BAB I

PENDAHULUAN

1.1. Latar Belakang

Pada era globalisasi yang kita kenali sekarang ini informasi telah menempatkan Indonesia menjadi salah satu bagian dari masyarakat informasi dunia, sehingga mengharuskan untuk dibentuknya pengaturan mengenai pengelolaan informasi dan transaksi komunikasi di tingkat Nasional sehingga pembangunan teknologi informasi dapat dilakukan secara optimal, merata dan menyebar ke seluruh lapisan masyarakat di Indonesia sebagai salah satu tujuan untuk mencerdaskan kehidupan bangsa dan negara.[1]

Kecanggihan teknologi komputer tidak dipungkiri telah memberikan kemudahan terutama dalam membantu pekerjaan manusia. Selain itu, perkembangan teknologi komputer tersebut juga berdampak negatif seperti memunculkan kejahatan – kejahatan baru dengan memanfaatkan komputer sebagai modus operandinya.[2] Kemajuan teknologi tidak hanya membawa perubahan kepada kehidupan masyarakat tetapi juga membawa perubahan yang signifikan bagi perubahan sosial, budaya dan ekonomi juga pola penegakan hukum.

[1]Dikdik M Arif Mansyur dan Elisatris Gultom ,*CYBER LAW Aspek Hukum Teknologi Informasi,* (Bandung: PT Refika Aditama,2005), hlm.3.

[2]Maskun, *Kejahatan Siber Cyber Crime Suatu Pengantar*, (Jakarta: Kencana,2013). hlm.17.

Teknologi dan hukum merupakan dua unsur yang saling mempengaruhi dan keduannya juga mempengaruhi masyarakat. Heidegger berpendapat bahwa di satu sisi teknologi dapat dilihat sebagai sarana untuk mencapai tujuan tertentu. Akan tetapi, di sisi lain teknologi juga dapat dilihat sebagai aktivitas manusiawi. Pada dasarnya, setiap teknologi dikembangkan untuk memenuhi kebutuhan tertentu dan melalui teknologi itu diberikan suatu manfaat dan layanan bagi manusia termasuk meningkatkan keefisienan dan keefektivitasan kerja. Teknologi dan masyarakat bersifat dinamis karena terus berkembang, sedangkan hukum bersifat statis. Teknologi menuntut respon hukum, di satu sisi hukum berusaha mengakomodir perkembangan teknologi demi kepentingan masyarakat, tetapi di sisi lain hukum memiliki tanggung jawab untuk tetap menjaga teknologi yang ada sekarang, sehingga tetap menjaga berbagai kepentingan atau kebutuhan masyarakat luas yang telah terpenuhi dengan teknologi yang telah ada itu.[3]

Pendekatan teknologi secara nyata telah banyak membantu penegak hukum dalam mengungkap berbagai kasus. Teknologi elektronik dimanfaatkan oleh penegak hukum salah satunya adalah dalam pembuktian. Namun pemanfaatan teknologi dalam rangka untuk pembuktian suatu tindak pidana masih perlu dikaji lebih lanjut dalam mekanisme hukum di Indonesia.

Penggunaan bukti elektronik dalam hukum pidana Indonesia memang telah tercantum didalam Undang – undang. Bukti elektronik masih tergolong

[3]Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana,* (Jakarta: Tatanusa,2012), hlm.31-31.

baru di Indonesia, sehingga pengaturannya juga masih tergolong baru, hal ini sebagaimana diketahui bahwa penerapan bukti elektronik tersebut tertuang dalam Undang – undang Nomor 19 tahun 2016 tentang Perubahan Atas Undang – undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Undang-Undang ITE ini dimaksudkan untuk menjawab permasalahan hukum yang seringkali dihadapi yaitu terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.namun kenyataan saat ini adalah ketidakmampuan sistem hukum konvensional dalam mengantisipasi dan menangani kasus kejahatan didunia maya. Hal ini di dasari oleh beberapa hal, misalnya persoalan tentang kegiatan dunia maya yang tidak dapat dibatasi oleh teritorial suatu negara, aksesnya dengan mudah dapat dilakukan dari belahan dunia manapun, kerugian dapat terjadi baik pada pelaku internet maupun orang lain yang tidak pernah berhubungan sekalipun.

Esensi Undang-Undang Informasi dan Transaksi Elektronik melingkupi seluruh transaksi berbasis elektronik seperti komputer serta jaringan dan memiliki kekuatan hukum. Undang-Undang ITE dipersepsikan sebagai *cyberlaw* di Indonesia, yang diharapkan bisa mengatur segala urusan dunia

internet (*cyber*), termasuk didalamnya memberi hukuman terhadap pelaku *cybercrime* guna melindungi masyarakat dari kejahatan di dunia maya.[4]

Dalam dunia kemananan komputer pun terjadi perkembangan. Bukti Elektronik yang dijadikan alat bukti juga memiliki permasalahan yang cukup kompleks. Jika melihat hal tersebut permasalahan yang paling utama dari bukti elektronik adalah mengenai keaslian dan integritasnya suatu bukti apakah dapat dipercaya. Untuk dapat mewujudkan hal itu maka dibutuhkanlah suatu investigasi bukti elektronik yang dikenal juga dengan Forensi Digital. Forensik digital merupakan metode investigasi dengan mengaplikasikan ilmu pengetahuan dan teknologi untuk memeriksa dan menganalisis suatu bukti elektronik. Proses forensik digital ini kemudian akan menemukan suatu bukti digital dari suatu sistem elektronik yang selanjutnya akan dianalisis agar dapat dijadikan bukti yang terpercaya yang selanjutnya menjadi digital evidence serta hasil uji forensik digital.

Pencarian bukti-bukti elektronik untuk menjerat pelaku seringkali merupakan pekerjaan yang sangat kompleks dimana dalam proses digital forensik yang dilakukan oleh seorang digital forensik analis/investigator harus mengikuti prosedur-prosedur yang diakui secara hukum baik nasional maupun internasional, termasuk juga mereka harus memahami secara teoritis hal-hal yang berkaitan dengan bukti digital yang ditemukan, disamping juga memahami bagaimana penggunaan software-software forensik untuk mencari

[4]Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime), Urgensi Pengaturan dan Celah Hukumnya,* (Jakarta: Raja Grafindo Persada,2013), hlm.17.

bukti-bukti digital tersebut dengan benar. Sering kali juga bukti-bukti digital tersebut sudah dihapus oleh pelaku untuk menghilangkan jejaknya. Di sinilah tantangan bagi seorang analis/investigator untuk menelusuri kembali bukti digital yang sudah hilang tersebut, bahkan mereka harus mampu untuk me-recover-nya kembali.[5]

Digital forensik analis atau investigator juga sering dipanggil ke persidangan sebagai saksi ahli untuk menjelaskan proses dan temuan dari bukti-bukti digital tersebut, dimulai dari temuan barang bukti elektronik di Tempat Kejadian Perkara (TKP), penerimaan barang bukti di laboratorium, pemeriksaan secara ilmiah dan analisis laboratoris kriminalistik hingga pembuatan laporannya. Oleh karena pentingnya digital forensik dalam pengungkapan kasus kejahatan komputer (*Computer crime*) dan kejahatan terkait komputer (*Computer-related crime*) untuk penegakan hukum di suatu negara temasuk indonesia, maka digital forensik haruslah senantiasa dikembangkan mengikuti perkembangan ilmu pengetahuan dan teknologi komputer. Digital forensik seharusnya dapat berada satu langkah di depan *computer crime* dan *computer –related crime*. Meskipun begitu sering kali digital forensik analis atau investigator mendapatkan temuan atau modus baru dari kejahatan tersebut .

Semakin berkembangnya tingkat kejahatan siber maupun kejahatan yang melibatkan barang bukti elektronik di masa depan tidak akan mudah dan lebih

[5]Muhammad Nuh Al- Azhar, *Digital Forensic: Panduan Praktis Investigasi Komputer,* (Jakarta: Salemba Infotek,2012), hlm.3.

rumit dalam rangka pembuktian. Maka digital forensik akan sangat dibutuhkan dalam rangka menjadi alat bantu untuk penegakan hukum di Indonesia dalam kejahatan siber maupun kejahatan yang melibatkan tindakan penyalahgunaan teknologi elektronik.

Terkait dengan pembuktian suatu tindak pidana, dalam era globalisasi ini semakin marak tentang penyalahgunaan teknologi, masyarakat justru kehilangan nilai – nilai moral dan sosial salah satunya adalah dengan menghina, mencaci dan mencemarkan nama seseorang semakin marak ditemukan di sosial media. Pengungkapan kasus seperti ini sulit dilakukan oleh aparat penegak hukum terutama dalam hal pembuktian. Rasa hormat harus diobjektifkan dan harus ditinjau dengan suatu perbuatan tertentu, seseorang pada umumnya tersinggung atau tidak.

Lebih lanjut lagi, bahwa perbuatan penghinaan di sosial media dapat dilakukan dengan cara apapun, misalnya seseorang melontarkan kata – kata tidak senonoh melalui sosmed maka sanksi yang dipertanggung jawabkan akan didasarkan pada UU Nomor 19 tahun 2016 tentang perubahan atas UU Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik.

Berdasarkan latar belakang diatas, penulis tertarik untuk melakukan penelitian mengenai Pembuktian tindak pidana melalui *Cyber Forensic* untuk tindak pidana penghinaan dengan harapan penulis dapat mengetahui peraturan *cyber forensic* di Indonesia serta pembuktian tindak pidana melalui *cyber forensic* atas tindak pidana penghinaan di social media, dengan judul

penelitian **"Pertanggungjawaban Pelaku Tindak Pidana Penghinaan di Sosial Media Berdasarkan Pembuktian Melalui *Cyber Forensik*".**

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang masalah di atas, maka yang menjadi rumusan masalah adalah:

1. Apa unsur-unsur tindak pidana penghinaan di social media?
2. Bagaimana pertanggungajwaban pelaku tindak pidana penghinaan di social media berdasarkan pembuktian melalui *Cyber Forensic*?

1.3. Tujuan Penelitian

Dari permasalahan diatas maka secara keseluruhan tujuan penelitian adalah:

1. Mengetahui unsur-unsur tindak pidana penghinaan di social media.
2. Mengetahui pertanggungjawaban pelaku tindak pidana penghinaan di social media berdasarkan pembuktian melalui *Cyber Forensic*.

1.4. Manfaat Penelitian

1. Manfaat Teoritis

   Dalam penelitian ini diharapkan mampu memberikan pemahaman kepada mahasiswa dan masyarakat luas pada umumnya terkait dengan Pertanggungjawaban pelaku tindak pidana penghinaan di social media berdasarkan pembuktian melalui *Cyber Forensic*.

2. Manfaat Praktis

   Dengan adanya penelitian ini diharapkan dapat menjadi wacana baru, sekaligus memberikan pemahaman yang lebih mendalam mengenai Pertanggungjawaban pelaku tindak pidana penghinaan di social media

berdasarkan pembuktian melalui *Cyber Forensic* kepada Para Penegak Hukum

1.5. Tinjauan Pustaka

1.5.1. Pertanggungjawaban Pidana

Pertanggungjawaban pidana dalam bahasa asing disebut sebagai "toereken-baarheid", "criminal responsibility", "criminal liability", pertanggungjawaban pidana ini dimaksudkan untuk menentukan apakah seseorang tersebut dapat dipertanggungjawabkan atas pidananya atau tidak terhadap tindakan yang dilakukan itu.[6]

Pertanggungjawaban atau yang dikenal dengan konsep liability dalam segi falsafah hukum, Roscoe Pound menyatakan bahwa: I..use simple word "liability" for the situation whereby one may exact legaly and other is legaly subjeced to the excaxtion" pertanggungjawaban pidana diartikan Pound adalah sebagai suatu kewajiban untuk membayar pembalasan yang akan diterima pelaku dari seseorang yang telah dirugikan.[7] Menurutnya juga bahwa pertanggungjawaban yang dilakukan tersebut tidak hanya menyangkut masalah hukum semata akan tetapi menyangkut pula masalah nilai-nilai moral ataupun kesusilaan yang ada dalam suatu masyarakat.

Pertanggungjawaban pidana adalah pertanggungjawaban orang terhadap tindak pidana yang dilakukannya. Terjadinya

---

[6]S.R Sianturi, *Asas-Asas Hukum Pidana Indonesia dan Penerapannya*, (Jakarta: Cet. IV Alumni Ahaem-Pateheam, 1996), hlm. 245.

[7]2 Romli Atmasasmita, *Perbandingan Hukum Pidana*, (Bandung: Mandar Maju,2000), Hlm. 65

pertangunggjawaban pidana karena telah ada tindak pidana yang dilakukan oleh seseorang. Pertanggungjawaban pidana pada hakikatnya merupakan suatu mekanisme yang dibangun oleh hukum pidana untuk bereaksi terhadap pelanggaran atas „kesepakatan menolak‟ suatu perbuatan tertentu.[8]

Dengan demikian, seseorang mendapatkan pidana tergantung dua hal, yakni (1) harus ada perbuatan yang bertentangan dengan hukum, atau dengan kata lain, harus ada unsur melawan hukum jadi harus ada unsur Objektif, dan (2) terhadap pelakunya ada unsur kesalahan dalam bentuk kesengajaan dan atau kealpaan, sehingga perbuatan yang melawan hukum tersebut dapat dipertanggungjawabkan kepadanya jadi ada unsur subjektif. Terjadinya pertanggungjawaban pidana karena telah ada tindak pidana/perbuatan yang dilakukan oleh seseorang.

Roeslan Saleh menyatakan "bahwa pertanggungjawaban pidana diartikan sebagai diteruskannya celaan yang objektif yang ada pada perbuatan pidana dan secara subjektif memenuhi syarat untuk dapat dipidana karena perbuatannya itu".[9]

Maksud celaan objektif adalah bahwa perbuatan yang dilakukan oleh seseorang memang merupakan suatu perbuatan yang dilarang. Indikatornya adalah perbuatan tersebut melawan hukum baik dalam arti melawan hukum formil maupun melawan hukum materiil. Sedangkan

---

[8]Chairul Huda, *Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan*, Cet.Kedua (Jakarta: Kencana, 2006), hlm.70.

[9]Roeslan Saleh dalam Hanafi Amrani dan Mahrus Ali, *Sistem Pertanggungjawaban pidana Perkembangan dan Penerapan*, (Jakarta: PT Rajawali Press, 2015), hlm 21.

maksud celaan subjektif menunjuk kepada orang yang melakukan perbuatan yang dilarang tadi. Sekalipun perbuatan yang dilarang telah dilakukan oleh seseorang, namun jika orang tersebut tidak dapat dicela karena pada dirinya tidak terdapat kesalahan, maka pertanggungjawaban pidana tidak mungkin ada.

Pertanggungjawaban pidana berbeda dengan perbuatan pidana. Perbuatan pidana hanya menunjuk kepada dilarang dan diancamnya perbuatan dengan suatu pidana. Apakah orang yang melakukan perbuatan kemudian dijatuhi pidana, tergantung dari pada perbuatan tersebut mengandung kesalahan. Sebab asas dalam pertanggungjawaban hukum pidana adalah "tidak dipidana jika tidak ada kesalahan (Geen straf zonder schuld; Actus non facit reum nisi mens sis rea) yang artinya penilaian pertanggungjawaban pidana itu ditujukan kepada sikap batin pelakunya, bukan penilaian terhadap perbuatannya. Pengecualian prinsip actus reus dan mens rea adalah hanya pada delik-delik yang bersifat strict liability (pertanggungjawaban mutlak), dimana pada tindak pidana yang demikian itu adanya unsur kesalahan atau mens rea tidak perlu dibuktikan.[10]

Secara lebih rinci, Sudarto menyatakan bahwa agar seseorang memiliki aspek pertanggungjawaban pidana, dalam arti dipidananya pembuat, terdapat beberapa syarat yang harus dipenuhi, yaitu:[11]

---

[10]Hasbullah F. Sjawie, *Pertanggungjawaban Pidana Korporasi Pada Tindak Pidana Korupsi*, (Jakarta: Prenada Media Group, 2015), hlm 1.

[11]Sudarto dalam Hanafi Amrani dan Mahrus Ali, *Sistem Pertanggungjawaban Pidana Perkembangan dan Penerapan*, (Jakarta: Rajawali Press, 2015), hlm 22.

1. Adanya suatu tindak pidana yang dilakukan oleh pembuat;
2. Adanya unsur kesalahan berupa kesengajaan atau kealpaan;
3. Adanya pembuat yang mampu bertanggungjawab;
4. Tidak ada alasan pemaaf.

Sistem pertanggungjawaban pidana dalam hukum pidana Indonesia saat ini menganut asas kesalahan sebagai salah satu asas disamping asas legalitas dalam Pasal 1 KUHPidana. Pertanggungjawaban pidana merupakan bentuk perbuatan dari pelaku tindak pidana terhadap kesalahan yang dilakukannya. Dengan demikian, terjadinya pertanggungjawaban pidana karena ada kesalahan yang merupakan tindak pidana yang dilakukan oleh seseorang, dan telah ada aturan yang mengatur tindak pidana tersebut.

1.5.2. Tindak Pidana *Cyber Crime*

Teknologi telekomunikasi telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Artinya, masyarakat berkembang menuju masyarakat baru yang berstruktur global. Sistem tata nilai dalam suatu masyarakat berubah, dari yang bersifat lokal-partikular menjadi global universal. Hal ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral, dan kesusilaan.[12]

Kemajuan teknologi yang merupakan hasil budaya menusia di samping membawa dampak positif, dalam arti dapat diperdayagunakan untuk kepentingan umat manusia juga membawa

[12]Abdul Wahid dan Mohammad Labib, *Kejahtan Mayaantara (Cybercrime)*, (Bandung: PT Refika Aditama, 2005), hlm. 23.

dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. J. E Sahetapy telah menyatakan dalam tulisannya, bahwa kejahatan erat kaitanya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Ini berarti semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaanya.[13]

Memasuki pembahasan terkait pengertian cyber crime maka akan menyinggung tentang keamanan suatu jaringan komputer atau informasi teknologi telekomunikasi. Terutama pada era globalisasi saat ini, yang membawa kemajuan teknologi sangat pesat maka hal tersebut tidak terlepas adanya resiko dari penyalahgunaan dari pemanfaatan teknologi sebagai kebutuhan informasi.

Penyalahgunaan komputer dibagi atas dua bidang utama. Pertama, adalah penggunaan komputer sebagia alat untuk melakukan kejahatan, contoh kasusnya adalah pencurian. Kemudian, yang kedua adalah komputer tersebut merupakan objek atau sasaran dari tindak kejahatan tersebut, contoh kasusnya adalah sabotase komputer sehingga tidak dapat berfungsi sebagimana mestinya.

Kejahatan dunia maya atau kejahatan siber (*Cybercrime*) merupakan kejahatan yang berbeda dengan kejaharan konvensional

[13]J. E Sahetapy dalam Abdul Wahid, *Kriminologi dan Kejahatan Kontemporer*, (Malang: Lembaga Penerbitan Fakultas Hukum Unisma. 2002).

(street crime). Cyber crime muncul bersamaan dengan lahirnya revolusi teknologi informasi. Sebagimana dikemukakan oleh Ronni R. Nitibaskara bahwa: "Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Penyimpangan social menyesuasikan bentuk dan karakter baru dalam kejahatan.[14]

Cyber crime atau kejahatan dunia maya dalam peraturan Perundang-undangan di Indonesia juga sering disebut dengan kejahatan tindak pidana yang berkaitan dengan teknologi informasi, hal ini sejalan dengan pengertian yang diberikan oleh Donn B. Parker yang memberikan definisi sebagai berikut: "*Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffered loss and a perpetrator by intention made or could have gain*", yang kemudian diterjemahkan oleh Andi Hamzah sebagai penyalahgunaan komputer didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan".[15]

Pengertian cybercrime menurut Prof Widodo adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang

[14]Ronni R Nitibaskara dalam Didik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, (Bandung: PT Refika Aditama, 2005), hlm. 25.

[15]Andi Hamzah, *Hukum Pidana yang berkaitan dengan komputer*, (Jakarta: Sinar Grafika Offset, 1993), hal. 18

menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan. Semua kejahatan tersebut adalah bentuk-bentuk perbuatan yang bertentangan dengan peraturan perundang-undangan, baik dalam arti melawan hukum secara material maupun melawan hukum secara formal.[16] Kemudian, definisi lain mengenai kejahatan komputer ini dikeluarkan oleh Organization of European Community Development (OECD) yaitu sebagai berikut: " any illegal, unethicall or unauthorized behavior relating to the authomathic processing and/or the transmission of data".[17] Dari definisi tersebut, kejahatan komputer ini termasuk segala akses illegal atau akses secara tidak sah terhadap suatu transmisi data. Sehingga telihat bahwa segala aktivitas yang tidak sah dalam suatu system komputer merupakan suatu kejahatan.

Sehingga tindak pidana cyber crime adalah suatu tindak pidana yang dilakukan dengan menggunakan jaringan teknologi informasi komputer untuk mendapatkan data secara ilegal serta dipergunakan untuk mengambil keuntungan yang tidak sah dan menyebabkan kerugian pada masyarakat.

1.5.2.1 Bentuk Tindak Pidana *Cyber*

Cybercrime mempunyai bentuk beragam, karena setiap negara tidak selalu sama dalam melakukan

[16]Widodo, *Aspek Hukum Kejahatan Mayantara*, (Yogyakarta: Aswindo, 2011), hlm. 7

[17]Andi Hamzah*, Aspek-aspek Pidana di Bidang Komputer*, (Jakarta: Sinar Grafika, 1989), hlm. 26

krimininalisasi. Begitu pula, dalam setiap negara dalam menyebut apakah suatu perbuatan tergolong kejahatan cybercrime atau bukan kejahatan cybercrime juga belum tentu sama. Secara teoritik, berkaitan dengan konsepsi kejahatan. Muladi mengemukakan bahwa asas mala in se mengajarkan bahwa suatu perbuatan dikategorikan sebagai kejahatan karena masyarakat dengan sendirinya menganggap perbuatan tersebut jahat. Sedangkan berdasarkan asas mala prohibita, suatau perbuatan dianggap jahat karena melanggar peraturan perundang-undangan.[18] Asas Mala Prohibita menghasilkan konsep si kejahatan dalam arti yuridis (yaitu sebagaimana diatur dalam peraturan perundang-undangan tertulis).

Cybercrime meliputi pelanggaran hak kekayaan intelektual, penghinaan atau pencemaran nama baik, pelanggaran terhadap kebebasan pribadi (privacy), ancaman dan pemerasan, ekploitasi seksual anak-anak dan pencabulan, perusakan sistem komputer, pembobolan kode akses, dan pemalsuan tanda tangan digital. Semua perbuatan tersebut dapat dipertanggungjawabkan secara pidana sesuai dengan yurisdiksinya. Cybercrime juga dapat berbentuk

[18]Muladi, Demokratisasi , *Hak Asasi Manusia, dan Reformasi Hukum di Indonesia*, (Jakarta: Habibie Center, 2002), hlm. 196

pemalsuan data, penyebaran virus komputer ke jaringan komputer atau sistem komputer, penambahan atau pengurangan sistem instruksi dalam jaringan komputer, pembulatan angka, perusakan data, dan pembocoran data rahasia. Ini diuraikan oleh Sue Titus Reid, bahwa cybercrime meliputi "*data diddling, the Trojan horse, the salami technique, superzapping, and date leakgage*.

Jonathan Rosenoer menjelaskan tentang bentuk-bentuk cybercrime sebagai berikut:

1. Hak cipta, termasuk hak eksklusif, subjek hak cipta, formalitas, pelanggaran, sumber risiko, situs web word wide, tautan hypertext, elemen grafis, email, pertanggungjawaban pidana, penggunaan wajar, amandemen pertama, dan penyewaan perangkat luna
2. Merek dagang
3. Pencemaran nama baik
4. Privasi, termasuk privasi hukum umum, hukum konstitusional, anonimitas, dan teknologi yang memperluas hak privasi
5. Tugas perawatan : Kelalaian, salah saji yang lalai, kerusakan peralatan, kerugian ekonomi yang mungkin tidak dapat dipulihkan, Batasan tanggung jawab kontrak

6. Tanggung jawab pidana; seperti; penipuan computer dan tindakan penyalahgunaan, penipuan dengan media elektonik (telepon, surel, internet), tindakan privasi komunikasi elektronik, pemerasan dan ancaman, pengungkapan, eksploitasi seksual anak, panggilan telepon cabul
7. Masalah procedural, termasuk yurisdiksi, tempat dan konflik hukum,.
8. Kontrak elektronik dan tanda tangan digital, termasuk perjanjian elektronik yang dapat ditegakkan, enkripsi kunci public dan tanda tangan digital

Selain penggolongan *cybercrime* sebagaimana terjabar di atas, Donn Parker mengklasifikasikan bentuk-bentuk cybercrime ke dalam empat klarifikasi :

1. Komputer sebagai objek,
2. Komputer sebagai subjek
3. Komputer sebagai Alat
4. Komputer sebagai Simbol

1.5.3. Penghinaan di Sosial Media

Penghinaan menurut pengertian umum “menghina” adalah menyerang kehormatan dan nama baik seseorang, akibat dari serangan ini biasanya penderita akan merasa malu, kehormatan yang di maksud disini bukan dalam bidang seksual melainkan kehormatan yang mencakup nama baik. Penghinaan atau dikenal juga pencemaran nama baik pada dasarnya adalah menyerang namabaik dan kehormatan

seseorang yang bukan dalam arti seksual sehingga orang itu merasa dirugikan. Kehormatan dan nama baik memiliki pengertian yang berbeda namun keduanya tidak dapat dipisahkan satu sama lain. karena menyerang kehormatan akan berakibat kehormatan dan nama baiknya tercemar, demikian juga menyerang nama baik akan berakibat nama baik dan kehormatan seseorang dapat tercemar.[19]

Dalam KUHP pasal 310 ayat (1) ketika menyangkut penghinaan harus memenuhi beberapa unsur seperti :

1. Perbuatan menyerang
2. Objek: Kehormatan dan Nama Baik
3. Caranya: dengan menuduhkan Perbuatan tertentu
4. Dengan Sengaja
5. Maksud terang supaya diketahui umum

Dalam Undang - undang Nomor 11 Tahun 2008 (UU ITE) juga telah mengatur mengani ketentuan pencemaran nama baik didalam Pasal 27 ayat (3) dan diancam sanksi pidana berdasarkan pasal 45 ayat (1).

Mahkamah Konstitusi telah memberikan putusan terhadap permohonan judicial *review* pasal 27 (3) Undang – undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi elektronik, dalam perkembangan hukumnya menyatakan bahwa unsur dimuka umum pada pasal 310 ayat 2 KUHP tidak dapat diterapkan didunia maya sehingga memerlukan unsur ekstensif yaitu mendistribusikan dan atau mentransmisikan dan atau membuat dapat diaksesnya informasi

[19] Mudzakir, *Delik Penghinaan dalam Pemberitaan Pers Mengenai Pejabat Publik, Dictum 3, 2004,* hlm.17.

elektronik dan atau dokumen elektronik yang memiliki muatan penghinaan dan atau pencemaran nama baik. Mahkamah Konstitusi menyatakan bahwa pasal – pasal didalam KUHP tidak cukup memadai untuk menjawab persoalan – persoalan hukum yang muncul di Dunia Maya saperti Penghinaan melalui Sosial Media.[20]

1.5.4. Pembuktian Menurut Hukum Acara Pidana

Pembuktian menjadi persoalan yang pelik, yang mana berlandasakan pada kaidah-kaidah hukum dan pengecualian-pengecualian dari kaidah hukum tersebut. Pembuktian menurut pemahaman umum adalah menunjukkan ke hadapan tentang suatu keadaan yang bersesuian dengan induk persoalan, atau dengan kata lain adalah mencari kesesuaian antara peristiwa induk dengan akar-akar peristiwanya. Dalam perkara hukum pidana kesesuaian itu tentu tidak harus diartikan sebagai kesamaan, tetapi dapat juga atau harus diartikan adanya kolerasi, atau adanya hubungan yang saling mendukung terhadap penguatan atau pembenaran karena hukum.

"Membuktikan" mengandung maksud dan usaha untuk menyatakan kebenaran atas suatu peristiwa, sehingga dapat diterima oleh akal terhadap kebanran peristiwa tersebu. Menurut Pitlo, pembuktian adalah suatu cara yang dilakukan oleh suatu pihak atas fakta dan hak yang berhubungan dengan

[20] Sutan Remy Syadeini, *Kejahatan & Tindak Pidana Komputer, (*Jakarta: Pustaka Utama Grafiti, 2009), hlm.34

kepentingannya. Kemudian menurut Abdulkadir Muhammad, Pembuktian adalah menyajikan fakta-fakta yang cukup menurut hukum untuk memberikan kepastian kepada Majelis Hakim mengenai terjadinya peristiwa atau hubungan.[21]

Sistem pembuktian menurut KUHAP tercantum dalam Pasal 183 KUHAP yang menyatakan bahwa : " Hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya " Bahwa berdasarkan rumusan Pasal 183 KUHAP tersebut mengenai sistem pembuktian mengatur bagaimana untuk menentukan salah atau tidaknya seorang terdakwa dan untuk menjatuhkan pidana kepada terdakwa, harus:

a. Kesalahannya dibuktikan sekurangnya dua alat bukti yang sah
b. Setelah terpenuhi kesalahannya dengan sekurangnya dua alat bukti yang sah tersebut hakim memperoleh keyakinan bahwa tindak pidana benar terjadi dan terdakwa yang bersalah melakukannya

Indonesia termasuk dari salah satu dari sekian negara yang menganut sistem Eropa Kontinental, maksudnya hakim yang menilai alat bukti yang diajukan hanya dengan dasar keyakinannya sendiri.

[21] Abdul Kadir Muhammad, *Hukum Acara Perdata Indonesia*, (Bandung :Citra Aditya Bakti, 2000), hlm. 115

Berbeda dengan negara - negara yang menganut sistem Anglo-Saxon. Di negara negara Anglo-Saxon para juri lah yang sebagai penentu apakah seorang terdakwa tersebut bersalah atau tidak. Hakim hanya sebagai pemimpin sidang dan menjatuhkan putusan

Pembuktian merupakan masalah yang memegang perananan dalam proses pemeriksaan sidang pengadilan. Pembuktian tentang tidak benarnya terdakwa melakukan perbuatan yang didakwakan, merupakan bagian yang terpenting atau dapat dikatakan sebagai titik sentral dalam hukum acara pidana. Melalui pembuktian ditentukan nasib terdakwa. Apabila hasil pembuktian dengan alat-alat bukti yang ditentukan undang-undang "tidak cukup" membuktikan kesalahan yang didakwakan kepada terdakwa maka terdakwa "dibebaskan" dari hukuman. Sebaliknya, kalau kesalahan terdakwa dapat dibuktikan derngan alat-alat bukti yang disebutkan pada Pasal 184 KUHAP, terdakwa dinyatakan "bersalah" dan kepadanya akan dijatuhkan hukuman.

Menurut Subekti, Pembuktian adalah upaya meyakinkan Hakim akan hubungan hukum yang sebenarnya antara pihak dalam berpekara, dalam hal ini antara bukti-bukti dengan tindak pidana yang didakwakan, dalam mengkonstruksikan hubungan hukum ini, masing-masing pihak menggunakan alat bukti untuk membuktikan dalil-

dalilnya dan meyakinkan hakim akan kebenaran dalil-dalil yang ditemukan.[22]

1.5.4.1. Pembuktian dalam Tindak Pidana Cyber

Pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang membuktikan kesalahan yang didakwakan kepada terdakwa. Dalam Pasal 184 ayat (1) KUHAP telah ditentukan secara limitatif alat bukti yang sah menurut undang-undang. Di luar alat bukti tersebut, tidak dibenarkan dpergunakan untuk membuktian kesalahan terdakwa. Pembuktian dengan alat bukti di luar jenis alat bukti yang disebut dalam Pasal 184 ayat (1) KUHAP, tidak mempunyai nilai serta tidak mempunyai kekuatan pembuktian yang mengikat.

Telah dijelaskan diatas bahwa Alat bukti yang sah untuk diajukan di depan persidangan, seperti yang diatur Pasal 184 Undang-undang Nomor 8 tahun 1981 Tentang Hukum Acara Pidana (KUHAP) adalah:

1) Keterangan saksi
2) Keterangan ahli
3) Surat
4) Petunjuk
5) Keterangan terdakwa

[22]Subekti, *Hukum Acara Perdata,* (Bandung: Badan Pembinaan Hukum Nasional Departemen Kehakiman- Bina Cipta, 1989), hlm. 78.

Kemudian dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dikenal dengan istilah Informasi Elektronik dan Dokumen Elektronik. Informasi Elektrnik ataupun Dokumen Elektronik ditegaskan pada pasal 1 angka 1 dan angka 4 Undang-Undanf Nomor 11 Tahun 2009 Jo. Undang-undang Nomor 19 Tahun 2019 tentang Informasi Elektronik dan Transaksi Elektronik yang berbunyi :

1. Pasal 1 angka 1 Undang-undang Nomor 11 Tahun 2008 Jo Undang-undang nomor 19 Tahun 2016.
   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. Pasal 1 angka 4 Undang-undang Nomor 11 Tahun 2008 Undang-undang nomor 19 Tahun 2016.
   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.

Selanjutnya pada Pasal 5 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik disebutkan :

1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.
3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang- Undang ini.
4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:

a) surat yang menurut Undang-undang harus dibuat dalam bentuk tertulis; dan
b) surat beserta dokumennya yang menurut Undang-undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Bukti Digital adalah Informasi yang disimpan atau ditransisikan dari bentuk/format digital ke format teks tertulis, video, gambar, dll yang harus dapat dimengerti oleh kalangan umum di saat digunakan dalam sebuah kasus peradilan. Bukti digital tidak bisa begitu saja digunakan sebagai bahan bukti di dalam kasus peradilan. Karena dari itu bukti digital memerlukan tahapan verifikasi sesuai standar hukum bukti digital untuk dijadikan sebagai bahan bukti di sebuah kasus peradilan.

1.5.5. *Cyber Forensic*

1.5.5.1. Pengertian *Cyber Forensic*

Forensik (berasal dari bahasa Latin forensis) yang berarti "dari luar", adalah bidang ilmu pengetahuan yang

digunakan untuk membantu proses penegakan keadilan melalui proses penerapan ilmu atau sains. Dalam bukunya Feri Sulianta mengatakan forensik memilki arti "membawa ke pengadilan". Istilah Forensik adalah suatu proses ilmiah (didasari oleh ilmu pengetahuan) dalam mengumpulkan, menganalisa, dan menghadirkan berbagai bukti dalam sidang pengadilan terkait adanya suatu kasus hukum.[23]

Berbeda dari forensik pada umumnya, *cyber forensic* atau digital forensik adalah pengumpulan dan analisa data dari berbagai sumber daya komputer ini mencakup: Sistem komputer, jaringan komputer, jalur komunikasi (mencakup secara fisik dan wireless), dan juga berbagai media penyimpanan yang dikatakan layak untuk diajukan dalam sidang pengadilan. Digital Forensik menjadi bidang ilmu yang menggabungkan dua bidang keilmuan, hukum dan komputer.[24]

Dalam digital forensic terdapat tiga entitas yang memiliki peran yang sangat penting, yaitu human sebagai aktor yang melakukan aktivitas, digital evidence sebagai objek dan aset vital, dan process sebagai pedoman yang harus diikuti sepanjang proses investigasi digital forensic

[23] Feri Sulianto, *Komputer Forensik,* (Jakarta: Elex Media Komputindo, 2008), hlm.2.
[24] *Ibid*., hlm.3.

berlangsung. Pedoman dalam pelaksanaan investigasi tersebut menggunakan metode ilmiah, artinya dalam setiap tahapan atau langkah yang dilakukan oleh tim investigasi ataupun lembaga hukum harus menjunjung tinggi kaidah metode ilmiah. Dengan berpedoman pada karakteristik metode ilmiah, maka process dalam bidang digital forensic harus mengacu pada langkah-langkah secara prosedural dan terstruktur. Proses dalam digital forensic dikenal dengan digital forensic investigation.

Digital forensic investigation diterapkan setiap dibutuhkan penyelidikan terhadap barang bukti digital sebagai hasil dari suatu insiden, untuk menentukan insiden itu termasuk sebagai kegiatan kriminal atau tidak. Dengan kata lain, *Cyber Forensic* atau digital forensic yakni metode atau teknik untuk mendapatkan bukti ditigal dengan mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik serta disimpan pada *device computer* sehingga dapat dijadikan alat bukti dalam mengungkap perkara yang dapat dipertanggungjawabkan secara hukum.

Menurut National Institute of Standards and Technology (NIST) ada empat tahapan dalam digital forensik yaitu *collection, examination, analysis dan reporting.* Pada

tahap *collection* merupakan tahap pengumpulan data, yang selanjutnya akan di identifikasi, pemberian label, perekaman data yang diperoleh dari sumber data yang relevan dan menggunakan prosedur yang sesuai sehingga integritas data dapat dipertanggunag jawabkan. Selanjutnya adalah tahapan *examination* untuk melakukan pemeriksaan terhadap data yang telah dikumpulkan dengan menggunakan kombinasi metode otomatis dan manual, sehingga dapat menilai dan melakukan ekstraksi data dengan tetap menjaga integritas data. Kemudian adalah tahap melakukan *analysis* menggunakan metode dan melakukan dokumentasi terhadap setiap langkah yang dilakukan, sehingga dapat memperoleh informasi yang berguna dan menjawab masalah-masalah dalam proses pemeriksaan dan pengumpulan data. Tahapan terakhir adalah *reporting* untuk melaporkan hasil dari analisa. tahapan ini meliputi beberapa prosedur diantaranya penjelasan bagaimana data diperoleh, penjelasan dari setiap tindakan yang dilakukan, penjelasan bagaimana alat dan prosedur yang dilakukan dan rekomendasi untuk perbaikan dari proses forensik.

1.5.5.2. *Cyber Forensic* dalam Perkara Pidana

Peran *cyber forensic* atau digital forensik dalam membantu pembuktian suatu kejahatan secara digital

sangatlah penting, namun digital forensik bukan hanya dapat digunakan untuk mengungkap bukti kejahatan digital tapi kejahatan konvensional yang memiliki barang bukti elektronik/digital. Tentunya digital forensik penting untuk menganalisis barang bukti elektronik dari kejahatan komputer (Computer crime) dan/atau kejahatan terkait komputer (Computer related crime).

Kejahatan terkait komputer adalah segala jenis macam kejahatan tradisional seperti pencurian, perampokan, pembunuhan, korupsi, narkoba, dan lain-lain. Sedangkan kejahatan komputer merupakan kejahatan yang menggunakan komputer sebagai alat utama untuk melakukan aksi kejahatannya, misalnya defacement (pengubahan halaman-halaman suatu situs secara ilegal), denial distributed of service (membuat suatu sistem tidak berjalan atau berfungsi sebagaimana mestinya), keylogging (merekam setiap aktivitas pengetikan di keyboard dan aplikasi yang tertampil di layar), identity theft (pencurian data-data penting dari orang-orang yang menjadi target), intrusion (masuk secara ilegal ke dalam suatu sistem), dan lain-lain.[25]

Digital forensik dalam perkara pidana membantu pembuktian suatu kasus kejahatan secara digital. Sesuai

[25] Muhammad Nuh Al-Azhar, *Op.,Cit,* hlm.7.

dengan Pasal 5 ayat (1) Undang-undang Republik Indonesia Nomor 11 Tahun 2008 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 mengungkapkan dalam dunia digital dan elektronik barang bukti yang asli tidak dianalisis, sebabnya barang bukti tersebut harus tetap dijaga, hal itu berbeda dengan membedah tubuh korban.

Pelaku kejahatan dalam kejahatan komputer tentunya dapat saja menghilangkan barang bukti dan berusaha menghindar dari pertanggung jawaban pidana. Penjahat biasanya selangkah lebih maju dari penegak hukum, dalam melindungi diri dan menghancurkan barang bukti. Dalam dunia digital forensik hal tersebut di sebut anti forensik. Untuk itu tugas ahli digital forensik untuk menegakkan hukum dengan mengamankan barang bukti, rekonstruksi kejahatan, dan menjamin jika bukti yang dikumpulkan itu akan berguna di persidangan.

Tujuan utama dari digital forensik adalah untuk mengamankan dan menganalisa bukti digital dengan cara menjabarkan keadaan terkini dari suatu artefak digital. Istilah artefak digital dapat mencakup sebuah sistem komputer,

media penyimpanan (harddisk, flashdisk, CD-ROM), sebuah dokumen elekteronik (misalnya sebuah email atau gambar), atau bahkan sederetan paket yang berpindah melalui jaringan komputer.

1.6. Metode Penelitian

1.6.1. Jenis Penelitian

Penulisan skripsi ini menggunakan metode penelitian yuridis normatif. Peneliti menggunakan metode yuridis normatif karena sasaran penelitian ini adalah hukum atau kaedah. Pengertian kaedah meliputi asas hukum, kaedah dalam arti sempit (value), peraturan hukum konkret. Penelitian yuridis normative adalah penelitian yang berobjekan hukum normatif berupa asas-asas hukum, sistem hukum.

Metode yuridis normatif juga disebut sebagai penelitian doktrinal. yaitu suatu penelitian yang menganalisis hukum baik yang tertulis dalam buku dan yurisprudensi. Berdasarkan metode tersebut, peneliti harus melakukan pengkajian secara logis terhadap ketentuan hukum yang dapat dianggap relevan dengan penelitian skripsi ini.[26]

1.6.2. Sumber Data

Penelitian ini merupakan penelitian normatif yang menitikberatkan pada studi kepustakaan dan data sekunder yang

[26]Amiruddin dan Zainai Asikin. *Pengantar Metode Penelitian Hukum*. (Jakarta: Grafiti Press. 2006), hlm, 118.

terdiri atas bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier:[27]

1. Bahan Hukum Primer

Bahan Hukum Primer adalah dokumen peraturan yang mengikat dan ditetapkan oleh pihak yang berwenang. Dalam penelitian ini bahan hukum primer diperoleh melalui :

a. Kitab Undang – undang Hukum Acara Pidana (KUHAP)
b. Undang – Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
c. Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2016 tentang Administrasi Penyidikan dan Penindakan Tindak Pidana di Bidang Teknologi Informasi dan Transaksi Elektronik
d. Surat Edaran Kejaksaan Agung Republik Indonesia Nomor B-1170/E/EJP/O7/2008 tentang Pola Penanganan Perkara Tindak pidana Informasi dan Transaksi Elektronik
e. Surat Edaran Kepolisian Republik Indonesia Nomor SE/2/11/2021 tentang Kesadaran Budaya Beretika untuk Mewujudkan Ruang Digital Indonesia yang Bersih, Sehat dan Produktif
f. Surat Keputusan Bersama Menteri Komunikasi dan Informatika Republik Indonesia, Jaksa Agung Republik Indonesia, dan

[27] *Ibid.*, hlm.120.

Kepala Kepolisian Negara Republik Indonesia Nomor 229 Tahun 2021 Nomor 154 Tahun 2021 Nomor KB/2/VI/2021 tentang Pedoman Implementasi Atas Pasal Tertentu dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

2. Bahan Hukum Sekunder

Bahan Hukum Seknuder adalah semua dokumen yang merupakan informasi, atau kajian yang berkaitan dengan penelitian ini yakni seperti Jurnal-Jurnal Hukum, Artikel Ilmiah, Karya Tulis Ilmiah, Majalah dan sumber dari Internet

3. Bahan Hukum Tersier

Bahan Hukum tersier adalah dokumen yang berisi konsep – konsep dan keterangan – keterangan yang mendukung bahan ukum primer dan bahan hukum sekunder seperti kamus, ensiklopedia yang relevan dengan penelitian skripsi ini.

1.6.3. Metode Pegumpulan

Metode pengumpulan data yang digunakan dalam penulisan karya ilmiah ini adalah studi kepustakaan (*library research*), yaitu dengan melakukan penelitian terhadap berbagai-bagai sumber bacaan seperti buku-buku pendapat sarjana, bahan kuliah, artikel, dan

beberapa sumber tulisan dari internet yang bertujuan mencari atau memperoleh konsepsi-konsepsi, teori-teori atau bahan-bahan yang relevan dengan penelitian skripsi ini

1.6.4. Metode Analisis Data

Data sekunder yang telah disusun secara sistematis kemudian dianalisa dengan menggunakan metode deduktif dan induktif. Metode deduktif dilakukan dengan membaca, menafsirkan dan membandingkan, sedangkan metode induktif dilakukan dengan menerjemahkan berbagai sumber yang berhubungan dengan topik skripsi ini, sehingga diperoleh kesimpulan yang sesuai dengan tujuan penelitian yang telah dirumuskan.

1.6.5. Lokasi Penelitian

Lokasi penelitian merupakan tempat dimana penelitian dilaksanakan. Penetapan lokasi penelitian merupakan tahap yang penting dalam penelitian kualitatif karena dengan ditetetapkannya lokasi penelitian maka objek dan tujuan telah ditetapkan sehingga akan mempermudah penulis dalam melakukan penelitian. Lokasi dalam penelitian skripsi ini adalah di Lingkungan Fakultas Hukum Universitas Pembangunan Nasional Veteran Jawa Timur, Kepolisian Negara Republik Indonesia Resort Gresik, dan di area Jawa Timur.

1.6.6. Waktu Penelitian

Waktu yang digunakan peneliti untuk penelitian ini dilaksanakan sejak tanggal dikeluarkannya ijin penelitian dalam kurun waktu kurang lebih 2 (dua) bulan, 1 bulan pengumpulan data dan 1 bulan pengolahan data yang meliputi penyajian dalam bentuk skripsi dan proses bimbingan berlangsung.

1.6.7. Sistematika Penulisan

Penulis ingin membahas lebih lanjut, maka penulis akan menjelaskan sistematika penulisannya lebih dahulu,agar penulisan penelitian ini tersusun dengan baik dan sistematis,sehingga mudah untuk dimengerti dan dipahami. Dimulai dari pendahuluan sampai dengan penutup,agar dapat diperoleh hasil yang tepat dan terarah. Pada penulisan ini memiliki kerangka penyusunan akan dibagi menjadi empat bab agar dihasilkan penulisan penelitian yang sistematis. Setiap bab memiliki keterkaitan satu sama lain. Secara lebih jelas dan terperinci akan diuraikan sebagai berikut :

Bab *Pertama*, sebagai bab pendahuluan, didalam bab ini memberikan gambaran secara umum dan menyeluruh tentang pokok permasalahannya. Suatu pembahasan sebagai pengantar untuk masuk ke dalam pokok penelitian yang akan dibahas berisi uraian mengenai latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, kajian pustaka, metode penelitian yang digunakan yuridis

normative, metode penelitian yuridis normative dan sistematika penulisan.

Bab *Kedua*, membahas tentang unsur-unsur tindak pidana penghinaan di social media yang dibagi menjadi 2 sub bab. Sub bab pertama tentang unsur-unsur tindak pidana penghinaan di social media dalam hukum positif di Indonesia. Sub bab kedua mengenai kekuatan pembuktian *Cyber Forensik* sebagai alat bukti dalam suatu tindak pidana penghinaan.

Bab *Ketiga*, membahas tentang pertanggungjawaban pelaku tindak pidana penghinaan di sosial media berdasarkan pembuktian melalui *Cyber Forensic* menurut hukum positif di Indonesia.

Bab *Keempat*, membahas mengenai penutup. Dalam bab ini penulis akan menguraikan beberapa kesimpulan dari penelitian ini yakni unsur-unsur tindak pidana penghinaan di Indonesia serta bagaimana pertanggungjawaban pelaku tindak pidana penghinaan di social media berdasarkan pembuktian melalui Cyber Forensik dan saran yang penulis sampaikan dari permasalahan terkait.