BAB I

PENDAHULUAN

Pada saat ini kita berada disuatu era yang disebut era teknologi informasi.Era ini dimulai sejak munculnya suatu teknologi baru yang disebut computer (computer).[1]Komputer merupakan suatu perangkat ataupun sistem elektronikyang mengolah atau memproses data atau informasi sebagaimana yangdiperintahkan, terdiri atas perangkat keras elektronik (*hardware*), danperangkat lunak program komputer (*software*), prosedur-prosedur(*procedures*) dan penggunaannya (*brainware*) serta data atau informasi itusendiri (*content*).[2]Ketika digunakan untuk pertama kalinya komputer muncul dalam bentukmainframe computer yang berukuran sangat besar, yang dalamperkembangannya ukuran untuk sebuah komputer semakin lama semakin kecildimulai dari PC (*personal computer)* yang berbentuk desktop, menyusul bentuk PC (*personal computer)* lain yangdisebut laptop atau notebook sampai jenis handphone tertentu dapatdifungsikan sebagai laptop mini.Dalam perkembangannya, komputer telah memunculkan sesuatu yangbaru di dalam kehidupan kita, yaitu internet.

Internet (*InterconnectedNetwork*) merupakan jaringan *(network*) komputer yang terdiri dari ribuanjaringan komputer independen yang dihubungkan satu dengan yang lainnya.Jaringan komputer ini dapat digunakan oleh lembaga pendidikan,pemerintahan,militer,organisasi,bisnis dan organisasi lainnya. Internet

[1]*Sutan Remy Syahdeini*, Kejahatan & Tindak Pidana Komputer (Jakarta : Grafiti), 2009, halaman 1.

[2]*Edmon Makarim*, Kompilasi Hukum Telematika, (Jakarta : RajaGrafindo Persada), 2003, halaman 54

merupakan jaringankomputer terbesar dunia.Internet sendiri pada dasarnya hanya sebuah mediapengantar sebagaimana media-media pengantar dalam bentuk lainnya.Adanya Internet menciptakan jenis dunia baru yang tak lagi dihalangioleh batas-batas teritorial antara negara yang dahulu ditetapkan. Internet membawa pada dunia tanpa batas dan menembus bataskedaulatan negara yang sebelumnya tidak pernah dikenal oleh manusia, yaitudunia yang disebut "*virtual world*" yang dalam bahasa Indonesia ada yangmenerjemahkannya dengan "dunia maya" atau "mayantara".

Disebut duniamaya oleh karena dunia tersebut tidak seperti dunia dimana kita hidup danmelakukan kegiatan.Dunia dimana kita hidup bersifat *physical* (fisik),sedangkan dunia virtual atau dunia maya bersifat *non-physical* (non-fisik).Oleh karena semua yang berkaitan dengan komputer diberi keterangan dengansebutan "*cyber*" maka untuk ruang lingkup yang berhubungan dengankomputer sering disebut pula "*cyberspace*" (ruang siber).[3]Dunia maya atau cyberspace adalah dunia atau ruang tempatberoperasinya kegiatan atau kehidupan internet.Dunia tempat beroperasinyakegiatan atau kehidupan manusia disebut *real world* (dunia nyata) atau*physical world* (dunia fisik). Walaupun peralatan komputer (yang disebutperangkat keras atau *(computer hardware*) berada di dunia nyata, tetapikegiatan program komputer (yang disebut perangkat lunak komputer atau*computersoftware*) tidak berlangsung di dunia nyata melainkan di duniamaya.

Munculnya dunia maya telah mengubah kebiasaan banyak orangterutama yang dalam kehidupannya terbiasa menggunakan internet.Dengan internet, kita

[3]*Sutan Remy Syahdeini*, Op.cid, 2009, halaman 8.

dapat melakukan hampir semua kegiatan yang dapat dilakukan didunia nyata *(real world*) dapat dilakukan di dunia maya, dengan kebebasanberaktivitas dan berkreasi yang paling sempurna. Namun dibalikkegemerlapan itu, internet juga menciptakan peluang-peluang baru bagikejahatan sebagai akibat negatif dari perkembangan teknologi.

Seiring dengan perkembangan teknologi komunikasi yang begitu pesat, orang-orang tertentudapat juga menyalahgunakan sarana Internet . Salah satu dampak negative teknologi Internet ini adalah munculnya penipuan melalui Media internetyang sudah sering terjadi di masyarakat.Kejahatan penipuan dengan menggunakan layanan internet telah banyakmemakan korban, pada umumnya yaitu masyarakat pengguna internet itu sendiri.Di dunia*virtual* orang melakukan berbagai kejahatan yang justru tidak dapat dilakukandi dunia nyata.Kejahatan tersebut dilakukan dengan menggunakan computer sebagai sarana perbuatannya.

Kejahatan yang dilakukan di dunia maya dengan menggunakan computer disebut "kejahatan komputer" atau "*cybercrime*". Memang belum adakesatuan pendapat dikalangan para ahli mengenai definisi *cyber crime*. Haltersebut disebabkan kejahatan ini (*cyber crime*) merupakan kejahatan yangrelatif baru dibandingkan dengan kejahatan-kejahatan konvensional.

Ada yangmenerjemahkan dengan kejahatan cyber, kejahatan di dunia maya, kejahatanvirtual, bahkan ada yang mempergunakan istilah aslinya yaitu *cyber crime*tanpa menerjemahkannya.

Cyber crime merupakan salah satu bentuk atau dimensi baru darikejahatan masa kini yang mendapat perhatian luas di dunia internasional.[4]Permasalahan

[4] *Dikdik M. Arief Mansur*, SH, MH ; Elisatris Gultom, SH, MH, Cyber Law Aspek Hukum

Cyber crime harus di tangani secara seriuskarena dampak dari kejahatan ini sangat luas dan banyak merugikanperekonomian masyarakat sehingga apabila tidak ditanggulangi secara diniakan berkembang dan jika tidak terkendali dampaknya akan sangat fatal bagikehidupan masyarakat.[5]Di Indonesia sendiri, sampai saat ini tidak ada rumusan baku tentangdefinisi *cyber crime*. Namun demikian, bukan berarti tidak adanya hukum diIndonesia yang mengatur mengenai *cyber crime*.Saat ini Indonesia telahmemiliki UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.Sebelum berlakunya Undang-Undang tersebut, tentu saja hal itu hanya dapatdilakukan oleh penegak hukum sepanjang di dalam KUHP memang dapatditemukan pasal-pasal yang pas untuk dipakai menjatuhkan pidana bagipelaku kejahatan komputer tersebut.

Namun setelah Indonesia memilikiUndang-undang No.11 Tahun 2008 tentang Informasi dan transaksiElektronik, maka penegak hukum tidak perlu lagi mencari-cari dalam KUHPpasal-pasal yang dapat diterapkan untuk menjatuhkan pidana terhadap pelakukejahatan komputer. Undang-Undang No.11 tahun 2008 adalah adalah ketentuan yang berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Undang-Undang ITE boleh disebut sebuah cyberlaw karena muatan dan cakupannya luas membahas pengaturan di dunia maya, meskipun di beberapa sisi

[5] *Volodymyr Golubev*, cyber crime and legal problems of Internet usage, dalam Tindak Pidana Mayantara : Perkembangan Kajian Cyber Crime di Indonesia , (Jakarta : RajaGrafindo Persada), hal 1

ada yang belum terlalu lugas dan juga ada yang sedikit terlewat. Muatan UU ITE adalah sebagai berikut:

1.Tanda tangan elektronik memiliki kekuatan hukum yang sama dengan tanda tangan konvensional (tinta basah dan bermaterai). Sesuai dengan e-ASEAN

2.Framework Guidelines (pengakuan tanda tangan digital lintas batas)

3.Alat bukti elektronik diakui seperti alat bukti lainnya yang diatur dalam KUHP

4.UU ITE berlaku untuk setiap orang yang melakukan perbuatan hukum, baik yang berada di wilayah Indonesia maupun di luar Indonesia yang memiliki akibat hukum di Indonesia[6]

Perbuatan yang dilarang (cybercrime) dijelaskan pada Bab VII (pasal 27-37):

a) Pasal 27 (Asusila, Perjudian, Penghinaan, Pemerasan)
b) Pasal 28 (Berita Bohong dan Menyesatkan, Berita Kebencian dan Permusuhan)
c) Pasal 29 (Ancaman Kekerasan dan Menakut-nakuti)
d) Pasal 30 (Akses Komputer Pihak Lain Tanpa Izin, Cracking)
e) Pasal 31 (Penyadapan, Perubahan, Penghilangan Informasi)
f) Pasal 32 (Pemindahan, Perusakan dan Membuka Informasi Rahasia)
g) Pasal 33 (Virus(Membuat Sistem Tidak Bekerja)

Dan mengenai latarbelakang lahirnya Undang-Undang No 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik,Presiden mengeluarkan Undang-

[6] Undang_undang no 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

undang ini untuk kepentingan dan kesejahteraan rakyat Indonesia dan luar Indonesia. Dalam pasal-pasal yang menjelaskan memberikan rasa aman dan mencerdaskan kehidupan bangsa.

Semakin berkembangnya kejahatan dalam masyarakat, sehingga hukum tjuga harus berkembang agar fungsinya sebagai pemberi rasa aman dapat terpenuhi, dengan adanya Undang-undang ini maka diharapkan masyarakat takut untuk melakuakan kesalahan, karna dijelaskan pada pada ayat (1), bertanggung jawab atas segala kerugian dan konsekwensi yang timbul, tetapi dalam Undang-Undang ITE pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan Transaksi Elektronik.Sebagaimana dimaksud pada ayat (1) diatur sebagai berikut:

1. Jika dilakukan sendiri,segala akibat hokum dalam Pelaksanaan Transaksi Elektronik menjadi tanggung jawab para pihak yang bertransaksi.
2. Jika dilakukan melalui pemberi kuasa,segala akibat hokum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab pemberi kuasa.
3. Jika dilkukan melaui agen Elektronik,segala akibat hokum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara agen elektronik.

Melengkapi Kitab Undang–Undang Hukum Acara Pidana (KUHAP) yang telah ada, UU ITE juga mengatur mengenai hukum acara terkait penyidikan yang dilakukan aparat penegak hukum (kepolisian dan kejaksaan) yang memberi paradigma baru terhadap upaya penegakkan hukum dalam rangka meminimalkan potensi *abuse of power* penegak hukum sehingga sangat bermanfaat dalam rangka memberikan jaminan dan kepastian hukum. “Penyidikan di bidang teknologi informasi dan transaksi elektronik dilakukan dengan memperhatikan perlindungan

terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data atau keutuhan data, sesuai ketentuan peraturan perundang-undangan (Pasal 43 ayat (2).Sedangkan Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat dan wajib menjaga terpeliharanya kepentingan pelayanan umum Pasal 43 ayat (3).

Namun demikian perlu disikapi bahwa tidak mustahil adakejahatan komputer tertentu yang ternyata belum dinyatakan sebagai tindakpidana (belum diatur) oleh UU No.11 Tahun 2008 tentang Informasi danTransaksi Elektronik tersebut.[7]
Fenomena *cyber crime* memang harus diwaspadai karena kejahatan iniagak berbeda dengan kejahatan lain pada umumnya. Kejahatan mayantaradapat terjadi tanpa diperlukan interaksi langsung antara pelaku dengan korbankejahatan. Bisa dipastikan dengan global internet, semua negara yangmelakukan kegiatan internet hampir pasti akan terkena imbas perkembangan*cyber crime* ini.Modus kejahatan dalam dunia maya memang agak sulit dimengerti olehorang-orang yang tidak menguasai pengetahuan teknologi informasi.

Sebab,salah satu karakter pokok *cyber crime* adalah penggunaan teknologi informasidalam modus operandinya.Salah satu ciri *cyber crime* adalah memanfaatkan jaringan teknologiinformasi secara global.Aspek global menimbulkan kondisi seakan-akandunia tidak ada batasnya (*borderless*). Keadaan ini dapat mengakibatkanpelaku, korban serta tempat dilakukannya tindak pidana *(locus delictie*) terjadi di negara yang berbeda-beda. Hukum pidana adalah hukum yang terikat pada ruang dan waktu,sehingga mengenai kapan dan dimana

[7]Loc.cit

tindak pidana dilakukan harus jelasdiketahui.Penentuan tempat terjadinya tindak pidana menjadi sangatpenting, apabila penuntut umum tidak memuat unsur ini dalamdakwaannya mengakibatkan dakwaan tersebut batal demi hukum. Hal initentu saja akan berakibat fatal dalam upaya penegakan hukum.Internet merupakan media yang bersifat lintas batas wilayah dannegara, sehingga apabila terjadi tindak pidana akan sulit untukmenentukan *locus delictie*-nya, karena akan bersinggungan dan melibatkankepentingan negara lain. Hal ini menjadi kendala pula dalam penegakanhukumnya akan tetapi tidak bisa dibiarkan berlarut-larut dan harus segeradicarikan alternatif pemecahannya.

Locus Delictie menurut *Black's Law Dictionary is the placewhere an offense is commiteted: the place where the last event necessaryto make the actor liable occurs.*Terjemahannya adalah *locus delictie* merupakan tempat dimanasuatu tindak pidana terjadi tempat dimana kejadian (tindak pidana) dapatmenyebabkan pelaku harus bertanggungjawab.[8]

Penentuan Locus Delictie menjadi persoalan ketika pembuat danpenyelesaian delik tidak berada di suatu tempat yang sama. Seperti yangterjadi dalam cyber crime, dimana perbuatan melawan hukum yangdilakukan di suatu tempat dapat berakibat di tempat lain,demikian pulasebaliknya. Untuk menyelesaikan permasalahan ini adalah mengikuti salahsatu pola dari empat macam ajaran sebagai berikut :

1. Ajaran tindakan badaniah, untuk menentukan tempat kejadian, pusatperhatian adalah kepada tempat dimana pelaku melakukan suatu tindakpidana, unsur-unsur tindak pidana pada saat itu menjadi sempurna.

[8] *Bryan A. Garner*, Black"s Law Dictionary seventh Edition, St. Paul Minn: West Group, 1999, hal. 951

2. Ajaran tempat bekerjanya alat, tempat kejadiannya adalah dimana alatyang digunakan bekerja dan telah sempurna atau menimbulkan suatutindak pidana.
3. Ajaran akibat dari tindakan, tempat tindak pidana adalah di tempatterjadinya suatu akibat,yang merupakan penyempurnaan dari tindakpidana yang telah terjadi.
4. Ajaran berbagai tempat tindak pidana, tempat tindak pidana adalahgabungan dari ketiga-tiganya atau dua diantara ajaran-ajaran tersebutdiatas.[9]

Keempat teori locus delictie ini yang kemudian akan digunakan untukmenentukan kewenangan pengadilan mengadili tindak pidana khususnyayang dilakukan dengan memanfaatkan media Internet.Banyak permasalahan yang muncul ketika *cyber crime* dapat diungkapoleh aparat penegak hukum, khususnya apabila dalam kejahatan tersebutterkait unsur-unsur asing, seperti pelakunya orang asing, korbannya orangasing atau tempat terjadinya di luar negeri tetapi pengaruhnya dirasakan diIndonesia.Salah satu permasalahan hukum utama yang muncul bersamaandengan terungkapnya kejahatan tersebut adalah masalah kerumitan berkenaandengan yurisdiksi hukum karena tidak lengkap dan tidak konsistennya hukum suatu negara.

Dalam hukum Internasional berlaku ketentuan bahwa tidak seorang pundapat secara sah diekstradisi dari satu negara untuk menghadapi tuntutan dinegara lain kecuali apabila kedua negara tersebut menganut kriminalitas ganda*(dual*

[9] *E.Y Kanter dan S.R Sianturi*, Asas-Asas hukum Pidana di Indonesia dan Penerapannya, (Jakarta : Penerbit Storia Grafika), 2002, halaman 113-115

criminality), Artinya suatu tindak pidana harus dianggap diakui oleh bhukum negara tersebut dan sama tingkatannya dalam jenis tindak pidananya(*same level criminality*) sebelum ekstradisi tersebut dipertimbangkan olehpengadilan.

Berdasarkan uraian di atas sangat menarik sekali bagipenulis untuk mencoba melakukan pembahasan tantang kejahatan dunia maya (*Cyber Crime*)terutama tentang penipuan yang terjadi dalam dunia maya dan meneliti upaya penanggulangannya dengan judul "***Kajian Hukum Tindak Pidana Penipuan Data Pada Media Online Menurut Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik"***. Diambilnya judul ini oleh penulis untuk diteliti adalah karena kejahatan internet (*cyber crime*) itu merupakan jenis kejahatan baru yang tidak lagi memakai kekerasan fisik (*non violence*)

B. Alasan Pemilihan Judul

Sesuai dengan judul skripsi serta ruang lingkup pembahasannya yakni hal mengenai penipuan yang terjadi di dunia maya yang tergolong ke dalam tindak kriminal di dalam dunia maya (*cyber crime*) maka dapat diberikan kerangka pemikiran sebagai berikut:

Peradaban manusia mengalami perubahan drastis pada dekade dipenghujung abad ke 19.Perubahan tersebut utamanya menyangkut pergaulanyang tidak terbatas dengan menggunakan media telekomunikasi.Dalam tatapergaulan dunia yang baru itu, sudah tidak terlihat sekat-sekat atau batas suatu Negara tidak lagi dipersoalkan warna kulit, ras dan golongan.Karena tidak lagi dipisahkan oleh jarak dan waktu, hubungan dapat dilakukan kapan saja, dimana sajadan dari mana

saja.Kemudian inilah yang dikenal sebagai hubungan global.Indonesia merupakan bagian dari tata pergaulan hubungan global itu.Sebagaibagian dari masyarakat global, mau tidak mau kita harus melaksanakanpemahaman dunia dalan tatanan yang baru itu.Perkembangan teknologi khususnya dibidang telekomunikasi dantransportasi dianggap sebagai lokomotif dan turut mempercepat proses globalisasidi berbagai aspekkehidupan.

Perusahaan telekomunikasi seperti *Microsoft World*memberikan berbagai fasilitas dan kemudahan dalam mengakses aneka kebutuhaninformasi berkat dukungan software dan hardwareyang mereka hasilkan.

Kebutuhan atas peningkatan arus informasi antar manusia, dengan kemampuanmengirim dan menerima data dan informasi melalui jaringan komputer sudahmenjadikebutuhan yang tidak dapat ditawar-tawar lagi. Kemudahan-kemudahanitu dapat dilihat dalam berbagai bentuk kerjasama seperti pertemuan ekonomi,politik, budaya, yang selain dilakukan secara fisik, juga dilakukan dengan mediateknologi komunikasi. Dunia menjadi komunitas baru yang serba efektif, efisien serta modern.Terjadi komunikasi bebas tanpa batas yang melintasi batas-bataswilayah kedaulatan suatu Negara.Pengaruh globalisasi yang menyangkut perkembangan ilmu pengetahuandan teknologi, terutama dalam bidang informasi, komunikasi dan transportasi telah mengakibatkan dunia semakin transparan membuat dunia seakan – akantanpa batas. Konsekuensi logis dari perkembangan dibidang teknologikomunikasi, transportasi dan informasi tersebut juga berdampak kepada terjadinyaproses perubahan sosial yang akselerasinya dari waktu ke waktu semakin cepat.

Masyarakat yang dihadapkan kepadakondisi tersebut telah menimbulkan dampak terhadap meningkatnya kejahatan. Kejahatan-kejahatan yang dipengaruhi oleh pengaruhnegatif arus globalisasi yang mempengaruhi masyarakat untuk cenderungmengadopsi gaya hidup orang-orang Barat yang mencerminkan hidupdengan penuh kebebasan, kepuasan serta maraknya tindakan kriminalitas denganmenyalahgunakan perkembangan dan kemajuan teknologi tersebut, sehinggamasyarakat kita cenderung meniru untuk berbuat dalam hal kejahatan yang sama.Seperti: *carding*(Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet) *hacking*(kegiatan memasuki system melalui system operasional yg lain,yg dijalankan oleh Hacker) *joy computing*(pemakaian komputer orang lain tanpa izin) . Hal ini termasuk pencurian waktu operasi komputer dan lain-lain.

Dimasa yang akan datang perkembangan teknologi canggih tersebut akan lebih memotivasi para kriminal untuk menciptakan modus operandi baru terhadap perbuatan tindak pidana yangsebelumnya belum pernah dikenal sama sekali, sebagaimana adagium yang cukup populer di dunia Internasional bahwa masyarakat itu sendirilah yang menciptakan bentuk, jenis dan jumlah kejahatan yang terjadi. Sehingga untuk mengantisipasinya tentumemerlukan pula suatu sistem hukum baru.Salah satu bentuk kejahatan dari klasifikasi kejahatan dengan dimensi baru adalahKejahatan yang pada prosesnya menggunakan teknologi informasi khususnya komputer/internet.

Kehadiran Internet memang sangat banyak manfaatnyadisamping mempercepat perolehan informasi juga aksesnya yang dapatdimanfaatkan untuk

berbagai bidang kebutuhan hidup lainnya, misalnya melaluiSitus Internet digunakan untuk mengirim e-mail, hiburan dan sebagainya.Dalam dunia perdagangan penawaran barang dan jasa dengan transaksiyang berlangsung melalui Internet, konsumen melihat gambaran mengenaibarang dan uraian jasa di Internet kemudian setelah setuju dilanjutkan denganpembayaran melalui Internet dengan menyebutkan nomor kartu kredit.Disinilahtantangan yang sering disebut menyangkut keamanan transaksi, dimana parapengguna jasa merasa khawatir dengan menyebutkan nomor kartu kreditnya diInternet.Hal ini dikarenakan berpotensial disalahgunakan,misalnya penagihanlebih besar dari pada harga yang disepakati, nomor kartu kredit bisa digunakanoleh orang lain.

Kejahatan Internet (*cyber crime*)sudah menjadi problematika yang tidak dapat di elakan ladi keberadaanya, olehkarenanya Negara-negara didunia khususnya Indonesia mengupayakansebuah aturan hukum bersama untuk mengatur masalah cybercrime ini. Kejahatan internet (*cyber crime*) berbeda dengankejahatan konvensional seperti membunuh, mencuri, merampok dsb, karena tidak semua orang dapat melakukan kejahatan ini.

Dengan uraian di atas maka dapat dibuat alasan pemilihan judul dalam skripsi ini adalah:

1. Untuk memperdalam ilmu di bidang Hukum,khususnya penerapan hukum pidana tentang pidana pelaku tindak kriminal dalam dunia maya(*cyber crime*)
2. Untuk memberi suatu gambaran terhadap masyarakat,baik dalam bentuk teori maupun praktek,tentang kejahatan dalam dunia maya.

3. Untuk mengetahui secara mendetail kekuatan hukum tentang Informasi Transaksi Elektronik.

C. Perumusan Masalah

Permasalahan merupakan suatu persoalan yang harus dicari pemecahannya,guna memudahkan pembahasan agar tidak menyimpang dari materi pokok dalam penulisan skripsi. Berdasar dari latar belakang masalah diatas, untuk mendukung efektivitas komunikasi dengan memanfaatkan secara optimal teknologi informasi demi tercapainya keadilan, kemanfaatan dan kepastian hukum, yang menjadi perkara kejahatan dunia maya, dengan demikian dapat dirumuskan masalahnya sebagai berikut :

1. Apa yang dimaksud dengan kejahatan media online(*Cyber Crime)*?
2. Bagaimana unsur-unsur tindak pidana penipuan dalam dunia maya berdasarkan UU no 11 tahun 2008 ?
3. Bagaimana proses tranformasi barang bukti menjadi alat bukti dalam tindak pidana melalui sarana Elektronik,mengacu kepada KUHP dan UU no 11 tahun 2008 menurut masing-masing UU ?
4. Faktor apa saja yang melatarbelakangi lahirnya *Cyber Crime*?
5. Sanksi apa yang diberikan terhadap pelaku tindak pidana *cyber crime*?
6. Bagaimana penanggulangan tindak pidana *cyber crime* di Indonesia?

D. Hipotesa

1.Ketentuan hukum di Indonesia mengenai Tindak pidana media online ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana sepanjang dengan menggunakan bantuan atau sarana Sistem Elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana media online,sehingga ketentuan hukum Indonesia sudah mengatur mengenai *cyber crime*.

2.Undang-Undang No 11 tahun 2008 tentang Informasi dan Transaksi elektronik tidak secara khusus mengatur mengenai tindak pidana penipuan.Selama ini tindak pidana penipuan itu sendiri diatur dalam pasal 378 KUHP dengan rumusan sebagai berikut: "Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan menggunakan nama palsu atau martabat (*hoedaningheid*) palsu; dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam, karena penipuan, dengan pidana penjara paling lama empat tahun."

Walaupun UU ITE tidak secara khusus mengatur mengenai tindak pidana penipuan, namun terkait dengan timbulnya kerugian konsumen dalam transaksi elektronik terdapat ketentuan Pasal 28 ayat (1) UU ITE yang menyatakan:

"Setiap Orang dengan sengaja, dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik."

Terhadap pelanggaran Pasal 28 ayat (1) UU ITE diancam pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp1 miliar, sesuai pengaturan Pasal 45 ayat (2) UU ITE.

Jadi, dari rumusan-rumusan Pasal 28 ayat (1) UU ITE dan Pasal 378 KUHP tersebut dapat kita ketahui bahwa keduanya mengatur hal yang berbeda. Pasal 378 KUHP mengatur penipuan sementara Pasal 28 ayat (1) UU ITE mengatur mengenai berita bohong yang menyebabkan kerugian konsumen dalam transaksi elektronik.Walaupun begitu, kedua tindak pidana tersebut memiliki suatu kesamaan, yaitu dapat mengakibatkan kerugian bagi orang lain. Tapi, rumusan Pasal 28 ayat (1) UU ITE tidak mensyaratkan adanya unsur "menguntungkan diri sendiri atau orang lain" sebagaimana diatur dalam Pasal 378 KUHP tentang penipuan.

3.Melalui Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), informasi elektronik/dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Yang dimaksud dengan dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam 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.

Kitab Undang-undang Hukum Acara Pidana memang tidak menyebutkan secara jelas tentang apa yang dimaksud dengan barang bukti. Namun dalam **Pasal 39 ayat (1) KUHAP** disebutkan mengenai apa-apa saja yang dapat disita, yaitu:benda atau tagihan tersangka atau terdakwa yang seluruh atau sebagian diduga diperoleh dari tindakan pidana atau sebagai hasil dari tindak pidana,benda yang telah dipergunakan secara langsung untuk melakukan tindak pidana atau untuk mempersiapkannya;benda yang digunakan untuk menghalang-halangi penyelidikan tindak pidana;benda yang khusus dibuat atau diperuntukkan melakukan tindak pidana;benda lain yang mempunyai hubungan langsung dengan tindak pidana yang dilakukan.[10]

Dalam KUHPdisebutkan bahwa alat bukti yang sah adalah: keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Dalam sistem pembuktian hukum acara pidana yang menganut stelsel *negatief wettelijk*, hanya alat-alat bukti yang sah menurut undang-undang yang dapat dipergunakan untuk pembuktian.Hal ini berarti bahwa di luar dari ketentuan tersebut tidak dapat dipergunakan sebagai alat bukti yang sah.[11]

Dalam kasus *cyber crime*transformasi barang bukti menjadi alat bukti adalah benda atau tagihan tersangka atau terdakwa yang seluruh atau sebagian diduga diperoleh dari tindakan pidana atau sebagai hasil dari tindak pidana,benda yang telah dipergunakan secara langsung untuk melakukan tindak pidana atau untuk mempersiapkannya,benda yang digunakan untuk menghalang-halangi penyelidikan tindak pidana,benda yang khusus dibuat atau

[10] Kitab Undang-undang Hukum Acara Pidana
[11]Martiman Prodjohamidjojo, *Sistem Pembuktian dan Alat-alat Bukti*, hal. 19

diperuntukkanmelakukan tindak pidana,benda lain yang mempunyai hubungan langsung dengan tindak pidana yang dilakukan(perangkat elektronik yang digunakan).

4.Faktor yang melatarbelakangi lahirnya *cyber crime* adalah karena akses internet yang tidak terbatas memungkinkan orang untuk dapat sembarangan dalam memanfaatkan teknologi. Setiap orang dapat dengan bebas dan gampang melakukan sesuatu tanpa adanya batasan yang mengatur.Informasi yang diberikan pun terkesan sebagai formalitas tanpa.Hal ini dapat disalahgunakan orang untuk melakukan tindak kejahatan secara bebas dan tanpa terlacak.Inilah yang menjadi penyebab utama terjadinya *cybercrime*. Para pelaku pada umumnya cerdas, mempunyai rasa ingin tahu yang besar dan fanatik akan teknologi komputer. Pengetahuan pelaku kejahatan komputer tentang cara kerja sebuah komputer jauh diatas rata-rata pengguna komputer lainnya.

5.Sanksi yang diberikan terhadap pelaku tindak pidana *cyber crime*di Indonesia cukup berat,sanksi tersebut di atur pada pasal 45-52 Undang-Undang No 11 tahun 2008 tentang Informasi dan transaksi Elektronik.

6.Penanggulangan tindak pidana *cyber crime* di Indonesia dalam upaya-upaya yang dapat dilakukan terkait dengan masalah pembuktian oleh pengadilan dan penyidikan oleh polri dalam cyber crime dapat digunakan berbagai macam cara, antara lain dengan mengoptimalkan Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, mengembangkan pengetahuan dan kemampuan penyidik dalam Dunia Cyber, menambahkan dan meningkatkan fasilitas komputer forensik dalam POLRI.Dansalah satu langkah lagi agar

penanggulangan *cyber crime* ini dapat dilakukan dengan baik, maka perlu dilakukan kerja sama dengan *Internet Service Provider* (ISP) atau penyedia jasa internet. Meskipun *InternetService Provider* (ISP) hanya berkaitan dengan layanan sambungan atau akses Internet, tetapi *Internet Service Provider* (ISP) memiliki catatan mengenai ke luar atau masuknya seorang pengakses, sehingga ia sebenarnya dapat mengidentifikasikan siapa yang melakukan kejahatan dengan melihat *log file* yang ada.[12]

E. Tujuan penelitian

Adapun yang menjadi tujuan penelitian penulis dalam penulisan skripsi ini adalah sebagai berikut,Untuk menganalisa,mengetahui dan memahami lebih lanjut bagaimana sebenarnya penerapan hukum pida terhadap pelaku *cyber crime*mulai dari factor terjadinya *cyber crime*,sanksi bagi pelaku tindak pidana cyber crime penanggulangan tindak pidana *cyber crime* dan unsur-unsur tindak pidana penipuan yang terjadi di dunia maya.

Sebagai bahan sumbangsih ilmiah bagi masyarakat untuk mengetahui tentang kajian hukum pidana *cyber crime*khususnya penipuan pada dunia online.

F. Pengumpulan Data

Sebagai karya ilmiah maka dalam penulisan skripsi ini penulis mengumpulkan data serta bahan-bahan tulisan dengan menggunakan metode penelitian kepustakaan.Penelitian Kepustakaan (Library Research) yaitu penelitian yang dilakukan dengan membaca buku-buku ilmiah,majalah,media massa serta

[12] http://id.wikipedia.org/wiki/Penyelenggara_jasa_Internet diakses 22/6/2014pukul 22:00

peraturan perundang-undangan yang berhubungan erat untuk mendukung penulisan skripsi dan penelitian lapangan (Field Research)Untuk dijadikan landasan dan alur penulisan ilmiah berupa teori-teori hukum tentang kajian hukum tindak pidana *cyber crime*.

G. Sistematika Penulisan

Untuk memudahkan penyusunan dan pemahaman skripsi ini,penulis membuat suatu sistematika penulisan secara teratur yang terdiri dari beberapa bagian yang mempunyai hubungan erat antara yang satu dan yang lainnya.

Adapun susunan bab-bab tersebut adalah sebagai berikut:

BAB I: PENDAHULUAN

Di dalam bab ini diuraikan mengenai pendahuluan sebagai pengantar yang mengantarkan kita menuju uraian-uraian selanjutnya.pendahuluan ini berisikan tentang latar belakang,alasan pemilihan judul,permasalahn,hipotesa,tujuan penelitian dan sistematika penulisan.

BAB II: KAJIAN TENTANG PENIPUAN

Dalam bab ini membahas kajian tentang penipuan terdiri dari pengertian dan unsur-unsur penipuan menurut hukum pidana.

BAB III: KAJIAN TENTANG *CYBER CRIME*

Dalam bab ini diuraikan tentang kajian *cyber crime* terdiri dari pengertian *cyber crime*,jenis-jenis *cyber crime* menurut undang-undang Informasi dan Transaksi Elektronik.

BAB IV: PROSES DAN SANKSI HUKUM BAGI PELAKU PENIPUAN MELALUI MEDIA ONLINE

Dalam bab ini menguraikan tentang pelaku dan korban *cyber crime* dalam masyarakat dalam kajian hukum pidana yang terdiri dari yang meliputi bagaimana terbentuknya jaringan komputer di tengah masyarakat, faktor-faktor terjadinya*cyber crime*,kajian hukum tindak pidana penipuan menurut Undang Undang No 11 Tahun 2008.

BAB V: SIMPULAN DAN SARAN

Dalam bab ini berisikan tentang kesimpulan dari pembahasan yang telah dilakukan dan saran-saran yang merupakan sumbangsih pemikiran dari penulis.