JURNAL LITIGASI

Available online at: http://journal.unpas.ac.id/index.php/litigasi

JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

PERANAN ILMU DIGITAL FORENSIK TERHADAP PENYIDIKAN KASUS PERETASAN WEBSITE

SYNTHIANA RACHMIE
Fakultas Hukum Universitas Pasundan (UNPAS), Jl. Lengkong Besar No. 68 Bandung 40261, Telp: 022-4262226, Fax: 022-4217343, Hp: 08122451991, E-mail: synthiana.rachmie@unpas.ac.id

Abstrak

Digital forensik merupakan bagian ilmu forensik yang digunakan untuk penyelidikan dan penyidikan suatu perkara dalam investigasi materi (data) yang dan penemuan konten perangkat digital. Fokus penelitian ini bertujuan untuk mengkaji penerapan ilmu digital forensik yang dilakukan oleh penyidik dalam mendukung proses identifikasi suatu perkara untuk mencari alat bukti dengan waktu yang relatif cepat dan tepat, serta mengungkapkan alasan dan motivitasi atas tindakan yang dilakukan oleh pelaku. Metode penelitian dalam artikel ini menggunakan penelitian hukum normatif dan menggunakan metode pendekatan kasus (*case approach*) serta metode pendekatan konseptual. Pada penelitian ini, penerapan ilmu digital forensik telah dilakukan oleh penyidik namun belum dapat diterapkan secara maksimal serta dalam pelaksanaannya penerapan ilmu digital forensik juga dipengaruhi oleh jenis kasus yang ditangani oleh penyidik. Dalam hal tindak pidana peretasan website, penyidik melakukan investigasi melalui penerapan ilmu jaringan/internet forensik yang dilakukan melalui pengamatan dan mengumpulkan bukti-bukti sebagai petunjuk dalam suatu jaringan/internet yang diretas oleh pelaku. Sebaiknya ilmu digital forensik dapat dikuasai dan dipelajari secara mendalam oleh setiap penyidik yang memiliki kewenangan dalam melakukan proses investigasi sebagai penunjang ilmu pengetahuan lainnya selain ilmu hukum yang tentunya telah dikuasai dan pentingnya sarana prasarana yang memadai demi terciptanya investigasi yang komprehensif.

Kata Kunci: Digital Forensik, Peretasan Website, Investigasi.

Abstract

Digital forensic is part of forensic science being used for investigation and cases inquiry in terms of digital data finding. This research focused on understanding the application of investigator's expertise on digital forensic to support identification process of a case to obtain evidence in a relatively fast and precise time and to reveal the motive and mens rea behind the act of the offender. Conceptual approach was used in this research alongside the case approach. The findings showed that digital forensic science has been applied by investigators however it cannot be maximal for it also depends on what case the investigator is working on. In the case of website hacking, investigator used internet/network forensic through surveillance and collecting evidence as leads. It is suggested that every investigator should learn and master digital forensic science to support their expertise and other non-legal knowledge and it is vital to provide sufficient facilities and infrastructures to obtain a comprehensive investigation.

Keywords : *Digital Forensic, Web Hacking, Investigation.*

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

I. PENDAHULUAN

Teknologi komunikasi merupakan satu diantara produk ilmu pengetahuan serta teknologi. Teknologi komunikasi membuat perubahan besar terhadap pola interaksi antar manusia menjadikan komunikasi dengan komunitas lain dengan lebih mudah, dalam arti komunikasi dapat dilakukan dimana saja tanpa meninggalkan, bisa dilakukan dimana saja dan kapan saja. Interaksi sosial tidak lagi terkungkung dalam sekat territorial suatu negara. Teknologi komunikasi telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Sistem tata nilai dalam suatu masyarakat berubah, dari yang bersifat lokal partikular menjadi global universal. Hal ini pada akhirnya membawa dampak pergeseran nilai, norma, moral dan kesusilaan (Mohamad and Abdul 2005)

Pada perkembangannya, pemanfaatan teknologi melalui kecanggihan internet tersebut memiliki peran salah satunya sebagai media sosial bertujuan untuk mempermudah individu atau perusahaan dan organisasi untuk sharing konten-konten yang bermanfaat serta informasi terkini bersama dengan teman, keluarga, rekan kerja dan audiens termasuk target pelanggan. Menurut data statistik dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII 2019) dari total populasi sebanyak 264 juta jiwa penduduk Indonesia, ada sebanyak 171,17 juta jiwa atau sekitar 64,8 persen yang sudah terhubung ke internet dapat dikatakan juga bahwa jumlah pengguna internet di Indonesia tumbuh 10,12 persen dari tahun 2018 (APJII 2019).

Banyaknya pengguna teknologi informasi ini di samping membawa dampak positif dalam hal memudahkan komunikasi serta kepentingan lainnya antar manusia, juga penggunaan teknologi informasi ini membawa dampak negatif terhadap perkembangannya (Mohamad and Abdul 2005). Kejahatan menjadi ancaman yang lebih berbahaya dan kompleks seiring dengan adanya perkembangan teknologi berbasis digital. Hal ini disebabkan Signifikansi pertumbuhan teknologi sehingga proses pengungkapan kejahatan menjadi sangat

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

sulit (Iman, Susanto, and Inggi 2020) Kejahatan yang berhubungan dengan teknologi informasi secara umum dibagi menjadi dua, pertama yaitu kejahatan yang tujuannya menyerang sistem atau bahkan merusak jaringan komputer, dan kedua yaitu kejahatan komputer dan/atau perangkat digital lainnya yang menggunakan internet sebagai alat bantu dalam melancarkan kejahatan. Kejahatan tersebut dilakukan oleh para oknum yang memanfaatkan kecanggihan teknologi, menyalahgunakan ilmu pengetahuan penunjang teknologi infotmasi dan strategi serta celah pada aturan-aturan hukum yang berlaku (Hermansyah 2005)

Dalam kejahatan teknologi informasi dengan adanya kecanggihan internet dan beragam aplikasi beragam untuk melakukan peretasan jaringan dan/atau sistem komputer atau alat digital lainnya memungkinkan adanya kejahatan pada sistem serta jaringan komputer. Hal ini meniscayakan penegak hukum untuk melakukan berbagai tindakan dan menangani suatu kejahatan teknologi informasi dengan menggunakan ilmu dan aturan penunjang lainnya untuk memudahkan proses penenganan perkara tersebut. Sebagian besar negara terutama yang sistem dan norma-norma hukumnya belum menyentuh internet dan dunia siber, sedang berlomba-lomba untuk menyiapkan sistem, norma dan landasan hukum mengenai kejahatan penggunaan teknologi informasi (Faiz, Umar, and Yudhana 2017)

Seiring dengan perkembangan ilmu pengetahuan dan teknologi modern, menyebabkan penanganan terhadap kasus-kasus tindak pidana terutama dalam proses penyelidikan dan penyidikan mengalami kemajuan dan perkembangan. Diantaranya dapat dilihat dari bagaimana proses-proses penyelesaian perkara pidana dilakukan dengan penerapan ilmu penunjang lainnya oleh penyidik yang memiliki kompetensi sesuai dengan dimilikinya untuk memudahkan proses penanganan perkara tersebut.

Pada dasarnya terdapat 3 (tiga) bukti segitiga (*triangle evidence*) dalam proses penyelesaian perkara pidana yang menjadi sumber dalam pembuktian untuk mengungkap perkara pidana (H.S 2014) yaitu:

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

a. Tempat Kejadian Perkara (TKP), yaitu tempat terjadinya tindak pidana kejahatan dan/atau pelanggaran;
b. Korban adalah subjek hukum dari suatu kejahatan dan/atau pelanggaran merupakan pihak yang dirugikan oleh pelaku tindak pidana baik secara fisik, psikis maupun materi oleh pelaku kejahatan dan/atau pelanggaran, dewasa ini korban dalam tindak pidana tidak hanya manusia namun sebuah perusahaan/korporasi serta lingkungan hidup juga dapat menjadi korban dari suatu tindak pidana;
c. Barang bukti adalah benda/barang yang digunakan oleh terdakwa untuk melakukan tindak pidana atau benda/barang sebagai hasil dari suatu tindak pidana.

Selain daripada keterangan saksi dan keterangan tersangka/terdakwa yang dapat mengungkap secara cepat beberapa kejahatan/pelanggaran, barang bukti pun dapat memberikan petunjuk dan/atau membuat terang tindak pidana yang telah terjadi. Terkait dengan tindak pidana yang dilakukan secara digital menggunakan teknologi informasi sangat membutuhkan banyak barang bukti digital yang mampu menjelaskan jalannya suatu perkara pidana. Diantara beberapa ciri dari dari suatu data digital salah satunya adalah dapat secara mudah digandakan dan persis dengan data asli, sehingga perlu didalam kembali apakah data tersebut hasil dari penggandaan atau data yang asli, selain daripada itu data-data digital dengan sangat mudah dapat dirubah bakan dihilangkan. Misalnya , bila kita sedang mengakes sebuah berkas, terkadang berkas tersebut hilang ataupun tertimpa dengan berkas baru yang dapat diidentifikasi melalui waktu dan jam pada saat file tersebut diakses. Selain itu juga bila kita mengakses suatu aplikasi pada perangkat komputer maka berkas log dari aplikasi tersebut akan tertimpa dengan data atau berkas yang baru.

Dari dari keunikan yang terdapat dalam perangkat digital sebagai barang bukti dal am suatu perkara pidana yang menggunakan teknologi informasi ini,

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

pada pelaksanaan investigasi penyidik memerlukan ilmu penunjang lain untuk mencari bukti digital yang tersimpan didalam komputer yang digunakan oleh pelaku kejahatan, ilmu penunjang dimaksud salah satunya yaitu ilmu digital forensik. Diperlukan penerapan ilmu digital forensik ini untuk mengungkap fakta atau bukti yang berkaitan dengan kasus agar menjadi terang dan jelasnya suatu tindak pidana didalam persidangan. Dalam melakukan investigasi melalui digital forensik ada berbagai macam aplikasi sebagai analisis bantu yang beredar di pasar internet mulai dari aplikasi yang gratis maupun aplikasi yang berbayar, diantaranya yang terkenal yaitu Encase, Acces Data FTK, Belkasoft, Autopsy dan lain sebagainya untuk dapat melakukan pencarian alat bukti dalam proses penegakan hukum (Rizki 2018)

Digital forensik merupakan bagian ilmu forensik yang digunakan untuk penyelidikan dan penyidikan dalam investigasi materi (data) yang dan penemuan konten perangkat digital. Para Ahli mengatakan digital forensik adalah suatu rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mencari dan mengumpulkan bukti-bukti berbasis entitas maupun piranti digital sebagai alat bukti yang sah di pengadilan.

Digital forensik merupakan salah satu sarana untuk membantu penyidik dalam kewenangannya melakukan penyelidikan dan penyidikan yang diatur dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo Kitab Undang-undang Hukum Acara Pidana (KUHAP). Untuk dapat melakukan penerapan ilmu digital forensik dalam proses penyidikan perlu pemahaman yang lebih dalam mengenai ilmu teknologi selain daripada ilmu hukum yang biasa diterapkan dalam proses pengadilan pidana. Penerapan ilmu digital forensik dibagi menjadi 4 (empat) yaitu (Raharjo 2013)

1. **Forensik Komputer** yaitu penyidikan yang dilakukan terkait dengan data dan/atau aplikasi yang berada pada komputer tersebut yang didalamnya tercatat dalam berbagai berkas log;

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

2. **Forensik Jaringan/Internet** yaitu penyidikan yang dilakukan kepada data yang diperoleh berdasarkan pengamatan di jaringan;
3. **Forensik Aplikasi** yaitu penyidikan yang dilakukan dengan penggunaan aplikasi tertentu. Aplikasi tersebut memiliki fungsi audit karena aplikasi tersebut terdapat fitur untuk meninggalkan jejak suatu perangkat;
4. **Forensik Perangkat** yaitu penyidikan dengan tujuan untuk mendapatkan serta mengumpulkan data dan jejak kegiatan- kegiatan tertentu dalam suatu perangkat digital.

Untuk terciptanya penerapan ilmu digital forensik yang komprehensif diperlukan 3 (tiga) komponen terangkai yang harus dipenuhi untuk penerapan ilmu yang berkualitas. Ketiga komponen tersebut yaitu (Ruci and Ismaniah 2015).

1. Manusia (People), faktor kualitas manusia yang berpengaruh dalam proses penerapan ilmu digital forensik. Kualitas yang dibutuhkan tidak hanya mampu menggunakan computer namun diperlukan keahlian ilmu pengetahuan khusus dan pengalaman untuk dapat melakukan proses analisa menggunakan ilmu digital forensik;
2. Peralatan (Equipment), perlunya beberapa perangkat/alat untuk menunjang proses identifikasi menggunakan digital forensik untuk mendapatkan petunjuk guna menerangkan suatu perkara;
3. Aturan (Protocol), dalam komponen aturan diperlukan pemahaman secara mendalam dari sisi ilmu hukum dan pengetahuan lain seperti pengetahuan teknologi informasi untuk menunjang penerapan ilmu dapat menjadi berkualitas dan dengan aturan pula dibutuhkan untuk proses menggali, mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat.

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

Dalam proses penyidikan suatu kasus dalam hal ini kasus mengenai peretasan website, diperlukan sebuah penerapan ilmu digital forensik untuk membuat terang suatu tindak pidana tersebut. Melihat dari pembahasan tersebut, maka yang menjadi fokus dalam artikel ini adalah terkait bagaimana penerapan ilmu digital forensik dalam proses penyidikan kasus peretasan website serta bagaimana faktor-faktor yang mempengaruhi proses penerapan digital forensik dalam penyidikan peretasan website. Sehingga dapat memberikan pengetahuan sejauh mana peranan ilmu digital forensik yang digunakan dalam melakukan investigasi pada kasus peretasan website tersebut.

II. METODE PENELITIAN

1. Spesifikasi Penelitian

Penulisan ini menggunakan Metode penelitian hukum normatif. Menurut Johnny Ibrahim (Johnny 2013) proses penemuan kebenaran yang didasarkan pada logika keilmuan terutama dilihat dari sudut pandang normatif merupakan prosedur penelitian ilmiah yang menjadi ciri dari penelitian hukum normatif. Sudut pandang normatif sebagaimana dimaksud tak terbatas pada peraturan perundang-undangan *an sich*. Hal tersebut sebagaimana dikatakan oleh Peter Mahmud (Mahmud 2005). Penelitian hukum merupakan penelitian normatif akan tetapi tidak hanya meneliti hukum positivis.

Dalam penelitian hukum normatif, terdapat Logika keilmuan yang didasarkan pada disiplin ilmiah khusus dalam penelitian ini yang mengedepankan disiplin ilmiah mengenai digital forensik serta cara-cara kerja ilmu normatif, terhadap sumber-sumber hukum, peraturan perundang-undangan salah satunya Undang-undang No 8 Tahun 1981 tentang Kitab Undang-undang Hukum Acara Pidana dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Informasi dan Transaksi Elektronik, dokumen terkait seperti karya ilmiah maupun jurnal mengenai digital

JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

forensik dan beberapa buku literatur berkaitan dengan ilmu digital forensik dalam proses penyidikan suatu kasus peretasan website.

Dalam Penelitian ini pun digunakan metode pendekatan kasus (*case approach*) dengan menelaah beberapa kasus yang berkaitan langsung dengan isu hukum yang dihadapi, terutama kasus yang berkaitan dengan peretasan website, serta menggunakan pendekatan konseptual yang mengedepankan pandangan dan/atau doktrin yang berkembang mengenai digital forensik dalam ilmu hukum yang dapat menjadi pijakan untuk membangun argumentasi hukum dalam penyelesaian kasus peretasan website menggunakan ilmu digital forensik.

2. Materi Penelitian

Dalam penelitian ini , penulis berupaya menelaah peranan ilmu digital forensik yang memiliki kontribusi atau manfaat di dalam penegakan hukum pidana, salah satunya dalam melaksanakan tahapan penyidikan. Penyidik yang secara langsung melakukan proses penyelidikan dan penyidikan terhadap tersangka peretasan website merupakan Subjek dalam penelitian ini, lalu objek dalam penelitian ini adalah implementasi ilmu digital forensik dalam proses penyidikan kasus peretasan website.

3. Lokasi Penelitan

Penelitian ini berlokasi di Reskrimsus Polda Jabar Jalan Soekarno Hatta Nomor 748 Kota Bandung.

4. Sumber Data

Data sekunder yang menjadi data yang digunakan dalam penelitian khususnya dalam penelitian hukum normatif ini, terdiri dari beberapa bahan hukum diantaranya bahan primer, bahan hukum sekunder dan bahan hukum tersier. Bahan hukum Primer merupakan dokumen peraturan yang mengikat dan ditetapkan oleh pihak yang berwenang (Soedikno 2007). Bahan Hukum Sekunder dalam penelitian ini adalah bahan hukum primer yang diperoleh

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

melalui Kitab Undang-Undang Hukum Acara Pidana, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Informasi dan Transaksi Elektronik. Bahan hukum sekunder adalah semua dokumen yang berkaitan dengan penelitian ini, diantaranya termasuk tapi tidak terbatas pada jurnal-jurnal ilmu hukum dan ilmu digital forensik, karya tulis ilmah, artikel, serta beberapa sumber dari internet.

Bahan hukum tersier dalam peneltian ini adalah dokumen-dokumen yang didalamnya terdapat konsep serta keterangan yang mendukung bahan hukum primer dan bahan hukum sekunder antara lain seperti kamus, ensiklopedia atau dokumen lainnya yang relevan dengan penerapan ilmu digital forensik dalam proses penyidikan kasus peretasan website.

5. Teknik Pengumpulan Data

Studi kepustakaan (*library research*) menjadi teknik pengumpulan data yang digunakan dalam penulisan karya ilmiah ini, yaitu dengan melakukan penelitian terhadap berbagai sumber literatur bacaan ilmiah, serta wawancara tidak terstuktur yang dilakukan secara langsung kepada salah satu penyidik di Reskrimsus Polda Jabar bagian *Cyber Crime*.

6. Teknik Pengolahan Data

Terdapat tiga tahapan reduksi data dalam teknik pengolahan data yang digunakan pada penelitian yang memiliki data kualitatif ini , diantaranya proses pemilihan data, fokus pada penyederhanaan data, abstraksi data, serta transformasi data kasar yang didapatkan dari catatan-catatan tertulis di lapangan, penyajian data yang dijadikan sebagai kumpulan informasi yang tersusun sehingga dimungkinkan untuk melakukan penarikan kesimpulan atau pengambilan tindakan, serta penarikan kesimpulan yang dilakukan secara stimultan dengan tetap memperhatikan perkembangan perolehan data.

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

7. Analisis Data

Analisis data merupakan proses yang dilakukan setelah data didapatkan. Analisis data kualitatif dalam penelitian ini dilakukan dengan cara menguraikan secara deskriptif analisis serta preskriptif data-data yang telah terkumpul. Setelah itu, dari hasil analisa ini kemudian diambil kesimpulan deduktif yang berarti hendak mengambil kesimpulan khusus dari proses penelitian data dan fakta yang umum.

III. HASIL PENELITIAN DAN ANALISIS

A. Penerapan Ilmu Digital Forensik Dalam Proses Penyidikan Kasus Peretasan Website

Feri Sulianta mengatakan forensik memilki arti "membawa ke pengadilan". Istilah Forensik adalah suatu proses ilmiah dari ilmu pengetahuan dalam mengumpulkan, menganalisa, dan menghadirkan bukti-bukti dalam persidangan terkait adanya suatu kasus hukum (Feri 2008). Dalam proses penanganan tindak pidana kejahatan yang didalamnya menggunakan teknologi informasi tentunya akan membutuhkan proses investigasi forensik. Forensik merupakan suatu kegiatan kajian ilmiah yang dilakukan oleh ahli sesuai dengan kompetensinya bertujuan untuk melakukan identifikasi dan menentukan fakta-fakta yang berhubungan dengan perkara pidana dan bukti-bukti penunjang terjadinya perkara pidana dimaksud.

Analisis forensik merupakan suatu upaya penyidik dalam kewenangannya untuk memintakannya kepada ahli forensik melakukan kajian ilmiah sebagai salah satu langkah penting guna membuat terang suatu perkara pidana dalam kejahatan komputer menggunakan ilmu digital forensik yang dimiliki oleh ahli forensik tersebut. Salah satu bagian dari ilmu forensik adalah forensik digital yang cakupannya adalah penemuan atas hasil investigasi data yang telah ditemukan dalam perangkat digital seperti komputer, handphone dan lainnya. Berbeda dari forensik pada umumnya, digital forensik atau

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

komputer forensik adalah kegiatan ilmiah dalam melakukan pengumpulan serta analisa data dari berbagai sumber daya komputer atau perangkat digital lainnya yang mencakup pada sistem komputer, jaringan komputer, jalur komunikasi dalam bentuk fisik maupun non fisik, serta berbagai media penyimpanan data yang dianggap layak untuk diajukan dalam persidangan sebagai alat bukti penunjang proses penyelesaian perkara pidana. Hal tersebut memperlihatan dua bidang keilmuan yakni ilmu komputer serta ilmu hukum disatukan dalam penerapannya oleh bidang ilmu digital forensik.

Pendapat ahli mengemukakan pengertian digital forensik sebagai berikut :

1) Muhammad Nuh Al-Azhar menyatakan bahwa digital forensik adalah suatu bidang ilmu pengetahuan sekaligus teknologi komputer yang berorientasi pada kepentingan pembuktian hukum (Pro Justice), serta bertujuan untuk membuktikan kejahatan yang berteknologi tinggi atau *computer crime* secara ilmiah (*scientific*) sehingga bukti digital yang ditemukan dapat digunakan sebagai alat bukti yang sah dalam persidangan (Al-Azhar 2012);
2) Prayudi & Ashari menyatakan bahwa digital forensik merupakan suatu ilmu sekaligus metode untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi dan mempresentasikan barang bukti digital dalam rangka kepentingan proses penegakan hukum pidana dalam persidangan (Sudirman et al. 2019).
3) Menurut Lazaridis, Digital forensik adalah ilmu dan metode untuk melakukan penemuan, validasi dan interpretasi bukti digital yang ditemukan pada perangkat elektronik yang digunakan dengan kejatahan komputer (Handrizal 2017).

Ilmu digital forensik memiliki 4 (empat) prinsip dasar, yaitu (Ruuhwan, Riadi, and Prayudi 2016):

1. Data digital sebagai bukti tidak boleh dilakukan perubahan, karena

JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

keasliannya akan mempengaruhi kekuatan pembuktian hukum didalam persidangan.

2. Kompetensi orang ahli dalam melakukan analisa terhadap data digital karena akan berdampak pada tindakan yang dilakukan terhadap barang bukt data digital tersebut;
3. Terdapat standar operasional prosedur (SOP) secara teknis dan praktis mengenai langkah-langkah yang dilakukan terhadap media penyimpanan selama proses pemeriksaan terhadap data digital sebagai dasar perlakuan apabila dilakukan dikemudian hari oleh orang yang berbeda namun hasilnya akan sama dan dijamin keamanannya;
4. Tanggung jawab dari setiap orang yang terlibat dalam proses investigasi, pemeriksaan dan analisis dilakukan sesuai dengan ketentuan yang berlaku.

Digital forensik adalah suatu ilmu pengetahuan serta teknologi dibidang komputer yang bertujuan untuk mendapatkan, mengumpulkan dan menganalisa bukti-bukti digital yang dapat digunakan dalam suatu kejahatan teknologi informasi. Dalam melakukan proses investigasi kejahatan dalam teknologi informasi dapat dilakukan melalui metodologi forensik yang dibagi menjadi 2 (dua) kegiatan yaitu :

1. Search & Seizure. Investigator harus terjun langsung melakukan identifikasi, analisa bukti-bukti serta dapat melakukan penyitaan terhadap bukti-bukti untuk membantu proses penyidikan lebih lanjut sesuai dengan aturan hukum yang berlaku;
2. Pencarian Informasi dapat dilakukan oleh investigator melalui aktivitas yang tercatat dalam perangkat digital ataupun investigator dapat melakukan penyitaan media penyimpanan data untuk membantu proses penyidikan lebih lanjut (Rosalina, Suhendarsah, and Natsir 2016)

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

Setelah metodologi forensik dilakukan, investigator dapat melakukan penerapan ilmu digital forensik yang dibagi menjadi 4 (empat) (Raharjo 2013)kesemua ilmu dimaksud penerapannya harus disesuaikan dengan jenis perkara yang ditangani yaitu:

a) **Forensik Komputer** yaitu penyidikan yang dilakukan terkait dengan data dan/atau aplikasi yang berada pada komputer tersebut yang didalamnya tercatat dalam berbagai berkas log;
b) **Forensik Jaringan/Internet** yaitu penyidikan yang dilakukan kepada data yang diperoleh berdasarkan pengamatan di jaringan
c) **Forensik Aplikasi** yaitu penyidikan yang dilakukan dengan penggunaan aplikasi tertentu. Aplikasi tersebut memiliki fungsi audit karena aplikasi tersebut terdapat fitur untuk meninggalkan jejak suatu perangkat;
d) **Forensik Perangkat** yaitu penyidikan yang dilakukan untuk mengumpulkan data dan jejak atas kegiatan tertentu dalam suatu perangkat digital.

Digital forensik merupakan salah satu upaya untuk investigasi serta analisis bukti digital dari kejahatan komputer dan/atau kejahatan perangkat digital lainnya. Pada kajian ini, terdapat salah satu kasus tindak pidana yang proses penyelidikan dan penyidikannya menggunakan penerapan ilmu digital forensik yang ditangani oleh Satuan Reserse Kriminal Khusus Bagian Cyber Crime mengenai peretasan website MGHoliday (www.mgholiday.com) sebuah perusahaan distribusi hotel di Indonesia yang memiliki 6 (enam) *brand* (MG bedbank, Coorporate room deal, Room Deal, myhotelfinder.com, RajaKamar.com, dan Lalalaway) dengan sistem bisnis yang berbeda-beda. Dari hasil pemeriksaan penyidikan, pelaku mengaku Ia merupakan seorang *defacer* dan *injector* perangkat lunak ia mengaku melakukan kejahatan peretasan website tersebut karena menginginkan penetrasi dan mencari kelemahan yang terdapat dalam website MGHoliday serta ia termotivasi untuk dapat bergabung bekerja di perusahaan MGHoliday. Hal tersebut terungkap setelah

JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

penyelidikan dan penyidikan dilakukan oleh penyidik melalui metode jaringan/internet forensik.

Selanjutnya pelaku mengaku melakukan kejahatan tersebut berawal dari adanya bantuan berupa informasi akun dan password admin MGHoliday, pelaku dapat menembus sistem keamanan database melalui *tools sqlmap burp suite* yang berfungsi sebagai *remote database* maupun melakukan *extract* terhadap *database* MGHoliday dimaksud, *tools sqlmap burp suite* biasanya disalahgunakan oleh *hacker* demi mencapai tujuan yang dimaksud oleh pelaku *hacker*. Pelaku juga mengaku pada saat melakukan peretasan website MGHoliday, ia juga melakukan :

1) Mengubah password, email dan nama pengguna admin MGHoliday;
2) Melihat isi saldo admin MGHoliday untuk transaksi;
3) Melakukan reservasi hotel diseluruh negara bagian asia tenggara

Pelaku dikenakan pasal 46 ayat (1) Jo Pasal 47 Jo Pasal 30 ayat (2) dan/atau Pasal 31 ayat (2) Undang-undang Nomor 16 Tahun 2019 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Dalam hal melakukan investigasi, penyidik memerlukan penerapan ilmu digital forensik, apabila ditinjau dari kejahatan yang dilakukan maka ilmu digital forensik salah satunya yang dilakukan yaitu melalui jaringan forensik merupakan proses penangkapan, pencatatan serta analisa terkait aktivitas jaringan dalam suatu perangkat digital guna mendapatkan bukti digital (*digital evidence*) dari kejahatan yang dilakukan terhadap, atau dijalankan menggunakan jaringan komputer tersebut.

Jaringan Forensik merupakan salah satu dari ilmu forensik digital, dimana bukti didapat dari jaringan dan dianalisa berdasarkan pengetahuan dari serangan jaringan. Hal ini bertujuan untuk menemukan pelaku kejahatan dan merekonstruksi tindakan serangan penyusupan melalui jaringan. Jaringan

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

Forensik berakar dari keamanan jaringan dan deteksi penyusupan. Jaringan Forensik berkaitan dengan perubahan data dari mili detik ke mili detik. Investigasi serangan cyber atau penyusupan adalah investigasi forensik jaringan. Tantangan utama yang dihadapi dari forensik jaringan adalah bagaimana cara untuk mempertahankan keaslian bukti digital tersebut, kemudian digunakan dalam proses di pengadilan (Aji, Fadlil, and Riadi 2017).

Berdasarkan hasil penelitian wawancara terhadap salah satu penyidik di Satuan Reserse Kriminal Khusus Cyber Crime Polda Jawa Barat, untuk melaksanakan investigasi mengggunakan jaringan/internet forensik terdapat beberapa tahapan yang harus dilakukan metode ilmu jaringan forensik yaitu :

1. Akuisisi dan Pengintaian

   Proses akuisisi serta pengintaian merupakan proses untuk mendapatkan serta mengumpulkan data volatil (sistem online) dan data non-volatil (disk/perangkat terkait) dengan menggunakan berbagai perangkat penunjang lainnya. Proses akuisisi ini terdapat beberapa tahapan :

   - Pengumpulan Data Volatil yang dikumpulkan dari berbagai sumber yang ada, yakni register proses, penyimpanan data dalam bentuk virtual dan fisik, serta keadaan jaringan. Waktu yang singkat serta kritis dan mengharuskan mengambil tindakan setelah terjadi insiden, hal ini disebabkan oleh sumber informasi yang umumnya berjalan dalam periode yang singkat, karena data volatil tersebut bersifat sementara;
   - Melakukan *Trap and Trace* proses dimana hal ini diperuntukkan dalam hal monitoring *header* dari trafik internet tanpa memonitor isinya, proses ini merupakan cara non intrusif untuk menentukan sumber serangan jaringan atau untuk mendeteksi kelainan trafik karena hanya mengumpulkan header paket TCP/IP dan bukan isinya.

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

2. Analisa

   Proses Analisa merupakan proses analisis serta pendalaman data yang didapatkan dari proses sebelumnya, yang berkutat pada analisa *real-time* dari data volatil, analisa *log-file*, korelasi data dari berbagai perangkat pada jaringan yang dilalui serangan dan pembuatan time-lining dari informasi yang diperoleh. Proses analisa tersebut juga terdapat beberapa tahapan yaitu:

   - Log File sebagai Sumber Informasi

     Log file dapat merupakan sumber informasi yang penting tentang berbagai sumber daya sistem, proses-proses penggunaan perangkat digital serta aktivitas pengguna;
   - Interpretasi Trafik Jaringan

     Traffic jaringan dalam suatu perangkat digital harus dilakukan identifikasi guna mengetahui serta mengenali apabila terdapat trafik pola trafik jaringan yang tidak normal dan mencurigakan ataupun yang normal, dimana dapat dilihat dari alamat IP sumber terlihat tidak lazim (palsu) karena berupa satu set alamat IP cadangan yang biasanya digunakan di dalam jaringan sebagai alamat privat dan tidak pernah muncul di internet.

3. Recovery

   Proses *Recovery* merupakan proses untuk mendapatkan/memulihkan kembali data yang telah hilang akibat adanya intrusi, khususnya informasi pada disk yang berupa file atau direktori.

Digital forensic akan sangat membantu dalam proses pembuktian suatu kasus kejahatan secara digital. Berdasarkan Pasal 5 ayat (1) Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik bahwa Informasi elektronik dan/atau dokumen elektronik dan/atau cetaknya merupakan alat bukti hukum yang sah. Ahli digital forensik, Christopher

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

mengungkapkan dalam proses pembuktian suatu perkara terkait dengan kejahatan digital dan elektronik bukti yang asli tidak dianalisis, karena bukti tersebut harus tetap dijaga keasliannya, hal itu berbeda dengan membedah tubuh korban (Dewi 2016).

Dalam hal ini penyidik memiliki kewenangan melakukan penyidikan yang diberikan oleh Undang Undang Nomor 8 Tahun 1981 tentang Kitab Undang-undang Hukum Acara Pidana yaitu pada Pasal 2 ayat (1) penyidikan adalah serangkaian tindakan penyidik dan menurut cara yang diatur dalam Undang-undang ini untuk mencari serta mengumpulkan bukti yang terjadi dan guna menemukan tersangkanya.

Pada pelaksanaannya penyidikan dilakukan oleh pejabat polisi yang diberikan kewenangan oleh Undang-undang untuk melakukan penyidikan sesuai dengan kompetensi yang penyidik miliki. Apabila kasus yang ditangani oleh penyidik tersebut merupakan kejahatan yang menggunakan teknologi informasi maka proses penyelidikan dan penyidikan memerlukan penerapan ilmu teknologi informasi untuk dapat menerangkan suatu perkara tersebut, salah satunya menggunakan penerapan ilmu digital forensik sangat penting bagi proses penegakan hukum.

B. Faktor-faktor yang Mempengaruhi Proses Penerapan Digital Forensik dalam Penyidikan Peretasan Website

Dalam melakukan pencarian bukti-bukti digital, seorang ahli forensik tersebut harus memahami dan mengikuti prosedur-prosedur mengenai ilmu komputer dan ilmu hukum yang diakui secara nasional maupun internasional, selain itu ahli forensik juga perlu mendalami teori-teori yang berkaitan dengan bukti digital yang ditemukan baik secara online maupun yang terdapat dalam suatu perangkat, dan ahli forensik harus memahami penggunaan *software* atau aplikasi forensik untuk mencari bukti-bukti digital tersebut dengan tepat dan akurat. Sehingga ahli forensik harus memiliki ilmu yang berkompeten secara

JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

khusus dan memiliki pengalaman dalam hal melakukan investigasi ilmu digital forensik tersebut.

Pada prakteknya, mayoritas bukti digital yang digunakan oleh pelaku dalam melakukan kejahatan tersebut langsung dihapus oleh pelaku untuk menghilangkan jejaknya. Dalam proses inilah, salah satu keahlian dari seorang analis/investigator untuk dapat mendalami kembali bukti digital yang sudah hilang tersebut, serta mereka harus mampu untuk melakukan *recovery* data yang dibutuhkan tersebut untuk menjadi bukti digital yang dibutuhkan untuk menyelesaikan perkara pidana (Al-Azhar 2012). Seorang analis/investigator memerlukan keahlian yang lebih khusus mengenai komputer dan sistem jaringan lain, serta pemberian pelatihan secara langsung sehingga diharapkan penerapan-penerapan ilmu tersebut dapat menambah pengalaman disertai dengan sertifikat pendukung yang menunjukkan keahlian forensik/investigator di bidang digital. Ada tiga kelompok sebagai ahli digital forensik (Purwanti 2014).

1. *Collection Specialist* yaitu orang bertugas mengumpulkan barang bukti digital;
2. *Examiner* yaitu orang yang telah memiliki kemampuan sebagai penguji terhadap media dan mengekstrak data pada suatu perangkat;
3. Investigator yaitu orang yang pada tingkatan ini sudah masuk kedalam tingkatan ahli atau sebagai Penyidik ahli.

Pada tahap ini penyidik diharuskan memiliki kompetensi yang sesuai untuk dapat melakukan investigasi, terhadap perkara pidana yang menggunakan teknologi informasi salah satunya yaitu penyidik harus memiliki keahlian khusus dalam ilmu digital forensik yang tersertifikasi. Berdasarkan hasil penelitian di Reskrimsus Polda Jawa Barat Unit Cyber Crime masih terdapat beberapa faktor-faktor yang mempengaruhi proses penyidikan dengan menggunakan metode ilmu digital forensik, antara lain adalah :

Available online at: http://journal.unpas.ac.id/index.php/litigasi
JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

a) Masih kurangnya sarana prasarana yang dibutuhkan untuk proses penerapan ilmu digital forensik;
b) Sampai saat ini Polda Jawa Barat baru bisa menangani perkara pidana yang berkaitan dengan jaringan/internet forensik;
c) Lamanya proses sertifikasi keahlian khusus yang dikeluarkan dari lembaga yang berwenang;
d) Diperlukan waktu yang cukup lama untuk melakukan koordinasi kepada Pusat Laboratorium Forensik dan/atau Monitoring Center Forensik yang bertempat di Mabes Polri Jakarta.

Sehingga pada prosesnya akan mempengaruhi waktu yang diperlukan dalam melakukan investigasi terkait perakara pidana yang menggunakan teknologi informasi.

IV. SIMPULAN DAN SARAN

A. Simpulan

Forensik digital merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi data digital yang ditemukan pada perangkat digital untuk kepentingan pembuktian hukum. Penerapan ilmu digital forensik telah diterapkan pada proses penyelidikan dan penyidikan di lingkungan Polda Jawa Barat namun belum dapat dilaksanakan secara maksimal keseluruhan ilmu digital forensik, hal ini dipengaruhi juga dengan jenis kasus yang ditangani oleh Polda Jawa Barat, salah satu penyidik mengungkapkan dalam hal melakukan proses penyelidikan dan penyidikan mereka harus dapat mengkualifikasikan jenis tindak pidana dengan metode teknologi apa yang digunakan, hal ini mempengaruhi dalam proses investigasi yang dilakukan melalui macam-macam ilmu digital forensik. Dalam hal tindak pidana peretasan website, pihak Polda Jawa Barat melakukan investigasi melalui penerapan ilmu jaringan/internet forensik yang dilakukan melalui pengamatan dan mengumpulkan bukti-bukti

JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

sebagai petunjuk dalam suatu jaringan/internet yang diretas oleh pelaku. Serta masih terdapat beberapa faktor-faktor yang mempengaruhi proses penyidikan dengan menggunakan digital forensik, salah satu faktor penghambatnya yaitu masih terdapat kekurangan sarana prasarana yang memadai untuk dapat melakukan akses penerapan ilmu digital forensik secara keseluruhan karena Polda Jawa Barat baru dapat menangani tindak pidana yang kualifikasi penerapan ilmunya menggunakan ilmu jaringan/internet forensik saja sehingga dalam pelaksanaannya sangat mempengaruhi waktu yang diperlukan dalam melakukan proses investigasi terkait perakara pidana yang menggunakan teknologi informasi dikarenakan harus melakukan koordinasi terlebih dahulu dengan Pusat Laboratorium Forensik dan/atau Monitoring Center Forensik yang bertempat di Mabes Polri Jakarta.

B. Saran

Penerapan ilmu digital forensik sangat berguna bagi proses penyelidikan dan penyidikan untuk membuat terang suatu perkara pidana yang menggunakan teknologi informasi, sebaiknya ilmu digital forensik dapat dikuasai dan dipelajari secara mendalam oleh setiap penyidik yang memiliki kewenangan dalam melakukan proses investigasi sebagai penunjang ilmu pengetahuan lainnya selain ilmu hukum yang tentunya telah dikuasai serta selain itu sebaiknya sarana prasarana untuk melakukan investigasi di lingkungan Polda Jawa Barat. Dan dalam proses investigasi perkara pidana yang menggunakan teknologi informasi sebaiknya faktor yang menghambat berjalannya proses penerapan ilmu digital forensik dapat diminimalisir dengan cara sebagai berikut terpenuhinya kelengkapan sarana prasarana penunjang investigasi untuk perkara pidana yang menggunakan teknologi informasi; perluasan kemampuan baik dari sisi kualitas maupun kuantitas untuk dapat melakukan investigasi dengan ilmu digital forensik (Forensik Komputer, Forensik Jaringan/internet, Forensik Aplikasi dan Forensik Perangkat);

JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

diberikan kemudahan dan percepatan dalam proses sertifikasi keahlian khusus digital forensik sesuai dengan ketentuan yang berlaku; diberikan kemudahan dan percepatan dalam berkoordinasi dengan Pusat Laboratorium Forensik dan/atau Monitoring Center Forensik yang bertempat di Mabes Polri Jakarta.; adanya pelatihan yang diberikan oleh instansi terkait secara berkala untuk penyidik dalam penunjang keahlian khusus mengenai digital forensik.

DAFTAR PUSTAKA

Aji, Sukma, Abdul Fadlil, and Imam Riadi. 2017. "Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan." *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika* 3 (1): 11. https://doi.org/10.26555/jiteki.v3i1.5665.

Al-Azhar, Muhammad Nuh. 2012. *Digital Forensic Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek.

APJII. 2019. "Jumlah Pengguna Internet Di Indonesia Tembus 171 Juta Jiwa." Kompas.Com. 2019. https://tekno.kompas.com/read/2019/05/16/03260037/apjii-jumlah-pengguna-internet-di-indonesia-tembus-171-juta-jiwa.

Dewi, Ni Komang Ratih Kumala. 2016. "Digital Forensik Dalam Kasus Pembunuhan." Balipost. 2016. http://balipost.com/read/opini/2016/08/18/57582/digital-forensik-dalam-kasus-pembunuhan.html.

Faiz, Muhammad Nur, Rusydi Umar, and Anton Yudhana. 2017. "Implementasi Live Forensics Untuk Perbandingan Browser Pada Keamanan Email." *JISKA (Jurnal Informatika Sunan Kalijaga)* 1 (3): 108. https://doi.org/10.14421/jiska.2017.13-02.

Feri, Sulianta. 2008. *Komputer Forensik*. Jakarta: Elex Media Komputindo.

H.S, Brahmana. 2014. *Kriminalistik Dan Hukum Pembuktian*. Langsa: LKBH Fakultas Hukum Universitas Samudra.

JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

Handrizal, Handrizal. 2017. "Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete Dan Recuva Data Recovery Untuk Digital Forensik." *J-SAKTI (Jurnal Sains Komputer Dan Informatika)* 1 (1): 84. https://doi.org/10.30645/j-sakti.v1i1.31.

Hermansyah. 2005. *Hukum Perbankan Nasional Indonesia: Ditinjau Menurut Undang-Undang No. 7 Tahun 1992 Tentang Perbankan Sebagaimana Telah Diubah Dengan Undang-Undang No. 10 Tahun 1998, Dan Undang-Undang No. 23 Tahun 1999 Jo Undang-Undang No. 3 Tahun 2004 Tentang Bank Indon*. Kedua. Jakarta: Kencana.

Iman, Nur, Aris Susanto, and Rahmat Inggi. 2020. "Analisa Perkembangan Digital Forensik Dalam Penyelidikan Cybercrime Di Indonesia (Systematic Review)." *Jurnal Telekomunikasi Dan Komputer* 9 (3): 186. https://doi.org/10.22441/incomtech.v9i3.7210.

Johnny, Ibrahim. 2013. *Teori Dan Metodologi Penelitian Hukum Normatif*. Malang: Bayumedia.

Mahmud, Peter. 2005. *Penelitian Hukum*. Jakarta: Prenada Media Group.

Mohamad, Labib, and Wahid Abdul. 2005. *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama.

Purwanti, Indah Tri. 2014. "Digital Forensik Sebagai Alat Bukti Tindak Pidana." https://id.scribd.com/doc/231708186/Digital-Forensik-Sebagai-Alat-Bukti-Tindak-Pidana.

Budi Raharjo. 2013. "Sekilas Mengenai Forensik Digital." *Jurnal Sosioteknologi* 12 (29): 384–87. https://doi.org/10.5614/sostek.itbj.2013.12.29.3.

Rizki, Sari. 2018. "ANALISIS DIGITAL FORENSIC DALAM MENGUNGKAPKAN TINDAK KEJAHATAN CYBER PADA TAHAP PEMBUKTIAN PENDAHULUAN Tindak Kejahatan Cyber Yang Semakin Berkembang Pesat Mengharuskan Pemerintah Segera Melakukan Upaya Penanggulangan Dari Segi Peraturan Perundang-Undangan Maupun Dari Segi Kebijakan Lainnya . Pengaturan Terhadap Tindak Kejahatan Cyber Dalam Hukum Positif Di Indonesia Merujuk Kepada Undang-Undang No . 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik . Dalam Penegakan Hukum Unsur Membuktikan Dengan Kekuatan Alat Bukti Yang Sah Dalam Hukum Acara Pidana Merupakan Masalah Yang Tidak Kalah Pentingnya Untuk Diantisipasi Di Samping Unsur Kesalahan Dan Adanya Perbuatan Pidana . Undang-Undang No . 8 Tahun 1981 Tentang Hukum Acara Pidana Yang Selanjutnya Disebut KUHAP , Pada Pasal 184 Menyebutkan Tentang Alat

JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

Bukti Yang Sah Terdiri Dari : Alat Bukti Surat Merupakan Alat Bukti Yang Paling Berkaitan Dengan Bahan Komputer . Para Ahli Mengatakan Surat Merupakan Tulisan Yang Diartikan Sebagai Setiap Tanda-Tanda Baca Yang Dapat Dimengerti Yang Bertujuan Untuk Mengungkapkan Isi Pikiran . Permasalahannya Adalah Tidak Semua Orang Dapat Membaca Dan Mengerti Tulisan Dari Kode Komputer . Maka Suatu Mekanisme Ilmiah Yang Disebut Dengan Ilmu Forensik Sangat Diperlukan Dalam Rangka Mencari Bukti Yang Ada . Dalam Undang-Undang No 11 Tahun 2008 (Undang-Undang ITE) Bukti Digital Disebut Dengan Informasi Elektronik Dan Dokumen Elektronik Sebagaimana Disebutkan Pada Pasal 5 Ayat (1) Dan Ayat (2). Pasal 5 Berbunyi : (1) Informasi Elektronik Dan / Atau Dokumen Elektronik Dan / Atau Hasil Cetak Nya Merupakan Alat Bukti Hukum Yang Sah . (2) Informasi Elektronik Dan / Atau Dokumen Elektronik Dan / Atau Hasil Cetak Nya Sebagaimana Dimaksud Ayat (1) Merupakan Perluasan Dari Alat Bukti Yang Sah Sesuai Dengan Hukum Acara Yang Berlaku Di Indonesia . Lebih Lanjut Dalam Pasal 1 Ayat (1), Informasi Elektronik Adalah : ' Satu Atau Sekumpulan Data Elektronik , Termasuk Tetapi Tidak Terbatas Pada Tulisan , Suara , Gambar , Peta , Rancangan , Foto , Electronic Data Interchange (EDI), Surat Elektronik (Electronic Mail), Telegram , Teleks , Telecopy Atau Sejenisnya , Huruf , Tanda , Angka , Kode Akses , Simbol , Atau Perforasi Yang Telah Diolah Yang Memiliki Arti Atau Dapat Dipahami Oleh Orang Yang Mampu Memahaminya .'" 2 (November): 780–87.

Rosalina, Vidila, Andri Suhendarsah, and M Natsir. 2016. "Analisis Data Recovery Menggunakan Software Forensic : Winhex and X-Ways Forensic." *Jurnal Pengembangan Riset Dan Observasi Sistem Komputer* 3 (1): 51–55.

Ruci, Meiyanti, and Ismaniah. 2015. "Perkembangan Digital Forensik." *Jurnal Kajian Ilmial UBJ* 15 (September 2015).

Ruuhwan, Ruuhwan, Imam Riadi, and Yudi Prayudi. 2016. "Analisis Kelayakan Integrated Digital Forensics Investigation Framework Untuk Investigasi Smartphone." *Jurnal Buana Informatika* 7 (4): 265–74. https://doi.org/10.24002/jbi.v7i4.767.

Soedikno, Mertokusumo. 2007. *Mengenal Hukum (Suatu Pengantar)*. Yogyakarta: Liberty.

Sudirman, Asep, Bambang Sugiantoro, Yudi Prayudi, S Si, and M Kom. 2019. "Kerangka Kerja Digital Forensic Readiness Pada Sebuah Organisasi (Studi Kasus : Pt Waditra Reka Cipta Bandung)" 2 (2): 82–88.

Available online at: http://journal.unpas.ac.id/index.php/litigasi

JURNAL LITIGASI (e-Journal), Vol. 21 (1) April, 2020, p.104-127
DOI: http://dx.doi.org/10.23969/litigasi.v21i1.2388

PERATURAN PERUNDANGAN

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UndangUndang Nomor 11 Tahun 2008 Informasi dan Transaksi Elektronik.

Undang Undang Nomor 8 Tahun 1981 tentang Kitab Undang-undang Hukum Acara Pidana.