JURNAL SOSTEKMAS:
Jurnal Ilmu Sosial, Teknologi, dan Pengabdian Masyarakat
jurnal.sostekmas@um-tas.com

PENERAPAN ALAT BUKTI DALAM TINDAK PIDANA INFORMASI DAN TRANSAKSI ELEKTRONIK

Malisya Putri

STIH - BENHUR

Melisyaputri12@gmail.com

ABSTRAK

Seiring dengan semakin pesatnya perkembangan komunikasi melalui internet, memunculkan pula berbagai kejahatan yang dilakukan dengan media internet. Tidak dapat dipungkiri bahwa penggunaan internet yang canggih dan cepat tersebut memunculkan pula kejahatan yang sangat canggih dan sulit untuk diketahui pelakunya. Hal ini disebabkan karena internet merupakan suatu media komunikasi yang tidak terlihat (maya), sehingga pelaku kejahatan dapat dengan mudah menghilangkan jejak tanpa dapat diketahui dengan jelas. Metode penelitian yangt digunakan adalah penelitian hukum normatif empiris. Hasil penelitian menunjukkan bahwa proses penerapan alat bukti tindak pidana ITE diawali dengan proses penyelidikan dan penyidikan, kemudian alat bukti elektronik tersebut akan dilakukan pemeriksaan melalui proses tahapan digital forensik, yaitu; Pengambilan (*acquisition*); Pemeriksaan dan analisa, dan Dokumentasi dan presentasi.

Kata Kunci: Alat Bukti, Informasi, Transaksi Elektronik

ABSTRACT

Along with the increasingly rapid development of communication via the internet, various crimes have also emerged that are committed using the internet medium. It cannot be denied that the use of the sophisticated and fast internet has also given rise to very sophisticated crimes and it is difficult to identify the perpetrators. This is because the internet is an invisible (virtual) communication medium, so that criminals can easily remove traces without being clearly identified. The research method used is empirical normative legal research. The research results show that the process of implementing evidence for ITE crimes begins with an inquiry and investigation process, then the electronic evidence will be examined through a digital forensics stage process, namely; Acquisition; Examination and analysis, and Documentation and presentation.

Keywords: *Evidence, Information, Electronic Transactions*

PENDAHULUAN

Internet merupakan sebuah dimensi baru dalam kehidupan manusia. Internet adalah sebuah alat penyebaran informasi secara global, sebuah mekanisme penyebaran informasi dan sebuah media untuk berkolaborasi dan berinteraksi antar-individu dengan menggunakan komputer tanpa terhalang batas geografis.

Perkembangan penggunaan Internet yang ditandai oleh pertumbuhan perusahaan-perusahaan penyedia jasa internet dan meningkatnya jumlah pengguna jasa ini, tidak disertai dengan perkembangan hukum di bidang ini. Demikian pula dengan perkembangan zaman,

banyak kejahatan konvensional dilakukan dengan modus operandi yang canggih dalam proses beracara diperlukan teknik atau prosedur khusus untuk mengungkap suatu kejahatan.

Seiring dengan semakin pesatnya perkembangan komunikasi melalui internet, memunculkan pula berbagai kejahatan yang dilakukan dengan media internet. Tidak dapat dipungkiri bahwa penggunaan internet yang canggih dan cepat tersebut memunculkan pula kejahatan yang sangat canggih dan sulit untuk diketahui pelakunya. Hal ini disebabkan karena internet merupakan suatu media komunikasi yang tidak terlihat (maya), sehingga pelaku kejahatan dapat dengan mudah menghilangkan jejak tanpa dapat diketahui dengan jelas.

Terlepas dari manfaat yang diperoleh dengan kemajuan teknologi di bidang komputer, belakangan muncul persoalan ketika jaringan-jaringan komputer yang dipergunakan oleh berbagai pihak tersebut disalahgunakan oleh pihak-pihak tertentu untuk kepentingan yang berseberangan, atau dikenal dengan kejahatan komputer (*computer crime*). Dalam istilah lain, kejahatan ini lebih dikenal dengan *cyber crime* atau Tindak Pidana Informasi dan Transaksi Elektronik.

Sebelum disahkannya Undang-Undang tentang Informasi dan Transaksi Elektronik, salah satu hal yang menjadi kendala dalam penanganan praktik tindak pidana dunia maya ini adalah bahwa bukti-bukti berupa *software,* data elektronik, atau data dalam bentuk elektronis *(elektronik evidence*) lainnya yang belum dapat diterima sebagai alat bukti dalam hukum Indonesia. Sebagai cabang ilmu hukum, Hukum Siber termasuk sangat baru.

Hukum Siber bertumpu pada disiplin-disiplin ilmu hukum yang telah lebih dulu ada. Beberapa cabang ilmu hukum yang menjadi pilar hukum siber adalah Hak Atas Kekayaan Intelektual, Hukum Perdata Internasional, Hukum Perdata, Hukum Internasional, Hukum Acara dan Pembuktian, Hukum Pidana Internasional, Hukum Telekomunikasi, dan lain-lain.[1]

Cyber crime memiliki sifat efisien dan cepat serta sangat menyulitkan bagi pihak penyidik dalam melakukan penyidikan terhadap tindak pidana *cyber crime* terutama dalam proses pengumpulan alat bukti. Di dalam penyidikan berdasarkan Pasal 1 angka 2 KUHAP, penyidik/polisi mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya.

Alat bukti adalah segala sesuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat-alat bukti tersebut dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan oleh terdakwa. Penyidik harus lebih dulu memperoleh atau mengumpulkan bukti permulaan atau *probable cause*, baru dapat menjatuhkan dugaan terhadap seseorang. Artinya cukup fakta dan keadaan berdasarkan informasi yang sangat dipercaya bahwa tersangka sebagai pelaku tindak pidana berdasar bukti dan tidak boleh semata-mata berdasar konklusi.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai suatu norma hukum khusus terdapat suatu prinsip-prinsip hukum yang juga baru, yang menyimpang dari sistem hukum yang ada sebagaimana diatur dalam KUHP maupun KUHAP. Salah satunya adalah mengenai alat bukti elektronik yang baru diakui sebagai suatu alat bukti

[1] http://repository.usu.ac.id/bitstream/handle/123456789/36008/10E00138.pdf?sequence=1` diakses pada tanggal 10 Maret 2023

yang sah dalam hukum pembuktian di Indonesia. Di mana sebelum Undang-Undang tentang Informasi dan Transaksi Elektronik disahkan, dalam hal pembuktian tindak pidana dunia maya ini selalu terbentur pada keterbatasan cakupan alat bukti sementara tindak pidana dunia maya ini semakin hari semakin sering terjadi dan memerlukan pembuktian yang sebenar-benarnya.

Hal lain yang perlu diperhatikan adalah upaya untuk memenuhi persyaratan hukum guna menentukan apakah seseorang yang telah menjadi tersangka itu pantas disangka telah melakukan tindak pidana *cyber crime* berdasarkan alat bukti yang sah dan cukup menurut ketentuan Perundang-undangan.

Aparat penegak hukum dihadapkan pada kesulitan untuk menentukan kualifikasi kejahatan apakah yang dapat dituduhkan pada pelaku *cyber crime* atau tindak pidana informasi dan transaksi elektronik, mengingat sukarnya menemukan serta menerapkan alat bukti. Sementara itu, pesatnya teknologi informasi melalui internet telah mengubah aktivitas-aktivitas kehidupan yang semula perlu dilakukan dengan kontak fisik, kini dengan menggunakan media informasi dan teknologi, aktivitas keseharian dapat dilakukan secara virtual atau maya. Masalah sulit yang dihadapi penegak hukum saat ini adalah bagaimana menjaring pelaku *cyber crime* yang mengusik rasa keadilan tersebut dikaitkan dengan sistem hukum acara pidana yang berlaku.

Berhadapan dengan kasus *cyber crime*, pembuktian menjadi masalah yang sulit. Seringkali penegak hukum di Indonesia mengalami kesulitan dalam menjerat pelaku *cyber crime* karena masalah pembuktian (*documentary evidence*) yang tidak memenuhi ketentuan hukum acara pidana Indonesia. Sementara upaya penjeratan terhadap pelaku-pelaku c*yber crim*e harus tetap dilakukan, upaya perluasan alat bukti serta penerapannya menjadi solusi untuk menegakkan hukum.[2]

METODE

Selaras dengan ruang lingkup dan tujuan serta permasalahan yang telah di sampaikan sebelumnya, maka peneliti menggunakan jenis penelitian hukum normatif empiris yaitu penelitian yang dilakukan atau ditujukan hanya pada peraturan-peraturan yang tertulis atau bahan hukum yang lain.

HASIL DAN PEMBAHASAN

Proses Penerapan Alat Bukti Dalam Tindak Pidana Informasi Dan Transaksi Elektronik

Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global. Di samping itu, perkembangan teknologi informasi telah menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum. Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai (user) atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer.

[2] Dikdik M. Aries Mansur Dan Elisatris, *Cyber Law, Aspek Hukum Teknologi Informasi*, (Bandung: Refika Aditama, 2005) hal 100.

UU ITE dipersepsikan sebagai *cyberlaw* di Indonesia, yang diharapkan bisa mengatur segala urusan dunia Internet (siber), termasuk didalamnya memberi *punishment* terhadap pelaku *cybercrime. Cybercrime* dideteksi dari dua sudut pandang:

1) Kejahatan yang Menggunakan Teknologi Informasi Sebagai Fasilitas: Pembajakan, Pornografi, Pemalsuan/Pencurian Kartu Kredit, Penipuan Lewat *Email (Fraud*), Email Spam, Perjudian Online, Pencurian Account Internet, Terorisme, Isu Sara, Situs Yang Menyesatkan, dsb.
2) Kejahatan yang Menjadikan Sistem Teknologi Informasi Sebagai Sasaran: Pencurian Data Pribadi, Pembuatan/Penyebaran Virus Komputer, Pembobolan/Pembajakan Situs, *Cyberwar, Denial of Service* (DOS), Kejahatan Berhubungan Dengan Nama Domain, dsb.

Cybercrime menjadi isu yang menarik dan kadang menyulitkan karena:

a. Kegiatan dunia cyber tidak dibatasi oleh teritorial Negara
b. Kegiatan dunia *cyber* relatif tidak berwujud.
c. Sulitnya pembuktian karena [illegible]ektronik relatif mudah untuk diubah, disadap, dipalsukan dan dikirimkan [illegible]n belahan dunia dalam hitungan detik.
d. Pelanggaran hak cipta dimungkinkan secara teknologi.
e. Sudah tidak memungkinkan lagi menggunakan hukum konvensional.

Penerapan Teknologi Informasi dan Transaksi Elektronik akan menimbulkan berbagai perubahan sosial. Oleh karena itu, perlu untuk diperhatikan bagaimana upaya melakukan transformasi teknologi dan industri dalam mengembangkan struktur sosial yang kondusif. Apabila partisipasi masyarakat dan peranan hukum tidak berjalan dengan maksimal, maka upaya pengembangan teknologi tidak saja kehilangan dimensi kemanusiaan tetapi juga menumpulkan tujuan yang akan dicapai.

Peranan hukum diharapkan dapat menjamin bahwa pelaksanaan perubahan itu akan berjalan dengan cara yang teratur, tertib dan lancar. Perubahan yang tidak direncanakan dengan sebuah kebijakan hukum acap kali akan menimbulkan berbagai persoalan baru dalam masyarakat. Di sinilah hukum akan berfungsi dalam menghadapi perubahan masyarakat.

Hukum acara pidana atau hukum pidana formil merupakan aturan-aturan untuk melaksanakan hukum pidana materil dalam proses peradilan pidana, mulai dari tahap penyidikan, penuntutan, persidangan, sampai pada pelaksanaan putusan pengadilan. Hukum acara pidana mengatur prosedur yang harus dilakukan oleh aparat penegak hukum dalam menjalankan kewenangannya dan mengatur tahap- tahap proses peradilan pidana. Hukum acara pidana menegaskan hak dan kewajiban para saksi, tersangka dan terdakwa dalam setiap tahap dalam proses peradilan pidana. Dengan adanya aturan yang dimaksud, diharapkan kebenaran materil dapat terungkap, keadilan dapat ditegakkan, ketertiban dapat dijaga, hak asasi manusia dapat dilindungi, dan penyalahgunaan wewenang dapat dihindari.

Payung hukum pidana formil yang berlaku di Indonesia adalah Undang- Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana yang disebut juga Kitab Undang-Undang Hukum Acara Pidana (KUHAP). KUHAP merupakan hukum acara untuk melaksanakan hukum pidana materil yang utamanya diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP). Dalam perkembangannya, terdapat begitu banyak undang-undang yang lahir kemudian yang memuat pengaturan dan sanksi pidana yang tidak diatur dalam KUHP.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan undang-undang yang secara khusus mengatur mengenai transaksi elektronik dan didalamnya juga diatur perbuatan-perbuatan yang dikategorikan sebagai tindak pidana siber serta sanksi pidananya.

\Penerapan alat bukti sangat erat kaitannya dengan pembuktian. Pembuktian sebenarnya telah dimulai pada tahap penyidikan. Pembuktian bukan dimulai pada tahap penuntutan maupun persidangan. Dalam penyidikan, penyidik akan mencari pemenuhan unsur pidana berdasarkan alat-alat bukti yang diatur dalam perundang-undangan. Pada tahap penuntutan dan persidangan kesesuaian dan hubungan antara alat-alat bukti dan pemenuhan unsur pidana akan diuji.

Dalam rangka penegakan hukum sesuai Sistem Peradilan Pidana, Polri bertugas melakukan penyidikan tindak pidana yang dilaksanakan oleh penyidik/ penyidik pembantu pada fungsi reserse kriminal Polri maupun fungsi operasional Polri lainnya yang diberi wewenang untuk melakukan penyidikan serta mengkoordinasikan dan melakukan pengawasan terhadap Penyidik Pegawai Negeri Sipil (PPNS). Peranan penyidik Polri dalam sistem Peradilan Pidana berada pada bagian terdepan dan merupakan tahap awal mekanisme

Penyidikan tindak pidana pada hakekatnya merupakan wujud penegakan hokum yang diatur dalam perundang-undangan mengingat tugas-tugas penyidikan tindak pidana banyak berkaitan dengan hal-hal yang menyangkut Hak Asasi Manusia (HAM). Salah satu tugas dari penyidik kepolisian adalah melakukan pemeriksaan terhadap tersangka tindak pidana. Pemeriksaan yang dilakukan oleh Penyidik dalam rangka penyidikan merupakan kegiatan untuk mendapatkan keterangan, kejelasan dan keidentikan tersangka dan atau saksi dan atau alat bukti maupun tentang unsur-unsur tindak pidana yang telah terjadi sehingga kedudukan atau peranan seseorang maupun alat bukti di dalam tindak pidana tersebut menjadi jelas dan dituangkan dalam Berita Acara Pemeriksaan (BAP).

Pada dasarnya seluruh kegiatan dalam proses hukum penyelesaian perkara pidana, sejak penyidikan sampai putusan akhir diucapkan di muka persidangan oleh majelis hakim adalah berupa kegiatan yang berhubungan dengan pembuktian atau kegiatan untuk membuktikan. Walaupun hukum pembuktian perkara pidana terfokus pada proses kegiatan pembuktian di sidang pengadilan, tetapi sesungguhnya proses membuktikan sudah ada dan dimulai pada saat penyidikan. Bahkan, pada saat penyelidikan, suatu pekerjaan awal dalam menjalankan proses perkara pidana oleh negara. Yang dimaksud dengan mencari bukti sesungguhnya adalah mencari alat bukti, karena bukti tersebut hanya terdapat atau dapat diperoleh dari alat bukti dan termasuk barang bukti.

Bukti yang terdapat pada alat bukti itu kemudian dinilai oleh pejabat penyelidik untuk menarik kesimpulan, apakah bukti yang ada itu menggambarkan suatu peristiwa yang diduga tindak pidana ataukan tidak. Bagi penyidik, bukti yang terdapat dari alat bukti itu dinilai untuk menarik kesimpulan, apakakah dari bukti yang ada itu sudah cukup untuk membuat terang tindak pidana yang terjadi dan sudah cukup dapat digunakan untuk menemukan tersangkanya.

Proses penegakan hukum Oleh Kepolisian diawali dengan proses penyelidikan. Dimana, Penyelidikan berdasarkan ketentuan Pasal 1 angka 5 KUHAP adalah serangkaian tindakan penyelidik untuk mencari dan menemukansuatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam Undang-Undang ini. Sedangkan penyelidik berdasarkan ketentuan Pasal 1 Angka 4

KUHAP adalah pejabat polisi negara Republik Indonesia yang diberi wewenang oleh Undang-Undang ini untuk melakukan penyelidikan. Setelah penyelidikan selesai makan ditingkatkan ke tahap penyidikan.

Berdasarkan Pasal 1 angka 2 KUHAP, Penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam Undang-Undang untuk mencari serta mengumpulkan bukti yang terjadi guna menemukan tersangkanya. Sedangkan penyidik diatur dalam Pasal 1 angka 1 KUHAP yang mengatur bahwa penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang- undang untuk melakukan penyidikan.

Pasal 42 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur bahwa penyidikan terhadap tindak pidana Informasi Dan Transaksi Elektronik dilakukan berdasarkan ketentuan dalam hukum acara pidana dan ketentuan dalam UU ITE. Maksudnya, semua aturan yang ada dalam KUHAP tetap berlaku sebagai ketentuan umum (*lex generalis)* kecuali yang disimpangi oleh UU ITE sebagai ketentuan yang khusus (*lex specialis*). Dengan kata lain, ketentuan-ketentuan mengenai penyidikan yang tidak diatur dalam UU ITE tetap diberlakukan sebagaimana diatur dalam KUHAP. Pengaturan ini juga selaras dengan ketentuan dalam Pasal 284 ayat (2) KUHAP yaitu bahwa terhadap semua perkara diberlakukan ketentuan KUHAP, dengan pengecualian untuk sementara mengenai ketentuan khusus acara pidana sebagaimana tersebut pada undang-undang tertentu, sampai ada perubahan dan atau dinyatakan tidak berlaku lagi. UU ITE ialah salah satu contoh dari ketentuan khusus acara pidana sebagaimana tersebut pada undang-undang tertentu dan ketentuan khusus acara pidana ini tetap berlaku sebelum ditinjau kembali, diubah atau dicabut.

Penyidik yang diberikan kewenangan untuk melakukan penyidikan tindak pidana Informasi dan Transaksi Elektronik ialah penyidik polisi Negara Republik Indonesia (penyidik Polri) dan penyidik pegawai negeri sipil tertentu di lingkungan pemerintah yang lingkup tugas dan tanggung jawabnya di bidang teknologi informasi dan transaksi elektronik. Penegasan ini selaras dengan pengaturan dalam KUHAP yang mendefinisikan penyidik sebagai pejabat polisi Negara Republik Indonesia atau pejabat pegawai negeri tertentu yang diberi wewenang khusus oleh Undang-Undang untuk melakukan penyidikan.

Pemberian kewenangan kepada polri dan pejabat pegawai negeri tertentu untuk melakukan penyidikan tindak pidana yang tidak diatur dalam KUHP, seperti yang diatur dalam UU ITE merupakan pengaturan yang umum ditemui dalam perundang-undangan Indonesia. Pada prinsipnya, kepolisian Negara Republik Indonesia merupakan alat negara utama yang berperan dalam penegakan hukum dalam penyidikan untuk semua tindak pidana.

Sedangkan pejabat pegawai negeri sipil yang mengemban fungsi kepolisian, diberikan kewenangan sebagai penyidik berdasarkan undang-undang yang menjadi kewenangannya untuk melakukan penyidikan terhadap tindak-tindak pidana tertentu. Penyidik Polri memiliki kapasitas dan kapabilitas untuk melakukan semua penyidikan. Akan tetapi, PPNS diberikan wewenang tertentu untuk melakukan penyidikan karena mereka yang dinilai ahli atau memiliki kompetensi untuk memahami tindak- tindak pidana tertentu disektornya masing-masing.

Berkaitan dengan penerapan alat bukti tindak pidana informasi dan transaksi elektronik, UU ITE telah mengatur bahwa upaya paksa yang dapat digunakan oleh aparat penegak hukum untuk memperoleh alat bukti elektronik ialah melalui penggeledahan dan penyitaan sistem elektronik atau melalui intersepsi atau penyadapan.

Aparat penegak hukum menggunakan cara penggeledahan dan penyitaan apabila penyidik sudah mengetahui secara jelas sumber alat bukti elektronik tersebut (lokasi komputer, laptop, USB, server milik tersangka, korban, atau saksi). Sedangkan berdasarkan batasan-batasan yang diatur dalam perudang- undangan, intersepsi atau penyadapan dapat digunakan oleh aparat penegak hukum sebagai cara mengumpulkan informasi dan keterangan terkait dengan suatu tindak pidana (tersangka, tindak pidana yang dipersangkakan, saksi, lokasi tindak pidana). Informasi tersebut dapat dijadikan alat bukti.

Berdasarkan sistem pembuktian di Indonesia, kesalahan terdakwa ditentukan oleh minimal dua alat bukti yang sah dan keyakinan hakim. 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 penggeledahan dan penyitaan maupun intersepsi.

Pasal 43 ayat (6) Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, menyatakan bahwa: "Dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam."

Keharusan izin dari ketua pengadilan setempat adalah dalam rangka check and balance antara aparat penegak hukum dari eksekutif dengan peradilan dari yustisi. Dengan demikian kemungkinann penyalahgunaan wewenang dapat dicegah. Ketentuan izin dalam UU ITE harus selaras dengan KUHAP, oleh karena itu penggeledahan dan penyitaan sistem elektronik harus dilakukan dengan:

a) Disaksikan minimal dua orang saksi.
b) Dibuat acara penggeledahan dan /atau penyitaan (Pasal 34 ayat (1) KUHAP).[3]

Selain itu, penyidik harus memperhatikan Pasal 43 ayat (2) UU ITE yaitu harus dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan public, intregitas data, atau keutuhan data sesuai dengan ketentuan peraturan perundang-undangan.

KUHAP telah memberikan pengaturan yang jelas mengenai upaya paksa penggeledahan dan penyitaan secara umum, tetapi belum terhadap sistem elektronik. Akan tetapi, KUHAP belum mengatur mengenai intersepsi atau penyadapan, hal ini diatur di dalam berbagai undang-undang yang lebih spesifik. Oleh karena itu, ketentuan tentang persyaratan formil dan materil mengenai alat bukti elektronik harus mengacu pada KUHAP, UU ITE, dan undang-undang lain yang mengatur secara spesifik mengenai alat bukti elektronik tersebut.

Alat bukti elektronik adalah Informasi Elektronik dan/atau Dokumen Elektronik yang memenuhi persyaratan formil dan persyaratan materiil yang diatur dalam Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Barang bukti dapat dikatakan alat bukti digital karena berbentuk Informasi Elektronik dan/atau Dokumen Elektronik yang sesuai dengan kriteria Pada Pasal 1 angka 1 dan angka 4 Undang-Undang No. 11 tahun 2008 yang meliputi 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

[3] http://eprints.ums.ac.id/30305/7/NASKAH_PUBLIKASI.pdf. Di Akses Pada tanggal 10 Juli 2023

oleh orang yang mampu memahaminya dan bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya, yang dalam putusan diatas merupakan alat bukti yang mempunyai kedudukan untuk menjelaskan suatu tindak *cyber crime* yang mungkin dilakukan oleh tersangka, sehingga alat bukti digital ini memperjelas fakta yang terjadi dengan didukung alat bukti lainnya.

Persyaratan materil ialah ketentuan dan persyaratan yang dimaksudkan untuk menjamin keutuhan data (*integrity*), ketersediaan (a*vailability*), keamanan (*security)*, keotentikan *(authennticity*), dan keteraksesan *(accessibility*) informasi atau dokumen elektronik dalam proses pengumpulan dan penyimpanan dalam proses penyidikan dan penuntutan, serta penyampaiannya di sidang pengadilan.

Persyaratan materil alat bukti elektronik diatur dalam Pasal 5 ayat (3) UU ITE, yaitu informasi atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam UU ITE. Lebih lanjut, sistem elektronik diatur dalam Pasal 15 sampai dengan Pasal 16 UU ITE dan dari kedua pasal ini, dapat diperoleh persyaratan yang lebih rinci. Persyaratan formil alat bukti elektronik diatur dalam Pasal 5 ayat (4) dan Pasal 43 UU ITE.

Pasal 6 UU ITE juga memberikan persyaratan materil mengenai keabsahan alat bukti elektronik, yaitu bahwa informasi atau dokumen elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangan suatu keadaan.

Alat bukti elektronik harus memenuhi persyaratan baik secara formil dan materil sehingga alat bukti tersebut dapat 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 yakin dengan fakta-fakta hukum yang dihadirkan melalui alat bukti elektronik.

UU ITE secara komprehensif telah mengakui alat bukti elektronik sebagai perluasan alat bukti yang ada dalam hukum acara baik pidana maupun perdata, dan sebagai perluasan alat bukti dalam hukum acara yang ada pada saat ini. Untuk dapat dipercaya sebagai alat bukti, maka dapat dilakukan dengan cara menggunakan peralatan komputer untuk menyimpan dan memproduksi print-out, proses data seperti pada umumnya dengan memasukkan inisial dalam sistem pengelolaan arsip yang dikomputerisasikan dan menguji data dalam waktu yang tepat setelah data dituliskan oleh seseorang yang mengetahui peristiwa hukum nya.[4]

Pada dasarnya seluruh kegiatan dalam proses hukum penyelesaian perkara pidana, sejak penyidikan sampai putusan adalah berupa kegiatan yang berhubungan dengan pembuktian atau kegiatan untuk membuktikan. Mencari bukti sesungguhnya adalah mencari alat bukti. Bukti yang terdapat pada alat bukti itu kemudian dinilai oleh pejabat penyelidik untuk menarik kesimpulan, apakah bukti yang ada itu menggambarkan suatu peristiwa yang diduga tindak pidana ataukah tidak. Pembuktian sendiri ialah perbuatan membuktikan,

[4] Petrus Reinhard Golose, *Seputar Kejahatan Hacking. Teori Dan Studi Kasus* (Jakarta:Yayasan Pengembangan Kajian Ilmu Kepolisian, 2008), hal 72.

membuktikan berarti memberi atau memperlihatkan bukti, melakukan sesuatu sebagai kebenaran, melaksanakan, menandakan, menyaksikan, dan meyakinkan.

Alat bukti elektronik memiliki cakupan yang luas dan jenis yang beragam. Tiap jenis alat bukti elektronik tersebut memiliki karakteristik secara teknis yang memerlukan penanganan tersendiri dalam menentukan keabsahannya secara hukum. Oleh karena itu, perlu adanya kesepahaman diantara kalangan aparat penegak hukum mengenai prinsip-prinsip pengumpulan, penganalisaan, serta penyajian alat bukti elektronik yang beragam itu. Dalam hal diperlukan, dapat ditetapkan peraturan dan putusan yang lebih spesifik yang dijadikan pedoman dalam memeriksa alat bukti elektronik baik ditingkat penyidikan, penuntutan, maupun di persidangan.

Berdasarkan penjelasan di atas, bahwa salah satu syarat materil alat bukti elektronik dapat diterima di pengadilan ialah bahwa informasi dan dokumen elektronik harus dapat dijamin ketersediaan, keutuhan, keotentikan, dan keteraksesannya. Dengan dipenuhinya persyaratan materil dan juga persyaratan formil maka alat bukti elektronik memiliki nilai yang sama. Untuk menjamin terpenuhinya persyaratan tersebut diperlukan suatu metode ilmiah yang didukung teknologi khusus untuk memeriksa alat bukti elektronik.

Informasi elektronik atau dokumen elektronik, bila tidak ditangani dengan benar, dapat berubah, rusak atau hilang. Jika informasi tersebut hilang dan tidak dapat ditemukan kembali maka aparat penegak hukum tidak dapat memperoleh alat bukti elektronik. Jika informasi tersebut berubah atau rusak maka informasi yang dimaksud tidak dapat dijadikan alat bukti dipersidangan. Oleh karena itu, aparat penegak hukum dalam hal ini penyidik harus mencari, mengumpulkan, dan menganalisa informasi dengan cepat dan tepat.

Hal lain yang perlu diperhatikan dalam pengumpulan barang bukti yang menyimpan alat bukti elektronik ialah bahwa ada begitu banyak jenis alat dan media yang menyimpan informasi. Tidak hanya komputer, laptop, handphone, atau USB, tetapi juga router, modem, kamera digital, hardisk eksternal, CD atau DVD, serta PDA. Mengingat ada begitu banyak jenis media penyimpanan informasi dan teknologi, penanganannya memiliki karakteristik masing-masing.

Tahapan 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 yang terkait privasi seseorang yang tidak relevan dengan tindak pidana. Semua informasi yang tidak relevan tidak boleh diungkap di pengadilan. Dalam pengumpulan dan pemeriksaan alat bukti elektronik, banyak kasus di Indonesia, penyidik memerlukan kerjasama dengan penyelenggara telekomunikasi.

Berdasarkan informasi yang ia peroleh, penyidik harus menghubungi penyelenggara telekomunikasi yang dimaksud untuk memperoleh rekaman transaksi elektronik *(log file*) dari modem yang digunakan. Selain itu, penyelenggara juga dapat memberikan informasi mengenai identitas yang diberikan oleh pengguna layanan telekomunikasi pada waktu mendaftar SIM Card untuk pertama kalinya.

Alat bukti elektronik, sebagai alat bukti yang sah dalam pembuktian perkara pidana, tentu berbeda dengan alat-alat bukti lainnya, semisal surat ataupun saksi, yang dapat dengan mudah dilihat, dibaca dan dinilai kekuatannya pembuktian secara langsung.

Bukti elektronik, sebagaimana perkembangan teknologi informasi dengan berbagai karakteristiknya, tidak saja dari segi formalitasnya (cara memperoleh) maupun dari segi materiilnya (melihat nilai pembuktiannya) agar mempunyai kekuatan pembuktian dipersidangan, *reability* (dapat dipertanggungjawabkan keabsahannya), *necessity* (diperlukan untuk pembuktian) dan *relevance* (relevan dengan pembuktian). Sebagai salah satu alat bukti yang sah, karakteristik dari bukti elektronik memerlukan penanganan yang khusus pula.

UU ITE tidak mengatur perihal cara atau metode yang digunakan untuk mengumpulkan atau mengamankan, menampilkan, atau menjamin keutuhan informasi alat bukti elektronik karena pada dasarnya, UU ITE menganut sas netral teknologi. Maksudnya, cara atau metode pengumpulan dan pengamanan alat bukti elektronik dapat menggunakan teknologi yang tersedia sepanjang dapat memenuhi persyaratan keabsahan alat bukti elektronik.

Digital forensik yang juga dikenal dengan nama Computer Forensik adalah salah satu subdivisi dari ilmu forensik yang melakukan pemeriksaan dan menganalisa bukti legal yang ditemui pada computer dan menyimpan media digital, misalnya falshdisk, hardisk, CDROM, pesan email, gambar, atau bahkan, sederetan paket atau informasi yang berpindah dalam suatu jaringan computer.[5]

Dalam menangani bukti elektronik sehingga dapat diterima di persidangan adalah terpenuhinya prinsip-prinsip dasar sebagaimana yang telah dikeluarkan oleh *Association of Chief Police Officers (ACPO*) yang memberikan empat prinsip dalam penanganan alat bukti elektronik

Secara umum, digital forensik dapat dibagi menjadi :

a) Komputer forensik, yaitu forensik yang dilakukan terhadap komputer, laptop, atau hardisk dan media penyimpanan sejenis.
b) Mobile forensik, yaitu forensik yang dilakukan terhadap telepon genggam.
c) Audio forensik, yaitu forensik yang dilakukan terhadap suara.
d) Image forensik, yaitu forensik yang dilakukan terhadap gambar.
e) Video forensik, yaitu forensik yang dilakukan terhadap video dan CCTV.

Komponen pada digital forensik pada umumnya hampir sama dengan bidang yang lain. Komponen ini mencakup manusia *(people*), perangkat/peralatan *(equipment*) dan aturan (protocol) yang dirangkai, dikelola dan diberdayakan sedemikian rupa dalam upaya mencapai tujuan akhir dengan segala kelayakan dan kualitas.

Manusia yang diperlukan dalam komputer forensik merupakan pelaku yang tentunya mempunyai kualifikasi tertentu untuk mencapai kualitas yang iinginkan. Belajar forensik tidak sama dengan menjadi ahli dalam bidang forensik. Dibutuhkan lebih dari sekedar pengetahuan umum tentang komputer, tetapi juga pengalaman *(experience*) disamping berbagai pelatihan *(training*) pada materi-materi digital forensik yang telah ditempuh dan dibuktikan dengan sertifikat- sertifikat pendukung. Ada tiga kelompok sebagai pelaku digital forensik :

1) Collection Specialist, yang bertugas mengumpulkan barang bukti berupa digital *evidence.*
2) Examiner, tingkatan ini hanya memiliki kemampuan sebagai penguji terhadap media dan mengekstrak data.

[5] https:www.google.co.id/amp/s/aprilinaputri19.wordpress.com/2013/09/30/mengenal- lebih-tau-tentang-forensik-it-cyber-crime/amp. Diakses Pada tanggal 10 Juli 2023

3) Investigator, tingkatan ini sudah masuk kedalam tingkatan ahli atau sebagai penyidik.[6]

Berdasarkan prinsip ACPO yang telah dijelaskan di atas, prosedur digital forensik terbagi tiga tahap besar, yaitu :

a) Pengambilan (*acquisition*)
b) Pemeriksaan dan analisa
c) Dokumentasi dan presentasi

Melalui prinsip-prinsip dan tahapan dalam digital forensik, maka bukti elektronik akan sangat berperan dalam proses pembuktian dalam perkara pidana, dimana yang hendak dicari adalah kebenaran materiil. Beberapa hal yang dapat diungkap dan dibuktikan dengan bukti elektronik, adalah dapat mengidentifikasikan obyek (bukti elektronik), menentukan keterkaitan bukti elektronik dengan pelaku yang diduga melakukan tindak pidana, merekonstruksi masa lalu, melindungi yang tidak salah dan untuk menyiapkan ahli di persidangan.

Hal ni tidak lepas dari pengertian digital forensik sebagai salah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang ditemui pada komputer dan media penyimpanan digital. Menjabarkan keadaan kini dari suatu artefak digital yang dapat mencakup sebuah sistem komputer, media penyimpanan (seperti flash disk, hardisk, atau CD-ROM), sebuah dokumen elektronik (misalnya sebuah pesan email atau gambar JPEG), atau bahkan sederetan paket yang berpindah dalam jaringan komputer. Sehingga isi dari bukti elektronik yang diperoleh dari proses bukti elektronik tidak sekedar ada informasi apa dalam bukti elektronik akan tetapi dapat pula merinci urutan peristiwa yang menyebabkan terjadinya situasi terkini.

Proses penerapan alat bukti dalam tindak pidana infromasi dan transaksi elektronik di Kepolisian dimulai dari proses penyelidikan dan penyidikan. Penyelidikan maupun penyidikan tindak pidana cybercrime dilakukan setelah adanya laporan maupun pengaduan masyarakat terlebih dahulu kalau tindak pidana tersebut delik aduan contohnya pencemaran nama baik. Akan tetapi, kalau ia pidana umum tanpa adanya laporan aduan Kepolisian bisa saja melakukan tindakan.

Tahapan awal yang akan dilakukan dalam menangani tindak pidana Informasi dan Transaksi Elektronik adalah penyelidikan. Tujuan penyelidikan adalah untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan. Setelah penyelidikan selesai, maka tahap selanjutnya adalah melakukan penyidikan. Penyidikan dilakukan untuk mencari serta mengumpulkan bukti yang terjadi guna menemukan tersangkanya.

Pada tahap penyidikan, pihak penyidik akan melakukan penggeledahan dan penyitaan terhadap benda yang digunakan sebagai alat atau yang berhubungan dengan tindak pidana dan diduga mengandung alat bukti elektronik contohnya handphone, komputer, laptop, maupun alat komunikasi lain yang digunakan saat melakukan tindak pidana. Penggeledahan dan penyitaan tersebut dilakukan setelah meminta persetujuan penetapan sita dari pengadilan setempat dimana barang tersebut disita.

[6] http://e-dokumen.kemenag.go.id/files/VQ2Hv7uT1339506324.pdf. Di Akses Pada tanggal 12 Juli 2023

Ketika penyidik telah selesai melakukan penyidikan, penyidik wajib segera menyerahkan berkas perkara tersebut kepada Penuntut Umum. Hasil dari digital forensik tersebut yang selanjutnya akan dilimpahkan penyidik kepada Kejaksaan untuk dibawa ke Pengadilan. Apabila pada saat penyidik menyerahkan hasil penyidikan, dalam waktu 14 hari penuntut umum tidak mengembalikan berkas tersebut, maka penyidikan dianggap selesai.

Kendala yang Dihadapi Oleh Polisi Dalam Menerapkan Alat Bukti Tindak Pidana Informasi Dan Transaksi Elektronik.

Pada perkara *cyber crime* atau tindak pidana Informasi dan Transaksi Elektronik, alat bukti yang sah dan dapat diungkapkan dalam proses pembuktian ditentukan berdasarkan Pasal 5 Ayat (1) dan (2) UU ITE, yang menegaskan bahwa informasi dan atau dokumen elektronik dapat dianggap sebagai alat bukti yang sah secara hukum dalam proses pembuktian, khususnya pada perkara *cyber crime*. Alat-alat bukti tersebut merupakan perluasan dari alat-alat bukti sebagaimana diatur dan berlaku dalam hukum acara, khususnya hukum acara pidana, yakni sesuai ketentuan Pasal 184 KUHAP. Melihat ketentuan di atas, pada perkara cybercrime ini alat bukti yang digunakan adalah alat bukti yang dihasilkan dan mengandung unsur teknologi informasi.[7]

Informasi dan atau dokumen elektronik dapat dianggap sebagai alat bukti elektronik sebagaimana ditentukan sebagai perluasan alat bukti pada hukum acara pidana yang berlaku berdasarkan Pasal 5 Ayat (2) UU ITE tentang Informasi dan Transaksi Elektronik, juga terhadap alat-alat bukti tersebut dapat dilakukan penafsiran secara ekstensif/diperluas, sehingga informasi dan atau dokumen elektronik termaksud kekuatan hukum yang sama dengan alat bukti pada perkara pidana biasa sebagaimana diatur dalam Pasal 184 KUHAP.

Berdasarkan analisis di atas, maka alat-alat bukti yang ditentukan dalam Pasal 184 KUHAP dapat diterapkan pada perkara cybercrime melalui berbagai instrumen elektronik seperti informasi elektronik dan atau dokumen elektronik. Alat-alat bukti termaksud merupakan alat bukti yang sah secara hukum dan dapat digunakan pada proses pembuktian dalam perkara-perkara cyber crime, sesuai ketentuan Pasal 5 Ayat (1) dan (2) UU ITE, sehingga tidak terjadi kekosongan hukum serta diharapkan dapat mencapai kepastian hukum dan rasa keadilan.

Pembuktian alat bukti elektronik dalam perkara pidana sering ditemui kendala ketika memasukkan alat bukti elektronik ke dalam ketentuan alat bukti KUHAP dan cara untuk mengakui data elektronik sebagai alat bukti yang sah di dalam pengadilan. Namun kendala yang sangat nyata di alami oleh aparat penegak hukum, mulai dari penyidik, jaksa dan dan hakim adalah sumber daya manusia yang masih kurang tentang elektronik, sehingga di Indonesia masih jarang kita dapatkan polisi cyber, jaksa cyber dan hakim, yang seharusnya para aparat hukum cyber ini harus merata diseluruh wilayah hukum indonesia untuk memutuskan kasus cyber yang adil dan sah. Kendala lain yang dialami aparat penegak hukum adalah belum memadainya fasilitas pelengkap untuk memudahkan alat elektronik dijadikan barang bukti dalam persidangan.

[7] www.jurnal.unsyiah.ac.id/MIH/article/download/4564/3937. Di Akses Pada tanggal 12 Juli 2023

Pembuktian dalam hukum pidana merupakan sesuatu yang sangat vital perannya, mengingat dalam KUHAP (Kitab Undang-Undang Acara Pidana) peran suatu bukti sangat berpengaruh kepada pertimbangan hakim. Setiap kendala yang muncul membuat penegak hukum menjadi bingung untuk menyimpulkan suatu perkara dalam bidang Teknologi Informasi, yang mana bentuk barang bukti berbentuk digital.

Secara umum, kendala yang dihadapi oleh aparat penegak hukum dalam menerapkan alat bukti tindak pidana Informasi dan Transaksi Elektronik;

1) Kelemahan lain ada pada perangkat digital forensik (lab komputer forensik Mabes POLRI) yang belum dimiliki secara menyeluruh oleh POLRI di setiap daerah, mengingat penting keberadaannya dalam mencegah, maupun menangani kasus-kasus yang berkaitan dalam Cyber Crime.
2) Kejahatan dunia maya ini sering melibatkan antar negara (transnasional) dan tidak mengenal batas wilayah *(borderless*), dan diluar yuridiksi hukum Indonesia, dalam hal ini Polisi atau interpol kesulitan dalam melakukan penindakan dan pemeriksaan terhadap pelaku/operator yang sangat cerdik dalam menjalankan setiap modus kejahatannya.
3) Masih kurangnya sumber daya manusia dalam hal pengetahuannya tentang teknologi digital, kode-kode digital ditingkat POLRI, jaksa, hakim, sehingga dalam menangani tindak pidana dunia mayamengalami hambatan dalam pembuktian.
4) Masih lemahnya peraturan Undang-Undang yang mengatur tindak pidana dunia maya, dan faktor ini yang dapat dimanfaatkan oleh para pelaku tindak pidana dunia maya untuk mencari celah-celah hukum agar lolos dari jerat hukum.[8]

Adapun kendala yang dihadapi oleh penyidik di Kepolisian dalam menerapkan alat bukti tindak pidana Informasi dan Transaksi Elektronik adalah :

a. Kendala Internal, yaitu Kurang memadainya peralatan di SUBDIT II/ Unit Cyber Crime
b. Kendala Eksternal, yaitu :

1) Alat bukti yang terdapat dalam komputer mudah terhapus dan hilang sehingga sulit untuk dilakukan *clauning.*
Hal ini menjadi salah satu kendala yang dialami oleh pihak kepolisian dalam mengumpulkan alat bukti tindak pidana informasi dan transaksi elektronik disebabkan karena Dokumen yang telah dihapus oleh pemilik akun tidak bisa di munculkan kembali kecuali pemilik akun itu sendiri.

2) Pelaku menggunakan identitas palsu
Kendala lain yang dialami oleh pihak kepolisian dalam mengumpulkan alat bukti dalam tindak pidana informasi dan transaksi elektronik yaitu mayoritas pelaku menggunakan identitas palsu. Dimana, sebelum melakukan tindak pidana informasi dan transaksi elektronik, pelaku akan membuat akun dengan menggunakan identitas palsu. Hal ini menyebabkan pihak kepolisian mengalami kesulitan dalam melacak dan mengetahui dimana keberadaan pelaku berada.

[8] http://e-journal.uajy.ac.id/5962/2/HK110266.pdf. Di Akses Pada tanggal 14 Juli 2023

SIMPULAN DAN SARAN

Simpulan

Proses penerapan alat bukti tindak pidana ITE diawali dengan proses penyelidikan dan penyidikan. Dimana, pada tahap penyidikan pihak kepolisian akan melakukan penggeledahan dan penyitaan terhadap alat bukti elektronik. Kemudian alat bukti elektronik tersebut akan dilakukan pemeriksaan melalui proses tahapan digital forensik, yaitu; Pengambilan (*acquisition*); Pemeriksaan dan analisa, dan Dokumentasi dan presentasi.

Alat bukti yang telah diperoleh tersebut, setelah dilakukan penggeledahan dan penyitaan, serta dilakukan pemeriksaan melalui proses digital forensik di laboratorium forensik Kepolisian, selanjutnya pihak penyidik akan meminta keterangan ahli. Pihak penyidik akan meminta Keterangan ahli tentang alat bukti elektronik yang telah diperoleh sebelumnya apakah memiliki keterkaitan dengan tindak pidana informasi dan elektronik yang telah terjadi. Setelah memperoleh keterangan ahli, penyidik juga akan meminta keterangan dari saksi yang melihat, mendengar ataupun mengalami langsung peristiwa yang diduga sebagai tindak pidana infomasi dan transaksi elektronik tersebut.

Kendala yang dihadapi oleh penyidik dalam menerapkan alat bukti tindak pidana Informasi dan Transaksi Elektronik adalahh kendala internal, yaitu kurang memadainya peralatan di Unit *Cyber Crime*, dan kendala eksternal, yaitu :alat bukti yang terdapat dalam komputer mudah terhapus dan hilang sehingga sulit untuk dilakukan *clauning, kemudian* pelaku menggunakan identitas palsu.

Saran

Diharapkan Kepolisian dapat mengomptimalkan kinerja dalam penerapan alat bukti tindak pidana Informasi dan Transaksi Elektronik, tentunya harus sesuai dengan prosedur yang telah ditetapkan, karena berdasarkan alat bukti tersebut sangat menentukan terbitnya suatu putusan berkeadilan, asal saja alat bukti, kemudian penerapan alat bukti dalam tindak pidana Informasi Dan Transaksi Elektoronik dapat berjalan dengan efektif dan efisien.

UCAPAN TERIMA KASIH

Rasa terima kasih sebanyak-banyaknya penulis ucapkan kepada kedua orangtua, bapak Rektor STIH – BENHUR, para dosen dan pembimbing dari penelitian ini, sehingga selesainya penelitian saya ini.

DAFTAR PUSTAKA

Andi Sofyan dan Abdul Asis, 2014, *Hukum Acara Pidana*, Jakarta: Prenadamedia Group.

Budi Suhariyanto, 2013, *Tindak Pidana Teknologi Informasi (cybercrime):Urgensi Pengaturan dan Celah Hukumnya*, Jakarta:Rajawali Pers.

Burhan Ashshofa, 1998, *Metode Penelitian Hukum*, cet. 2, Jakarta: PT Rineka Cipta.

Dikdik M. Aries Mansur Dan Elisatris, 2005, *Cyber Law, Aspek Hukum Teknologi Informasi*, Bandung: Refika Aditama.

Eddy O.S Hiariej, 2012, *Teori dan Hukum Pemb*uktian , Jakarta: Penerbit Erlangga.

M. Yahya Harahap,1998, *Pembahasan Permasalahan dan Penerapan KUHAP*, Jakarta Pustaka kartini cetakan ke-2.

M. Husein Harun, 1991, *Penyidik Dan Penuntut Dalam Proses Pid*ana, Jakarta ɜka Cipta.

Nurdin dan Usman, *Konteks Implementasi Berbasis Kurikulum*, Grasindo, Jakarta,

Ngani Nico,I. Nyoman Budi Jaya dan Hasan Madani, 1984, *Mengenal Hukum Acara Pidana: Bagian Umum dan Penyidikan,* Yogyakarta: Liberty.

Petrus Reinhard Golose, 2008, Seputar Kejahatan Hacking. Teori Dan Studi Kasus Jakarta:Yayasan Pengembangan Kajian Ilmu Kepolisian

Sanipah Faisal, 1990, *Penelitian Kualitatif Dasar-Dasar dan Aflikasinya*, YA3, Malang.

Solichin Abdul Wahab, 2002, *Analisis Kebijaksanaan Dari Formulasi Ke Implementasi Kebijaksanaan Negar*a, Sinar Garfika, Jakarta.

Sri Mamudji, et al., 2005, *Metode Penelitian dan Penulisan Huk*um, Jakarta: Badan Penerbit

Undang-Undang Nomor 8 Tahun 1981 Tentang *Kitab Undang-Undang Acara Pidana.*

Undang-Undang Nomor 11 Tahun 2008 tentang *Informasi dan Transaksi Elektronik.*