BAB 1

PENDAHULUAN

A. Latar Belakang Masalah

Teknologi merupakan suatu faktor penting dalam era globalisasi yang berkembang secara cepat dan modern. Perkembangan teknologi dilandasi dengan berkembangnya mikro elektronika, material dan perangkat lunak. Perkembangan teknolgi juga diikuti dengan berkembangnya kehidupan manusia, yaitu semua kegiatan manusia yang biasanya dilakukan dengan manual, kini dapat dilakukan dengan digital. Perkembangan teknologi saat ini membuat kehidupan masyarakat sangat tergantung dengan teknologi itu sendiri terutama yang berkaitan dengan kehidupan masyarakat umum, seperti perbankan, administrasi, proses produksi, transportasi, dan lain sebagainya. Perusahaan-perusahaan besar semakin banyak yang menggunakan fasilitas internet sebagai sarana dalam memperluas bisnis mereka.Alasan utamanya adalah karena internet dapat mempermudah para pelaku bisnis dalam melakukan transaksi dengan rekannya.Salah satu contoh adalah kontrak dagang elektronik yang dilakukan melalui internet (E-Commerce).

Julian Ding menyatakan bahwa *E-Commerce as it is also known is a commercial transaction between a vendor and a purchaser or parties in similar contractual relationship for the supply of good, services or the*

acquisition or "right"[1]. Secara singkat dapat diterjemahkan sebagai berikut: E-Commerce adalah transaksi dagang antara penjual dan pembeli untuk menyediakan barang, jasa, atau mengambil alih hak. Kontrak ini dilakukan dengan media elektroik dimana para pihak tidak hadir secara fisik. Media ini terdapat didalam jaringan umum dengan sistem terbuka yaitu internet. Transaksi ini terlepas dari batas wilayah dan syarat nasional. E-Commerce ini mempunyai berbagai dampak positif dan dampak negatif. Dampak positif dari E-Commerce ini adalah dapat menghemat waktu, tenaga dan biaya. Sedangkan dampak negatifnya adalah munculnya berbagai kejahatan internet yang sering disebut dengan *cyber crime*.

The U.S. Department of Justice memberikan pengertian *Computer Crime* sebagai: *"... any illegal act requiring knowledge of Computer technology for its perpetration, investigation, or prosecution"*[2]. Pengertian lainnya diberikan oleh *Organization of European Community Development*, yaitu: *"any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data"*[3]. *Cyber crime* atau dalam berbagai literatur sering disebut juga kejahatan komputer atau *computer crime*, kejahatan di bidang komputer[4], kejahatan telematika[5], atau kejahatan mayantara dapat diatikan juga sebagai tindak pidana apa saja yang dilakukan dengan memakai komputer (*hardware*dan *software*) sebagai sarana/alat atau komputer sebagai objek, baik

[1] Julian Ding, *e-commerce: Law and Practice, (*Malaysia, Sweet and Maxwell Asia, 1999) hlm 25
[2] H. Kadish Sanford ed., *Enscyclopedia of crime and justice volume 1*, (New York, 1983) hal 218.
[3] Widyopramono , *Kejahatan di Bidang Komputer,* Jakarta, Pustaka Sinar Harapan, 1994) hal 29
[4] Ibid.,
[5] Al. Wisnubroto., *Strategi Penanggulangan Kejahatan Telematika, (*Yogyakarta, Atma Jaya Yogyakarta 2010)

untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain, atau tindakan yang dilakukan dengan menggunakan teknologi komputer yang canggih[6].

Adanya perubahan teknolgi dan informasi telekomunikasi yang pesat tentu akan membawa perubahan yang pesat pada tingkah laku manusia termasuk juga dalam bidang hukum. Salah satunya adalah berkembangnya kejahatan dengan menggunakan internet. Contoh kejahatan dengan menggunakan internet antara lain: Pengiriman dan penyebaran virus, Pemalsuan identitas diri, penyebar-luasan pornografi, penggelapan data orang lain, pencurian data, pengaksesan data secara illegal *(hacking)*, pembobolan rekening bank, perusakan situs *(cracking)*, pencurian nomer kartu kredit *(carding)*, penyediaan informasi palsu atau menyesatkan, Transaksi bisnis illegal, *Phishing* (rayuan atau tawaran bisnis agar mau membuka rahasia pribadi), *botnet* (penguasaan software milik korban untuk kegiatan pelaku menyerang komputer lain)[7].

Seperti yang kita ketahui, tindak pidana yang menggunakan teknologi *(cyber crime)* sangat sulit untuk diproses. Hal ini disebabkan oleh berbagai faktor, diantaranya belum banyak penyidik polri yang mendapat pendidikan mengenai cara penanganan *cyber crime*, alat bukti yang digunakan dalam pembuktian sangat terbatas. Faktor-faktor yang disebutkan sebelumnya khususnya mengenai alat bukti yang terbatas kini bukan lagi menjadi kendala

[6]H Eddy Djunaedi Karnasudirdja, *Yurispundensi Kejahatan Komputer*, (Jakarta, CV. Tanjung Agung, 2005) hal. 3

[7]Kukuhkurniant,*cyber crime di Indonesia* http://kukuhkurniant.blogspot.com/2011/03/cybercrime-di-indonesia.html diakses tanggal 21 November 2011

bagi penyidik untuk mengungkap kasus c*yber crime* sejak di undangkannya UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Dalam UU ITE khususnya dalam Pasal 44 Ayat (2) disebutkan bahwa alat bukti untuk tindak pidana *cyber* adalah informasi elektronik dan/atau dokumen elektronik. Jadi untuk tindak pidana *cyber* alat bukti yang digunakan adalah alat bukti yang terdapat pada Pasal 184 UU No.8 tahun 1981 (Kitab Undang-Undang Hukum Acara Pidana) ditambah dengan informasi dan dokumen elektronik.

Dalam sistem hukum kita dikenal adanya lima macam alat bukti, seperti yang tercantum dalam Pasal 184 KUHAP, yaitu: keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Dengan adanya UU ITE data elektronik dapat dijadikan alat bukti dalam kasus *cyber*. Permasalahannya adalah bagaimana cara untuk menemukan dan menjelaskan mengenai data elektronik yang akan dijadikan sebagai alat bukti di persidangan.

Terdapat berbagai macam ilmu bantu dalam menggungkap kasus tindak pidana. Macam-macam ilmu bantu antara lain: ilmu bantu logika, psikologi, kriminalistik, kedokteran, psikiatri, kriminologi, viktimologi, penologi, dan ilmu bantu *forensic cyber.*[8] *Forensic cyber* merupakan salah satu ilmu bantu yang dapat menemukan dan menjelaskan mengenai data elektronik sebagai alat bukti di persidangan.

[8] Syaiful Bakhri, *Hukum Pembuktian dalam Praktik Peradilan Pidana,(* Pusat Pengkajian dan Pengembangan Ilmu Hukum Universitas Muhamadiah, 2009) hlm 86-89

Forensic cyber merupakan suatu disiplin ilmu baru di dalam keamanan komputer, yang membahas atas temuan bukti digital setelah suatu peristiwa keamanan komputer terjadi.[9] Komputer forensik akan lakukan analisa penyelidikan secara sistematis dan harus menemukan bukti pada suatu sistem digital yang nantinya dapat dipergunakan dan diterima di depan pengadilan, otentik, akurat, komplit, menyakinkan dihadapan juri, dan diterima didepan masyarakat[10]. Sampai saat ini belum ada aturan hukum yang mengatur mengenai *forensic cyber*. Masalah lain yang masih menjadi perdebatan adalah mengenai eksistensi *forensic cyber* dalam sistem hukum pembuktian di Indonesia.

Berdasarkan latar belakang tersebut diatas, maka penulis tertarik untuk mengangkat judul: " ***Forensic cyber* dalam pembuktian *cyber crime* di Indonesia".**

B. Rumusan Masalah

Berdasarkan latar belakang masalah diatas, untuk mengkaji secara normatif yuridis terhadap peran ilmu *forensic cyber* dalam pembuktian tindak pidana*cyber crime*, maka dapat diambil perumusan masalah sebagai berikut:

1. Bagaimanakah peran *forensic cyber* dalam pembuktian *cyber crime*?

---

[9]Deris Setiawan, *Menjadi Detective dan Ahli Forensic Dunia Cybe,* http://www.google.co.id/url?sa=t&rct=j&q=skripsi%20forensik%20cyber&source=web&cd=6&ved=0CEEQFjAF&url=http%3A%2F%2Fderis.unsri.ac.id%2Fmateri%2Fderis%2Fdetectif%2520cyber.pdf&ei=fEbKTs7iGMbSrQehuoWODg&usg=AFQjCNEgZqZa2_JPE8oph_kIvP1t9lLXUw&cad=rja diakses tanggal 21 November 2011

[10]Ibid.

2. Bagaimanakah eksistensi *forensic cyber* dalam sistem hukum pembuktian di Indonesia?

C. Tujuan Penelitian

Penelitian yang dilakukan penulis mempunyai tujuan sebagai berikut:

1. Untuk mengetahui dan mengkaji peran *forensic cyber* dalam pembuktian *cyber crime*
2. Untuk mengetahui dan mengkaji eksistensi *forensic cyber* dalam sistem hukum pembuktian di Indonesia

D. Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Memberikan sumbangan pemikiran untuk pengembangan ilmu hukum pidana khususnya berkaitan dengan pengembangan hukum pidana bidang di telematika.
2. Memberikan sumbangan pegetahuan dan memberikan pemahaman bagi penulis, masyarakat dan mahasiswa lainnya mengenai *forensic cyber* dalam pembuktian *cyber crime* di Indonesia.

E. Keaslian Penelitian

Penelitian yang akan penulis tulis belum pernah ditulis sebelumnya oleh peneliti lain. Namun ada beberapa skripsi yang senada sebagai berikut:

1. PENGGUNAAN BUKTI ELEKTRONIK DALAM PEMBUKTIAN PERKARA KEJAHATAN DUNIA MAYA

   Skripsi ini berasal dari Fakultas Hukum Universitas Gajah Mada, tahun 2008, yang ditulis oleh Nuurlaila F. Aziizah.

   Skripsi tersebut membahas mengenai bagaimana penggunaan bukti elektronik dalam pembuktian perkara kejahatan dunia maya. Sedangkan penulisan yang akan penulis tulis akan membahas mengenai peran dari *forensic cyber* dalam pembuktian *cyber crime* dan bagaimana eksistensi *forensic cyber* dalam sistem hukum pembuktian di Indonesia.

2. KEKUATAN PEMBUKTIAN KONTRAK DAGANG ELEKTRONIK (E-COMMERCE) BERTANDA TANGAN DIGITAL DALAM PERADILAN PERDATA di INDONESIA

   Skripsi ini berasal dari Fakultas Hukum Universitas Atma Jaya, tahun 2008, yang ditulis oleh Maria Rista Sekundari

   Skripsi tersebut membahas mengenai sejauh mana kekuatan pembuktian kontrak dagang elektronik yang menggunakan tanda tangan digital dalam peradilan perdara di Indonesia Sedangkan penulisan yang akan penulis tulis akan membahas mengenai peran dari

forensic cyber dalam pembuktian *cyber crime* dan bagaimana eksistensi *forensic cyber* dalam sistem hukum pembuktian di Indonesia.

3. ASPEK-ASPEK HUKUM PEMBUKTIAN PERDATA TRANSAKSI ELEKTRONIK DENGAN SISTEM PEMBAYARAN WESTERN UNION

   Skripsi ini berasal dari Fakultas Hukum Universitas Atma Jaya Yogyakarta, tahun 2007, yang di tulis oleh Theresia Indah Prasetyaningsih

   Sripsi tersebut membahas mengenai bagaimanakekuatan pembuktian elektronik record apabila terjadi perbuatan melawan hukum akibat adanya transaksi elektronik dengan sistem pembayaran western union. Sedangkan penulisan yang akan penulis tulis akan membahas mengenai peran dari *forensic cyber* dalam pembuktian tindak pidana *cyber crime* dan bagaimana eksistensi *forensic cyber* dalam sistem hukum pembuktian di Indonesia

F. Batasan konsep

Dalam penelitian ini penulis membatasi beberapa hal yang akan diteliti. Hal yang akan diteliti yaitu mengenai:

1. Pengertian peran menurut "peran" atau "role" dalam kamus oxford dictionary diartikan :*Actor's part; one's task or function*. Yang berarti

aktor; tugas seseorang atau fungsi.[11] Istilah peran dalam "Kamus Besar Bahasa Indonesia" mempunyai arti pemain sandiwara (film), tukang lawak pada permainan makyong, perangkat tingkah yang diharapkan dimiliki oleh orang yang berkedudukan di masyarakat.[12]

2. Pengertian *forensic cyber* atau sering juga disebut komputer forensik adalah suatu disiplin ilmu baru di dalam keamanan komputer, yang membahas atas temuan bukti digital setelah suatu peristiwa keamanan komputer terjadi. Komputer forensik akan lakukan analisa penyelidikan secara sistematis dan harus menemukan bukti pada suatu sistem digital yang nantinya dapat dipergunakan dan diterima di depan pengadilan, otentik, akurat, komplit, menyakinkan dihadapan juri, dan diterima didepan masyarakat[13]
3. Pembuktian

   Pembuktian menurut hukum acara pidana adalah ketentuan yang membatasi sidang pengadilan dalam usaha mencari dan mempertahankan kebenaran, baik oleh hakim, penuntut umum, terdakwa, maupun penasehat hukum.
4. Tindak pidana adalah perbuatan yang oleh aturan hukum dilarang dan diancam dengan pidana, dimana pengertian perbuatan disini selain perbuatan yang bersifat aktif (melakukan sesuatu yang sebenarnya

---

[11] Darling Kindersley, *The New Oxford Illustrated Dictionary*, (Oxford University Press, 1982) 1466

[12] Departemen Pendidikan Nasional, *Kamus Besar Bahasa Indonesia* (Balai Pustaka, Jakarta) hal 854

[13] http://www.google.co.id/url?sa=t&rct=j&q=skripsi%20forensik%20cyber&source=web&cd=6&ved=0CEEQFjAF&url=http%3A%2F%2Fderis.unsri.ac.id%2Fmateri%2Fderis%2Fdetectif%2520cyber.pdf&ei=fEbKTs7iGMbSrQehuoWODg&usg=AFQjCNEgZqZa2_JPE8oph_klvP1t9lLXUw&cad=rja diakses tanggal 21 November 2011

dilarang oleh hukum) juga perbuatan yang bersifat pasif (tidak berbuat sesuatu yang sebenarnya diharuskan oleh hukum)

5. *Cyber crime* atau dalam berbagai literatur sering disebut juga kejahatan komputer atau *computer crime*, kejahatan di bidang komputer[14], kejahatan telematika[15], atau kejahatan mayantara dapat diatikan juga sebagai tindak pidana apa saja yang dilakukan dengan memakai komputer (*hardware* dan *software*) sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain, atau tindakan yang dilakukan dengan menggunakan teknologi komputer yang canggih

G. Metode Penelitian

1. Jenis Penelitian

Jenis penelitian yang akan digunakan oleh penulis adalah normatif yang bersifat *inkronito.* Penelitian ini merupakan usaha untuk menemukan apakah hukum yang diterapkan sesuai untuk menyelesaikan perkara atau masalah tertentu, dimanakah bunyi peraturan ditemukan, Penelitian normatif ini menggunakan sumber data sekunder sebagai sumber data yang utama.

[14] Ibid.,
[15] Al. Wisnubroto., *Strategi Penanggulangan Kejahatan Telematika,* (Yogyakarta, Atma Jaya Yogyakarta. 2010)

2. Sumber Data

Berdasarkan jenis penelitiannya yaitu penelitian hukum normatif maka sumber data penelitian ini ada dua macam yaitu : data primer dan data sekunder.

a. Data primer yang berupa :
    1.) Hasil wawancara dari Kepala Labkrim Mabes Polri
    2.) Hasil wawancara dari Kepala Satuan *Cyber Crime* Ditreskrimsus Polda Metro Jaya
    3.) Hasil wawancara dari Jaksa yang opernah menanganai kasus *cyber crime*
    4.) Hasil wawancara dari Hakim Pengadilan Negeri Jakarta Pusat yang pernah menangani kasus *cyber crime*

b. Data sekunder yang berupa :
    1.) Bahan Hukum Primer yang meliputi:
        a.) Kitab Undang-Undang Hukum Acara Pidana (KUHAP)
        b.) Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik
        c.) Undang-Undang No 31 tahun 1999 Tentang Pemberantasan Tindak Pidana

Korupsi yang telah diubah dengan Undang - Undang No. 20 Tahun 2001 tentang Perubahan Atas Undang - Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi

d.) Undang - Undang Nomor 19 Tahun 2002 tentang Hak Cipta

e.) Undang - Undang No. 8 Tahun 2010 tentang Pencucian Uang

f.) Undang - Undang No. 21 Tahun 2007 tentang Perdagangan Orang

g.) Undang-Undang No 44 tahun 2008 Tentang Pornografi

h.) Undang – Undang No. 36 Tahun 1999 tentang Telekomunikasi

i.) Undang – Undang No. 32 Tahun 2002 tentang Penyiaran

j.) Keppres Nomor 8 Tahun 1997 tentang DokumenPerusahaan

k.) Rancangan KUHAP Tahun 2010

2.) Bahan hukum sekunder yang meliputi:

a) Buku-buku yang membahas tentang Hukum Pembuktian dan *forensic cyber*

b) Makalah, tulisan ilmiah dan situs internet maupun media massa yang ada hubungannya dengan permasalahan yang diteliti dan hasil penelitian berupa definisi dan pendapat hukum.

3. Metode Pengumpulan Data

Metode pengumpulan data yang dipergunakan oleh penulis dalam penelitian ini adalah metode pengumpulan data dengan membaca dan mencatat buku, dokumen-dokumen, literatur-literatur, peraturan perundang-undangan, dan wawancara dengan narasumber.

4. Lokasi Penelitian

Lokasi penelitian dilakukan di Mabes Polri, Polda Metro Jaya, Kejaksaan Tinggi Jakarta , Pengadilan Negeri Jakarta Pusat

5. Narasumber

Narasumber adalah pihak yang berhubungan erat dengan permasalahan yang diteliti yaitu Kasubbid komputer forensik MABES POLRI Kompol M Nuh Al-Azhar MSc

6. Metode Analisis

Metode yang digunakan dalam mengolah dan menganalisis data yang diperoleh dalam penelitian adalah analisis kualitatif, yaitu analisis yang dilakukan dengan memahami data atau merangkai data yang telah dikumpulkan secara sistematis, sehingga diperoleh suatu gambaran mengenai masalah atau keadaan yang diteliti serta menggunakan metode berpikir deduktif yaitu pengambilan keputusan yang bersifat khusus. Pola pikir ini menarik kesimpulan dimulai dari pernyataan yang bersifat umum menuju pernyataan khusus dengan menggunakan penalaran.

H. Sistematika Penulisan Hukum

Dalam susb bab ini penulis menjelaskan mengenai sistematika penulisan skripsi ini. Dalam Bab I, penulis membahas mengenai latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, keaslian penelitian,batasan konsep, metode penelitian, dan sistematika penulisan. Dalam Bab II akan dijelaskan mengenai tinjauan umum tentang *cyber crime*, tinjauan umum tentang pembuktian dalam perkara pidana, tinjauan umum tentang *forensic cyber* dan penjelasan mengenai peran dan eksistensi *forensic cyber* di Indonesia. Bab III membahas mengenai kesimpulan dan saran yang diambil berdasarkan hasil penelitian.