secara lugas mengenai informasi apa saja yang ingin diperoleh, sehingga sebagai solusinya adalah diberikan hasil export data dokumen elektronik yang dapat untuk didapat untuk kemudian dilakukan pencarian secara mandiri oleh penyidik. Selain itu kurangnya sumber daya manusia yang mengerti dalam digital investigation menyebabkan lambatnya penanganan kasus yang berkaitan dengan ITE, karena untuk wilayah hukum Yogyakarta, untuk melakukan digital forensik harus melakukan permohonan pada Laboratorium Forensik Semarang , sehingga penanganan masih kurang optimal, maka agar penanganan awal proses penyelidikan dan penyidikan lebih optimal diperlukannya pendidikan tambahan bagi aparat penegak hukum dan Laboratorium forensik tersendiri.[11]

Tahap selanjutnya adalah tahap Penuntutan oleh Jaksa, pada tahap ini penuntut umum juga harus hati-hati dalam menggunakan alat bukti elektronik tersebut, sebelum dibuatkanya surat dakwaan, penuntut umum dapat melakukan penyidikan tambahan jika diperlukan. Sehingga alat bukti elektronik juga masih memiliki kedudukan yang berarti dalam

[11] *Ibid.,*

pembuatan surat dakawaan, keautentifikasian alat bukti tersebut juga menjadi penting karena akan diajukan dalam pembuktian dipersidangan oleh JPU. Hal yang paling penting dalam melakukan autentifikasi terhadap alat bukti elektronik yaitu mengatur dan mempertahankan keutuhan dari bukti tersebut. Tiap pihak yang menangani bukti tersebut harus mengidentifikasi apakah alat bukti elektronik tersebut yang dihadirkan di persidangan sama dengan alat bukti yang diproses pada tahap penyidikan. Dengan meminimalisasi jumlah pihak yang jumlah pihak yang menangani alat bukti tersebut, akan meninimalisasi kemungkinan dari alat bukti tersebut mengalami perubahan sejak pertama kali diperoleh.[12]

Dalam mencarai suatu data elektronik agar bias diterima sebagai alat bukti di pengadilan, aparat penegak hukum harus memastikan dan dapat membuktikan bahwa dalam data tersebut tidak ada informasi yang ditambah atau dikurangi, semua media telah diamankan dan pada saat meng-copy harus dilakukan dengan proses yang dapat dipercaya

Pada tahap pembuktian di pengadilan, alat bukti eleketronik haruslah dapat dibuktikan keabsahannya yaitu proses dalam melakukan penggledahan, penyitaan serta pemeriksaan bukti elektronik, bukan hanya dilakukan pembuktian terhadap informasi elektronik yang terdapat di dalam bukti elektronik tersebut tetapi harus juga dibuktikan keabsahannya maka informasi elektronik di dalam bukti elektronik tersebut menjadi valid, ini menjadi faktor penting di dalam penilaian hakim di pengadilan

[12] Wawancara Bapak Muh. Ismet Karnawa, S. H., M. H., Jaksa Muda Kejaksaan Negeri Sleman, pada hari Selasa, 17 Januari 2017, pukul 11.32 WIB

terhadap kekuatan alat bukti elektronik, serta dapat mempengaruhi keyakinan hakim terhadap informasi elektronik yang menjadi salah satu alat bukti elektronik di dalam pembuktian dalam perkara tindak pidana *cybercrime*.

Bukti elektronik yang telah diautentifikasi (mengatur dan mempertahankan keutuhan dari barang bukti), tidak dengan secara otomatis dapat dijadikan sebagai alat bukti dipersidangan. Bukti elektronik tersebut tetap perlu diidentifikasi dan dijelaskan isinya oleh saksi ahli dan terdakwa yang hadir dalam persidangan tersebut. Walaupun di dalam UU ITE alat bukti elektronik suadah diakui tetapi dalam pembuktian keberadaan dari suatu alat bukti elektronik tidak dapat berdiri sendiri, sehingga harus didukung dengan alat bukti lainnya. Hal tersebut sesuai dengan ketentuan yang terdapat dalam Pasal 183 KUHAP, yang dalam membuktikan kesalahan dari seseorang terdakwa dibutuhkan dua alat bukti yang saling mendukung dan dari alat–alat bukti tersebut hakim memperoleh keyakinan.

Keberadaan barang-barang bukti sangat penting dalam investigasi kasus-kasus *computer crime* dan *computer-related crime,* karena dengan barang bukti inilah penyidik dapat mengungkapkan kasus-kasus tertsebut dengan kornologi yang lengkap, untuk kemudian melacak keberadaan pelaku, menangkapnya dan akhirnya dijadikan dasar untuk mendukung pembuktian keselahan si pelaku. Oleh karena itu pemahaman yang

menyeluruh atas apa yang dimaksud dengan bukti elektronik pun akan sangat membantu usaha pengungkapan dan pembuktian di pengadilan.

Pengaturan atau pengakuan terhadap bukti elektronik sebagai salah satu alat bukti yang sah memang kurang. Berdasarkan berbagai peraturan berbagai peraturan yang telah mengakuinya, setidakanya hanya UU ITE yang memberikan penjelasan perihal bukti elektronik yang dapat dipergunakan sebagai alat bukti yang sah di muka persidangan, walupun penjelasan dimaksud bukunlah sebuah pendifeniskan yang dinyatakan secara tegas terhadap apa terhadap apa yang dimakud dengan terminology bukti elektronik.

Sehubungan dengan hal tersebut, Pasal 5 ayat (3) UU ITE mengatur bahwa "*informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam undang-undang ini." Artinya,* berlakunya informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagai alat bukti yang sah hanya diakui apabila menggunakan sistem elektronik yang sesuai dengan ketentuan yang diatur dalam UU ITE. Dalam hal ini yang dimaksud dengan sistem elektronik adalah sebagaimana diatur dalam Pasal 1 angka 5 UU ITE yang menyatakan bahwa sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisa, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.

Terkait dengan hal tersebut, diterimanya informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagai alat bukti yang sah bukanlah tanpa pengecualian. Menurut Pasal 5 ayat (4) UU ITE, informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya yang tidak dapat diterima sebagai alat bukti elektronik adalah apabila:

1. Di dalam suatu undang-undang ditentukan bahwa suatu surat yang akan dijadikan alat bukti harus dibuat dalam bentuk tertulis. Dalam hal ini surat yang menurut undang-undang harus dibuat tertulis meliputi tetapi tidak terbatas pada suarat berharga, suarat yang berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana, dan administrasi Negara.
2. Di dalam suatu undang-undang ditengtukan bahwa suatu surat yang akan dijadikan alat bukti harus dibuat dalam bentuk akta notaries atau akta yang dibuat oleh Pejabat Pembuat Akta.

Cara atau metode memperoleh informasi elektronik dan/atau dokumen elektronik tersebut haruslah dengan cara-cara yang sah dan benar. Perolehan informasi elektronik dan/atau dokumen elektronik tersebut haruslah dilakukan dengan tidak melawan hukum dan harus pula dapat dipertanggungjawabkan metode perolehannya sehingga kebenaran dan keutuhan informasi elektronik dan/atau dokumen elektronik dimaksud dapat terjamin.

Sutan Remy Sjahdeini, menyatakan bahwa “Berdasarkan ketentuan Pasal 5 UU ITE informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagai alat bukti hukum yang sah, namun sebelum di Indonesia diberlakukan sistem pengamanan elektronik berupa *asymmetric cryptosystem* atau *publik key cryptosystem* untuk pembuatan dan/atau pengiriman pesan (*messege*) yang bertujuan menjamin kebenaran isi dan/atau hasil cetaknya sebagai alat bukti hukum yang sah, maka ketentuan Pasal 5 UU ITE mengenai pemberlakuan informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagai alat bukti hukum yang sah tidak akan memberikan sifat mutlak kepada informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagai alat bukti hukum yang tidak dapat diragukan isi dan/atau keasliannya.

Barang bukti elektronik rentan diubah atau dirusak, karena itu penuntut umum harus secara seksama memeriksa rantai serah terima setiap barang yang berisi bukti elektronik sejak penyitaaan. Tidak boleh ada kesenjangan atau priode waktu yang tidak diketahui dalam rantai serah terima, dan barang bukti harus diamankan serta disimpan dengan benar setiap saat ketika sedang tidak diperiksa.

Penggunaan alat bukti elektronik tersebut harus lah benar-benar hati-hati dan mengedepankan keamanan, penggunaanya memang diperlukan hakim dalam menafsirkan hal tersebut. Berikut data Penggunaan Alat Bukti Elektronik Pada Wilayah Hukum Pengadilan Negeri Sleman.

TABEL IV

DAFTAR ALAT BUKTI ELEKTRONIK YANG DIGUNAKAN DALAM PEMBUKTIAN TINDAK PIDANA *CYBERCRIME* PADA WILAYAH HUKUM PENGADILAN NEGERI SLEMAN TAHUN 2015-2017

NO	NOMOR PERKARA	NAMA TERDAKWA	KLASIFIKASI TP		ALAT BUKTI/ BARANG BUKTI		STATUS KASUS dan PEMIDANAAN	KET
			PASAL	TINDAK PIDANA	NON-ELEKTRONIK	ELEKTRONIK		
1.	470/Pid.Sus/2014/ PN Smn	Marceelus Moses Parera Als Ongen Bin Daniel Mage	Pasal 45 ayat (1) Jo Pasal 27 ayat (1) UU ITE	Prostitusi Online	- 11 Kondom merek Sutera - 1 Kondom merek Fiesta	1 Handphone merek Blackberry warna merah simcard No 087839855614.	SELESAI 1 Tahun penjara	-
2.	37/Pid.Sus/2015/ PN Smn (Reg : 29 Jan 2015)	Albany Adhityatama bin Cecep Setiyantono	*Pasal 35 Jo Pasal 51 ayat (1) UU ITE*	Memanipulasi data	- Dua lembar kwitansi pembayaran tes masuk - Kertas sobekan kecil	- password nomor UPCM 14711205690 dan 140814685516047 - Log File - Komputer	SELESAI 3 Bulan Penjara	

						- Website : www.cbt.uii.ac.id		
3.	188/Pid.Sus/2016/ PN Smn (Reg : 12 April 2016)	Bonivasius Esdharyanto Als.Bonny Telo	Pasal 27 ayat (3) UU ITE	Pencemaran Nama baik melalui media sosial (facebook)	- 1 (satu) bendel copy salinan akta nomor : 07 tanggal 09 Januari 2013 tentang pernyataan keputusan rapat umum pemegang saham luar biasa PT. NONBAR - 1 (satu) bendel copy salinan akta Nomor : 72 tanggal 30 Desember 2013 tentang Jual Beli Saham. - 1 (satu) bendel copy salinan akta Nomor :	1 (satu) keping CD berisi softcopy atau file-file capture tampilan facebook akun “Anton” yang terlihat status facebook akun “BonnyTello II”. 14 (empat belas) lembar printout capture tampilan facebook akun “Anton” yang terlihat status/komentar facebook akun “BonnyTello II”. 1 (satu) keping CD berisi softcopy	SELESAI Pidana Penjara 6 Bulan	

					20 tanggal 29 Oktober 2009 tentang Perubahan Anggaran dasar PT. Nonton Bareng Bola	atau file-file capture tampilan facebook akun "Antonius Monica" yang terlihat status facebook akun "BonnyTello II"; 6 (enam) lembar printout capture dari akun facebook "Antonius Monica". 1 (satu) unit handphone merk Asus type Zenfon 6 warna hitam dengan IMEI 353233060058922 dan IMEI 353233060058930 9 (sembilan) lembar printout capture dari akun		

						facebook “BonnyTello II”.		
4.	242/Pid.Sus/2016/ PN Smn (12 May 2016)	Yusuva Cahyono Putro Als. Yusuf Als. Cahyo	Pasal 45 ayat (3) Jo. Pasal 29	Ancaman Kekerasan menggunakan ITE	-	- 1 (satu) buah sim card No. 085641710310 - 1 (satu) buah HP merk Nokia warna hitam Seri 1035 ; - 1 (Satu) lembar print out screen shot SMS “Selamat pagi bpk yang terhormat, silahkan evakuasi anak2 karena bom sudah terpasang disekolahan istri anda. Silahkan mau percaya atau tidak - Jihad kebatilan	MINUTASI PERKARA SUDAH DIPUTUS Pidana Penjara 7 buan	-

5.	249/Pid.Sus/2016/ PN Smn (16 May 2016)	Ujang Gunawan Als. Tulang Bin Jono Darmawan	Pasal 20 jo pasal 45 ayat (2) UU ITE	Penipuan menggunakan HP	-	1 (satu) buah Handphone merk Samsung warna hitam silver CT C3322;	Pidana Penjara 1 Tahun	
6 .	502/Pid.Sus/2016/ PN Smn (R: 12 October 2016)	Eko…Subowo Suprihatin Als.Eko	Pasal 45 ayat (1)jo pasal 27 ayat (1) UU ITE	Muatan kesusilaan menggunakan ITE (Perdagangan orang)	-2 (dua) lembar uang pecahan Rp. 100.000 (seratus ribu rupiah). 1 (satu) buah tas warna cokelat merk Polo Star 11 (sebelas) pcs kondom sutera 3 (tiga) buah Kartu Tanda Penduduk (KTP) atas nama EKO SUBOWO SUPRIHATIN Uang sebesar Rp. 262.000,- (dua ratus enam puluh dua ribu rupiah)	14 (empat belas) lembar print out capture screen/tampilan group facebook ANGEL ANGEL JOGJA MAGELANG SOLO dari akun facebook Cahyo Putra. 1 (satu) buah hand phone merk samsung duos warna putih dengan nomor hand phone terpasang 082242487246. 4..(empat) lembar	Pidana Penjara	

					1 (satu) buah dompet warna hitam	capture screen tampilan akun BBM sdr EKO dengan nama BBM PeHa. 1 (satu) lembar capture screen akun facebook Noviana menawarkan diri. 1 (satu) buah hand phone merk Xiaomi redmi note 2 warna putih dengan casing warna emas terpasang kartu paket telkomsel 1 (satu) buah hand phone merek Eagle warna hitam kombinasi orange terpasang		

						nomor HP 087843311650 6 (enam) lembar print out capture screen dari BBM 5954FD04 nama akun mom asu milik PUJI RASWATI 19 (sembilan belas) lembar print out screen capture dari akun facebook Noviana milik sdr. EKO SUBOWO SUPRIHATIN als EKO. 18 (delapan belas) lembar print out screen capture dari akun facebook Kristin milik sdr. EKO		

						SUBOWO SUPRIHATIN als EKO. 23 (dua puluh tiga) lembar print out screen capture dari akun facebook Hanny Keisha milik sdr. EKO SUBOWO SUPRIHATIN als EKO. 13 (tiga belas) lembar print out screen capture dari akun facebook Pejuang Hati dan Aya Dhewi sebagai admin group DEWI DEWI JOGJA milik sdr. EKO SUBOWO SUPRIHATIN als EKO.		

						8 (delapan) lembar prin out screen capture dari PIN BBM 74334E14 atas nama akun PeHa milik sdr. EKO SUBOWO SUPRIHATIN als EKO.		
7.	535/Pid.Sus/2016/ PN Smn (Reg : 1 November 2016)	ADIDYA INDRA WIBIHARSO Alias ADIT	Pasal 48 ayat (2) jo Pasal 32 ayat (2) UU ITE	memindahka atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada system elektronik orang lain yang tidak berhak	- Berita Acara yang dibuat sdr.ADIDYA INDRA WIBIHARSO tanggal 10 Maret 2016 - Surat Permohonan Maaf yang dibuat sdr. ADIDYA INDRA WIBIHARSO - Perjanjian kerja waktu	- 1 (satu) lembar print screen forwarded message tanggal 27 Januari 2016 email adidyaindra@gmail.com kepada duwi.harmoni@yahoo.com - 12 (dua belas) lembar print data customer OTAZEN HOME	penjara selama 6 (enam) bulan dan pidana denda sebesar Rp. 10.000.000 ,- (sepuluh juta rupiah),	

					tertentu nomor: 070/OTA-HRD/PKWT/X/2015 - Perjanjian kerja waktu tertentu nomor: 003/T.1068/OTA-HRD/PKWT/I/2016	- 1 (satu) lembar print rekapan data yang dikirim adidyaindra@gmail.com kepada duwi.harmoni@yahoo.com - 1 (satu) buah Flashdisk 8 GB merek SONY warna hitam data customer PT Otazen Home		
8.	Nomor 603/Pid.Sus/2016/PN Smn (Reg : 14 Desember 2016)	Marda Dwi Anggara Als Mardha Cungkrink	Pasal 45 ayat (1) jo pasal 27 ayat (1) UU ITE	Perdagangan Orang melalui media sosial	- 1 (satu) buah buku rekapan merk Mirage yang berisi pesanan baju acara kopdar (kopi darat) BIDADARI JOGJA ; - 1 (satu) buah spanduk/banne	- 4 (empat) lembar prinout printsreen capture group “AN[G]EL JO[G]JA” dari Remboy Anggara Cungkrink ; - 1 (satu) bendel printout konten	pidana penjara selama 3 (tiga) tahun dan denda sebesar Rp. 25.000.000 ,00 (dua puluh lima juta rupiah)	

					r dengan tulisan “See u again Bidadari Jogja Welcome to Bidadari n[a]kal Jogja dengan gambar wanita setengah telanjang bersayap;	group facebook “AN[G]EL JO[G]JA” dari akun Remboy Anggara Cungkrink ; - 8 (delapan) lembar printout screen capture chattingan akun WA atas nama Mardha Cungkrink AJ menawarkan wanita kepada akun WA dengan nama profil Angling; - 7 (tujuh) lembar printout screen capture chatingan akun WA atas nama Mardha Cungkrink AJ dengan pemilik nomor +		

						628991789576 - 1 (satu) buah Handphone tablet merk Asus warna biru; - 1 (satu) buah Hanphone merk Lenovo seri S90-A warna grey ; - 4 (empat) lembar printout screen capture percakapan BBM Vinadara Melinda dengan Mardha Cungkrink AJ II HK ; - 6 (enam) lembar printout screen anggota dari group BBM "AN[G]EL JO[G]JA";		

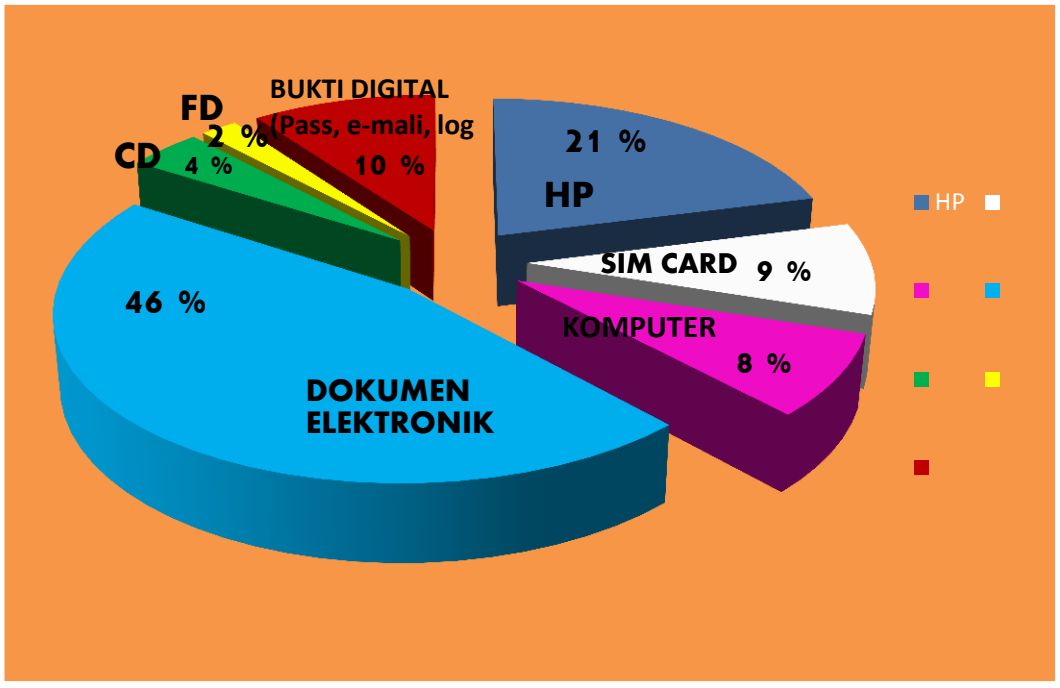
						- 33 (tiga puluh tiga) lembar printscreen group facebook BIDADARI JOGJA		
11.	93/Pid.Sus/2017/PN Smn (Reg : 23 Feb 2017)	Fatkhurrohman Als Fatur	Pasal 45 ayat (1) jo Pasal 27 Ayat (3) UU ITE	Pencemaran Nama Baik lewat Media Sosial	-	- Belum ada Pencatatan Barang Bukti	PROSES PERSIDANGAN	
12	161/Pid.Sus/2017/PN Smn (Reg : 3 April 2017)	Sugiharto Bin Satimin Maryoto	-	Perbuatan Tanpa ijin menggunakan spektrum frekuensi radio dan orbit satelit tanpa ijin pemerintah	-	Belum ada Pencatatan Barang Bukti	PROSES PERSIDANGAN	

Sumber : *Sistem Informasi Penelusuran Perkara Pengadilan Negeri Sleman*, http://pn-sleman.go.id/sipp/detail_perkara.com Diakses pada Tanggal 10 April 2015 Pukul 11.21 WIB.

Sebagaimana dari table diatas Pengadilan Negeri Sleman telah memutuskan perkara tindak pidana yang berkaitan dengan ITE atau tindak pidana *cybercrime*. Dalam pembuktian di persidangan menggnakan alat bukti elektronik. Penggunaan tersebut dimaksudkan karena tindak pidana tersebut bersingungan dengan elektronik maka otomatis jumlah presentase penggunaan alat bukti elektronik lebih banyak dibandingkan non elektronik. Berikut Jumlah presentase penggunaan alat bukti elektronik pada perkara di atas.

GRAFIK III

JUMLAH PRESENTASE PENGGUNAAN ALAT BUKTI ELEKTRONIK PADA PEMBUKTIAN PERKARA TINDAK PIDANA *CYBERCRIME* DI WILAYAH HUKUM PENGADILAN NEGERI SLEMAN



Sumber: SIPP PN Sleman, http://pn-sleman.go.id/sipp/detail_perkara.com Diakses pada Tanggal 10 April 2015 Pukul 11.21 WIB.

Dari Grafik III di atas, Penggunan alat bukti elektronik dalam pembuktian tindak pidana *cybercrime* sangatlah banyak dan beragam macamnya, jumlah presentasenya adalah bahwa dokumen elektronik memiliki presentase yang tinggi sebesar 46 %, selanjutnya penggunaan HP 21 %, SIM card adalah 9 %, Komputer adalah 8 %, FD adalah 2 %, CD adalah 4 %, dan bukti digital seperti alamat website, password, e-mail adalah 10 %. Dokumen elektronik diatas memilik presentase yang tinggi dikarenakan semua rekam jejak, informasi elektronik di cetak dalam bentuk dokumen. Untuk Penggunaan HP, Sim Card, Komputer, FD, CD oleh penuntut umum hanya di jadikan suatu barang bukti, bahwa kejadian tindak pidana tersebut benar telah terjadi, dan memberikan petunjuk bagi hakim dalam memutuskan suatu perkara yang di ajukan kepadanya.

Cara yang digunakan di hadapan Pengadilan dalam penggunaan alat bukti elektronik di atas adalah dengan cara memproses bukti elektronik dalam bentuk elektronik dari sistem elektronik menjadi *output* yang dicetak ke dalam media kertas, yakni di ubah perwujudannya dalam bentuk *hardcopy*, yaitu di print, tanpa adanya modifikasi. Lalu untuk memperkuatnya, *print-out* tersebut dianalisis oleh seorang saksi ahli untuk disampaikan validitasnya di hadapan pengadilan. Sedangkan cara hakim untuk melihat kevaliditasannya adalah dengan melihat persesuaian keterangan ahli dengan berita acara dan keterangan saksi, dan terdakwa disertai dengan penyamaan dengan bukti elektronik yang di hadapkan

kepadanya. Agar lebih jelasnya akan dipaparlan lebih rinci mengenai salah satu kasus diatas.

KASUS 1

Dari 12 (dua belas) perkara tindak pidana *cybercrime* yang pernah terjadi dan telah diputus serta memiliki kekuatan hukum tetap (*inkracht*) salah satunya adalah Putusan Nomor 37/Pid. Sus/2015/Pn. Smn dalam perkara terdakwa :

Nama	: Albany Adityatama Bin Cecep Setyantono
Tempat Lahir	: Yogyakarta
Umur/Tanggal Lahir	: 19 tahun/12 April 1996
Jenis Kelamin	: Laki-laki
Kebangsaan	: Indonesia
Tempat tinggal	: Notoyudan GT II/12117 Yogyakarta
Agama	: Islam
Pekerjaan	: Mahasiswa

Kronologi Kasus

Albany Adityatama pada hari Kamis tanggal 14 Agustus 2014 sekitar jam 11.00 WIB bertempat di Kampus Universitas Islam Indonesia (UII) di Jln.Kaliurang Km. 14,5 Ds. Umbulmartani Kec. Ngemplak Kab. Sleman yang masih termasuk di dalam daerah hukum Pengadilan Negeri Sleman, dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen

Elektronik milik orang lain atau milik publik. Adapun perbuatannya dilakukan dengan cara sebagaimana berikut :

Pada mulanya pada hari Senin tanggal 11 Agustus 2014 terdakwa dihubungi oleh sdr. MOH. RIZQI yang mengatakan bahwa ada adik temannya yaitu yang bernama saksi PUJI SEPTIARA sudah beberapa kali mengikuti ujian masuk Universitas Islam Indonesia (UII) akan tetapi selalu gagal. Kemudian sdr. MOH. RIZQI meminta tolong kepada terdakwa untuk meloloskan saksi PUJI agar diterima sebagai mahasiswa UII Fakultas Farmasi dengan cara terdakwa mengerjakan soal ujian tes masuk UII milik saksi PUJI. Pada waktu sdr. MOH. RIZQI menjanjikan imbalan berupa uang apabila saksi PUJI bisa lolos ujian dan diterima di UII dan Albany menyanggupinya. Kemudian pada hari Kamis tanggal 14 Agustus 2014 jam 06.30 WIB Albany dihubungi lagi oleh sdr. MOH. RIZQI yang mengatakan bahwa saksi PUJI sudah menunggu di kampus UII dan sdr. MOH . RIZQI memberikan ciri – ciri pakaian yang dikenakan oleh saksi PUJI. Setelah bertemu dengan saksi PUJI kemudian Albany dan PUJI mendaftar di loket dan setelah membayar dan menyerahkan syarat administrasi kemudian Albany mendapatkan no. UPCM : 1472122337 dan no. Slip 0140814085335500, sedangkan PUJI mendapatkan no. UPCM : 1471120569 dan no. Slip 0140814085516047. Kemudian Albany mencatat no. UPCM dan no. Slip milik saksi PUJI pada sobekan kertas begitu juga sebaliknya saksi PUJI mencatat no. UPCM dan no. Slip milik Albany pada sobekan kertas. Sekitar pukul 10.00 WIB Albany dan saksi PUJI masuk ke ruang ujian CBT (Computer Based Test) dan duduk di meja komputer yang berdampingan. Kemudian Albany dan saksi PUJI

log in pertama pada website UII www.cbt.uii.ac.id menggunakan no. UPCM dan no. Slip masing – masing untuk pengisian data diri guna pencetakan kartu ujian (UPCM). Setelah kartu ujian dicetak kemudian Albany dan saksi PUJI melakukan log in kedua pada website UII untuk mengerjakan soal ujian CBT (Computer Based Test). Pada saat itu Albany log in menggunakan no. UPCM dan no. Slip miliksaksi PUJI yang sebelumnya sudah dicatat di sobekan kertas sedangkan saksi PUJI log in menggunakan no. UPCM dan no. Slip milik terdakwa. Pada saat Albany sedang mengerjakan soal dengan menggunakan identitas saksi PUJI dan saksi PUJI sedang mengerjakan soal dengan menggunakan identitas Albany saksi AGUS KURNIAWAN selaku pengawas ujian yang sedang membagikan kartu ujian kepada masing – masing peserta menemukan kejanggalan pada identitas Albany dan saksi PUJI yaitu nama padakartu ujian berbeda dengan nama pada komputer padahal seharusnya nama pada kartu ujian sama dengan nama pada komputer. Kemudian saksi AGUS melaporkan hal tersebut kepada panitia ujian dan selanjutnya terdakwa dan saksi PUJI disuruh berhenti mengerjakan soal ujian dan keduanya dibawa ke ruang panitia untuk diamankan.

Maksud dari Albany mengerjakan soal ujian CBT secara online dengan menggunakan identitas milik saksi PUJI adalah agar saksi PUJI dapat lolos ujian dan dapat diterima sebagai mahasiswa UII dan terdakwa akan mendapatkan sejumlah imbalan berupa uang. Hal ini merupakan perbuatan yang merugikan pihak UII karena apabila saksi PUJI dapat diterima sebagai mahasiswa UII hal itu bukan berdasarkan dari kemampuan saksi PUJI sendiri akan tetapi disebabkan oleh perbuatannya.

Website UII www.cbt.uii.ac.id merupakan website resmi milik UII yang tidak bisa diakses secara umum sebelum Internet protocol addres dibuka oleh Badan Informasi System UII sehingga Perbuatannya diatur dan diancam pidana dalam pasal 32 ayat (1) Jo Pasal 48 ayat (1) UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik;

Analisis Kasus :

Dari kasus diatas cara yang digunakan di hadapan Pengadilan dalam penggunaan alat bukti elektronik di atas adalah dengan cara memproses bukti elektronik dalam bentuk elektronik dari sistem elektronik menjadi *output* yang dicetak ke dalam media kertas, yakni di ubah perwujudannya dalam bentuk *hardcopy*, yaitu di print, tanpa adanya modifikasi. Lalu untuk memperkuatnya, *print-out* tersebut dianalisis oleh seorang saksi ahli untuk disampaikan validitasnya di hadapan pengadilan. Sedangkan cara hakim untuk melihat kevaliditasannya adalah dengan melihat persesuaian keterangan ahli dengan berita acara dan keterangan saksi, dan terdakwa disertai dengan penyamaan dengan bukti elektronik yang di hadapkan kepadanya.

Penulis mencoba membandingakan penggunaan alat bukti elektronik dengan kasus yang berbeda

Kasus II

Tindak Pidana *Cybercrime* pernah terjadi di Sleman dan telah diputus serta memiliki kekuatan hukum tetap (*Inkracht*). Putusan tersebut berakhir di Pengadilan Negeri Sleman sesuai dengan Putusan Nomor 476/PID.SUS/2013/PN. SLMN dalam perkara terdakwa:

Nama	: HERMAN JOSEPH bin IE HIE SOENG;
Tempat Lahir	: Yogyakarta;
Umur/tanggal lahir	: 47 Tahun /18 Juni 1986;
Jenis Kelamin	: Laki-laki;
Kebangsaan	: Indonesia;
Tempat tinggal	: Desa Jaban RT. 03 RW. 25 Sinduharjo Ngaglik Sleman;
Agama	: Katholik;
Pekerjaan	: Wiraswasta (Pemilik warnet “Bella Net”);
Pendidikan	: S1;

Kronologi Kasus:

Pada hari Rabu tanggal 03 Juli 2013 sekitar pukul 14.00 wib sampai dengan pukul 17.00 wib atau setidak-tidaknya pada bulan Juli tahun 20l3 bertempat di warung Internet “ BELLA NET” jalan Gejayan, Mrican nomor 27 A Catur Tunggal, Depok, Sleman didalam daerah hukum Pengadilan Negeri Sleman, terdakwa telah dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, yang dilakukan dengan cara-cara sebagai berikut :

Herman Joseph Bin Ie Hie Soeng pada waktu dan tempat tersebut diatas selaku pemilik dan pengelola warnet “ BELLA NET” sewaktu dilakukan operasi Maya bidang ITE yang bermuatan pornografi oleh

petugas POLDA DIY didalam warnet CPU Server kedapatan untuk menyimpan file-file gambar porno dari situs porno, sehingga user (pemakai) dapat mengakses dari situs porno secara bebas dan setiap user yang menggunakan warnet tersebut dikenakan biaya Rp.3000,- (tiga ribu rupiah) per jam pada siang hari dan Rp.1.500,-(seribu lima ratus rupiah) pada malam hari, bahwa file-file gambar dari situs porno yang menggambarkan hubungan sexsual yang dilakukan oleh seorang laki-laki dan seorang perempuan dan gambar bergerak atau film tersebut juga menggambarkan seorang laki-laki dan seorang perempuan yang memperlihatkan alat kelaminnya kemudian melakukan ciuman, perabaan dan selanjutnya melakukan hubungan badan hal ini adalah perbuatan pelanggaran kesusilaan sehingga petugas melakukan penyitaan barang-barang berupa : 1(satu) buah CPU server, 3(tiga) buah CPU bilik nomor 10, 15 dan 17, 1(satu) buah CPU biling, 1(satu) buah monitor, 1(satu) Mouse, 1 (satu) buah Keyboard dan 1(satu) buah Swit, kemudian diproses sesuai hukum yang berlakU ;

Perbuatan nya sebagaimana diatur dan diancam pidana melanggar pasal 45 ayat (1) jo pasal 27 ayat (1) Undang Undang Republik Indonesia NO. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) ;

Dari perbuatan terdakwa tersebut Hakim memutus perkara sebagai berikut :

1. Menyatakan terdakwa Herman Joseph bin Ie Hie Soeng terbukti secara sah dan meyakinkan bersalah melakukan

kejahatan “ dengan sengaja dan tanpa hak mentransmisikan informasi elektronik yang memiliki muatan yang melanggar kesusilaan ” ;

2. Menjatuhkan pidana terhadap Herman Joseph bin Ie Hie Soeng pidana penjara selama : 8 (delapan) bulan ;
3. Memerintahkan bahwa hukuman tersebut tidak perlu dijalani, kecuali dikemudian hari ada perintah lain dalam putusan Hakim bahwa terpidana sebelum masa percobaan : 1(satu) tahun berakhir telah bersalah melakukan perbuatan pidana ;
4. Memerintahkan barang bukti berupa :
   a) 1 (satu) buah CPU server ;
   b) 3 (tiga) buah CPU biling,No.10,15 dan 17;
   c) 1 (satu) buah CPU biling;
   d) 1 (satu) buah monitor;
   e) 1 (satu) buah mouse;
   f) 1 (satu) buah keiboard;
   g) 1 (satu) buah swit;

   Dikembalikan kepada yang berhak Herman Yoseph Bin Ie Hie Soeng ; -1(satu) buah Flashdish tanpa tutup merk multech warna biru dirampas untuk dimusnahkan.
5. Membebankan terdakwa untuk membayar biaya perkara sebesar Rp.2.000,- (dua ribu rupiah) ;

Analisis Kasus

Ketika di Tempat Kejadian Perkara penyidik melakukan oleh Tempat Kejadian Perkara dengan dibuatkan Berita Acara Olah TKP dengan tahapan yang dilakukan terhadap barang bukti elektronik sebagai berikut:

1. Tempat Kejadian Perkara
    a. Pemotretan dan video terhadap barang bukti elektronik dan posisinya;
    b. Barang bukti elektronik dilakukan pengambilan dengan prosedur teknis;
    c. Dibuatkan Berita acara tindakan pengambilan barang bukti elektronik
    d. Dibuatkan surat perintah Penggeledahan barang bukti elektronik;
    e. Dibuatkan Berita Acara Penggeledahan barang bukti elektronik;
    f. Dibuatkan Surat Perintah Penyitaan barang bukti elektronik;
    g. Dibuatkan Berita Acara Penyitaan barang bukti elektronik;
    h. Dibuatkan Surat Tanda Penerimaan terhadap pemilik barang bukti elektronik;
    i. Pemohonan Penetapan Persetujuan Penggeledahan yang ditunjukan kepada Pengadilan Negeri;
    j. Permohonan Penetapan Persetujuan Penyitaan yang ditunjukan kepada Pengadilan Negeri;
    k. Penetapan Pengadilan;

l. Dibuatkan Surat Perintah Pembungkusan dan Penyitaan Barang bukti;

m. Dibuatkan Berita Acara Pembungkusan dan Berita Acara Permintaan Serah Terima barang bukti elektronik;

n. Diserahkan ke laboratorium forensik disertai dengan tanda terima, kemudian dibuatkan Surat Perintah Periksa kepada pemeriksa terhadap barang bukti elektronik;

2. Setelah barang bukti elektronik diterima oleh pemeriksa, barang bukti dicatat spesifikasinya seperti merk, model, nomor seri, serta ciri fisik lainnya, setelah itu barang bukti difoto dan diberi label sesuai dengan nomor barang bukti yang tercatat secara elektronik di manajemen Barang Bukti Digital (*Incident Mangemnt Suite cyber Crime Investigation Center*).

Penyidik dalam proses pengambilan, penyitaan serta pemeeriksaan barang bukti elektronik memperhatikan rantai serah terima barang bukti elektronik dengan menelaah bukti-bukti yang didapat dari sumber yang dikatakan original yang nantinya diajukan untuk proses hukum. Untuk menjaga integritas penanganan barang bukti maka dalam teknis pemeriksaan diserahkan naskah control dokumen, yang beriisikan tanggal dan paraf petugas penerimaan barang bukti elektronik serta pemeriksa barang bukti digital untuk menjelaskan apa saja yang dilakukan serta tanggal berapa barang bukti tersebut diterima. Denagan demikian *chain of custody merupakan dokumentasi kronologis dari* barang bukti yang disita,

termasuk identitas setiap orang yang pernah memegang barng tersebut dan lokasinya dari mulai pengumpulan hingga penyelidikan dari barang bukti tersebut menjadi jelas. Pengumpulan barang bukti elektronik di Tempat Kejadian Perkara dialakukan oleh penyelidik.

Bukti elektronik memang memiliki karakter yang unik, yaitu bentukanya yang elektronik, dapat digandakan dengan mudah , dan sifatnya yang mudah untuk dirubah. Oleh karenanya penanganan bukti elktronik, yaitu bagaimana bukti elktronik itu dapat diahdirkan ke muka persidangan secara autentik dan dapat dipresentasikan atau tidak rusak merupakan suatu hal yang amat penting. Proses ini merupakan sebuah proses yang berkelanjutan mulai dari tahap penggeledahan hingga tahap penyitaan dan diahdirkanya bukti elektronik tersebut dimuka persidangan.

Untuk dapat diterima sebagai alat bukti atau untuk dipercaya di dalam persidangan, maka suatu pesan dan dokumen yang berisi pesan haruslah otentik. Artinya barang bukti yang berisi informasi tersebut harus terlihat sama seperti apa yang telah diajukan oleh penuntut umum yang mengajukanya sebagai alat bukti. Alat bukti yang tidak dapat diidentifikasi atau tidak diotentikan tidak dapat dianggap alat bukti yang relevan. Oleh karena itu penuntut umum yang menghadirkan alat bukti elektronik harus menunjukan kepada hakim dalam persidangan bahwa alat bukti yang diajukan adalah benar sama seperti apa yang diajukan sehingga menjadi relevan.

Sedangan pengidentifikasian barang bukti elektronik berkaitan erat dengan informasi yang terkandung dalam dokumen elektronik tersebut. Agar isi dokumen elektronik dapat diterima sebagai alat bukti atau untuk membuktikan informasi elektronik tersebut dipersidangan, maka penuntut umum yang mengajukan alat bukti tersebut harus dapat membuktikan asal-usul dan integritas informasi elektronik tersebut.

Keotentikan suatu dokumen elektronik dapat ditegakkan melalui keterangan saksi yang menjelaskan tentang:

1. Prosedur yang digunakan untuk membuat dan menyimpan atau melindungi barang bukti elektronik tersebut;
2. Mata rantai penyimpanan barang bukti elektronik setelah barang bukti tersebut diambil

Salah satu aspek yang paling penting dalam otentifiaksi adalah menjaga dan mendokumentasikan rantai (kontinuitas kepemilikan) bukti. Dengan meminimalisasi jumlah pihak yang menganai bukti elektronik dan memeliharanya, maka menunjukan bahwa bukti elektroniktidak berubah sejak dikumpulkan. Otentifikasi dapat pula berarti melihat kelayakan suatu bukti dengan melihat isi catatan tidak berubah, bahwa informasi dalam catatan sebenarnya berasal dari sumber yang diklaim, baik manusia atau mesin, adanya informasi seperti tanggal yang jelas dari dokumen informasi tersebut yang menunjukan keakuratan.

Menurut M. Ismet Karnawa, pemeriksa barang bukti elketronik diajdikan keterangan saksi dengan cara pemeriksa barang bukti elektronik

dibuatkan Berita Acara Pemeriksaan oleh Penyidik. Selanjutnya di persidangan pemeriksa barang bukti elektronik memberikan keterangan-keterangan teknis sebagai saksi dan menjelaskan proses dalam melakukan pemeriksaan barang bukti sehingga mendapatkan dokumen elektronik atau informasi elektronik.[13]

Kendala dalam proses pembuktian di persidangan adalah kurangnya pemahaman secara teknis mengenai moodus operandi tindak pidan tersebut dan juga barang bukti elektronik yang menyimpan informasi elektronik seabagai alat bukti elektronik. Oleh karena itu, peranan ahli sangat penting dan dibutuhkan dalam persidangan. Ahli dalam proses persidangan dapat menjelaskan secara rinci dan detail mengenai pemahaman teknis tindak pidana tersebut sehingga memakan waktu jalannya persidangan.[14]

Dalam penyelesaian perkara pidana menurut hukam acara pidana, proses selanjutnya ialah menyelesaikan suatu perkara pidana yaitu pembuktian di sidang pengadilan. Pada dasarnya kegiatan pembuktian dilakukan dalam usaha mencapai derajat keadilan dan kepastian hukum yang setinggi-tingginya dalam putusan hakim. Pembuktian dilakukan untuk memutus perkara terbukti atau tidak sesuai dengan apa yang telah didakwakan oleh jaksa penuntut umum.

Ada dua syarat untuk mencapai suatu hasil pembuktian agar dapat menjatuhkan pidana. Kedua syarat ini saling berhubungan dan tidak

[13] Hasil wawancara dengan M. Ismet K, Jaksa Penuntut Umum pada Kejaksaan Negeri Sleman, pada Jumaat 20 Januari 2017 Pukul 09.23 WIB

[14] *Ibid.,*

terpisahkan. Pertama, hakim harus menggunakan minimal dua alat bukti yang sah dan kedua, hakim memperoleh keyakinan (Pasal 183 KUHAP). Keyakinan hakim ini harus dibentuk atas fakata-fakta yang di dapat dari alat-alat bukti yang disebutkan pada syarat pertama, yang telah ditenyukan oleh KUHAP serta keyakinan hakim masuk kedalam ruang lingkup kegiatan pembuktian. Hakim harus mempunyai keyakinan yang mutlak atas pemeriksaan digital forensik baik yang menyangkut prsosenya maupun hasilnya.[15]

Dari kasus diatas bahwa kasus diatas sebelumnaya dilakukan operasi maya, dan dalam pembuktiannya selain menggunakan alat-alat bukti elektronik, juga dengan keterangan saksi dan keterangan ahli. Dalam kasus tersebut medatangkan keterangan saksi 5 orang yakni:

Dari kelima saksi tersebut masih kurang dalam pembuktiannya untuk membuktikan perbuatan terdakwa sehingga penuntut umum mendatangkan saksi ahli ; saksi Ahli tersebut adalah Bisyron Wahyudi, S. Si. MT, saksi ahli dalam bidang teknologi informasi, keamanan informasi, computer digital forensik investigatin, menuruut keterangan ahli Bahwa yang dimaksud dengan mendistribusikan dan/atau mentransmisikan dan/atau menbuat dapat diaksesnya infoemasi elektronik dan/atau dokumen elektronik adalah mengirimkan atau menyebarkan informasi dan/atau dokumen yang berbasis jaringan telekomunikasi dan media elektronik melalui jaringan telekomunikasi dan/atau sistem komunikasi

[15] Hasil wawancra dengan Bapak I Puthu, hakim pada Pengadilan Negeri Sleman, pada hari Rabu , 3 januari 2017, pukul 13.10 WIB

elektronik, sehingga membuat informasi dan/atau dokumen elektronik tersebut bias dibaca, dilihat, ditempilkan dan diakses oleh orang lain.

Perbuatan pemilik wanet tersebut termasuk mendistribusikan dan atau mentrnasmisikan dan atau dokumen elektronik karena pemilik warnet tersebut menyediakan fasilitas bagi pelanggannya untk bisa melakukan interaksi dengan system elektronik baik secara berdiri sendiri atau dalam jaringan yang memungkinkan file porno yang tersimpan didalam komputernya bisa dibaca dilihat dan ditampilkan .

Dengan pihak pemilik menyimpan file-file yang bermuatan porno grafi berupa gambar serta BF(Blue Film) baik di CPU billing, CPU Pengguna dan CPU Server tersebut maka menjadikan filefile tersebut bisa diakses oleh konsumen warnet baik secara langsung pada CPU Pengguna maupun melalui jaringan computer yang menghubungkan CPU Penggugat dengan CPU Billing maupun CPU Server.

File yang bermuatan pornografi berupa gambar serta BF tersebut mengsndung gambar, sketsa, ilustrasi, foto, tulisan, suara, bunyi, gambar bergerak yang memuat kecabulan atau eksploitasi seksual yang melanggar norma kesusilaan dalam masyarakast, termasuk melanggar UU ITE.

Pemilik /pengelola warnet sebagai pihak yang bertanggung jawab atas file-file yang ada pada CPU baik server, pengguna maupun billing yang ada kaitannya dengan pornografi karena berada dalam kekeuasaan nya ; Bahwa suatu gambar atau film porno bida masuk kejaringan komputer yang tersimpan dalam CPU server dalam download user akibat

tindakan manusia secara sengaja yang bisa dilakukan oleh pemioik warnet ataupun pengguna warnet dengan cara mengunduh dari internet atau menyalin dari media elektronik lainnya seperti flashdisk, CD/DVD, hardisk portable dan file porno bisa disimpan dalam hardisk komputer wanet yang terhubung dengan jaringan yang tersedia serta media penyimpanan lain ; Bahwa untuk mengetahui kapan suatu file porno tersebut disimpan dalam CPU Computer bisa dilakukan dengan melihat properties atau metadata dari file tersebut.

Dari alat bukti tersebut hakim belum dapat memperoleh keyakinan sehingga diperlukan keterangan saksi dan ahli , sehingga alat bukti elektronik tersebut tidak dapat berdiri sendiri sebagai alat bukti harus ada alat bukti lainnya untuk membuktikan tindakan terdakwa, dan hakim juga tidak terikat dengan alat bukti elektronik tersebut, sehingga kekuatan alat bukti tersebut bersifat bebas.

Dari kedua kasus diatas dapat kita bandingkan bahwa penggunaan alat bukti elektronik dari satu perkara dengan perkara yang lain berbeda, hal ini tergantung bagaimana penggunaan dari alat bukti terhadap tindak pidana diatas, untuk suatu bukti elektronik yang dalam bentuk digital harus diprin-out terlebih dahulu, sedangkan untuk alat bukti elektronik dalam bentuk barang seperti obyek yang dilakukan maka alat bukti tersebut menjadi petunjuk.

Alat bukti elektronik dalam pembuktian Tindak pidana *cybercrime* meamang sangat penting dalam mengungkap suatu kejahatan tersebut

namun dalam persidangan hakim masih tetap berpatokan dengan dua alat bukti dan keyakinan hakim. Alat bukti elektrinik dalam pembuktian tindak pidana *cybercrime* harus diupayakan keotentikanya agar memberikan keyakinan kepada hakim tentang kejahtan tersebut. Sehungga hakim tidak salah dalam memutuskan suatu perkara tindak pidana *cybercrime* tersebut,