

BAB I

PENDAHULUAN

A. Latar Belakang

Pada dasarnya setiap undang-undang yang dibuat oleh pembuat undang-undang merupakan jawaban hukum terhadap persoalan masyarakat pada waktu dibentuknya undang-undang tersebut. Perkembangan hukum seharusnya seiring dengan perkembangan masyarakat, sehingga ketika masyarakatnya berubah atau berkembang maka hukum harus berubah untuk menata semua perkembangan yang terjadi dengan tertib di tengah pertumbuhan masyarakat modern¹, karena globalisasi telah menjadi pendorong lahirnya era teknologi informasi,² maksudnya adalah perkembangan budaya manusia dewasa ini telah mencapai taraf yang luar biasa, yang di dalamnya manusia bergerak menuju ke arah terwujudnya satu masyarakat manusia yang mencakup seluruh dunia; satu masyarakat global.

Dengan teknologi informasi serba canggih yang berhasil diciptakannya, manusia telah berhasil mengatasi jarak yang dahulu misalkan manusia yang satu dari yang lain, suku bangsa yang satu dari yang lain, bangsa yang satu dari yang lain, budaya dan agama

¹ Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi dan Pengaturan Celah Hukumnya*, (Jakarta: Raja Grafindo Persada, 2012), hlm 1

² *Ibid*, hlm 2

yang satu dari yang lain. Berkembangnya informasi menyebabkan jarak antar kota, antar pulau, antar negara, dan antar benua seolah tidak ada lagi.

Seiring dengan perkembangan kebutuhan masyarakat di dunia, teknologi informasi memegang peran penting, baik di masa kini maupun di masa mendatang. Setidaknya ada dua hal yang membuat teknologi informasi dianggap begitu penting dalam memacu pertumbuhan ekonomi dunia. Pertama, teknologi informasi mendorong permintaan atas produk-produk teknologi informasi, kedua adalah

memudahkan transaksi bisnis terutama bisnis keuangan disamping bisnis-bisnis lainnya.³

Teknologi informasi dengan sendirinya juga merubah perilaku masyarakat. Perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas dan menyebabkan perubahan sosial yang sangat cepat. Sehingga dapat dikatakan teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.⁴

Perbuatan melawan hukum dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, kejahatan dalam teknologi informasi disebut dengan *Cyber Crime*. *Cyber Crime*

³ *Ibid*

⁴ *Ibid*, hlm 3

adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi dan komunikasi tanpa batas, serta memiliki sebuah karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan tingkat keamanan yang tinggi, dari sebuah informasi yang disampaikan dan diakses oleh pengguna internet.⁵

Cyber crime dibagi menjadi 2 kategori, yakni *cyber crime* dalam pengertian sempit dan dalam pengertian luas. *cyber crime* dalam pengertian sempit adalah kejahatan terhadap sistem komputer, sedangkan *cyber crime* dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.⁶ Sebagaimana diatur dalam Pasal 35 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE yang menjelaskan bahwa :

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik”.⁷

Dalam hal ini terdapat tiga pendekatan untuk mempertahankan keamanan di *cyberspace*, pertama adalah pendekatan teknologi, kedua pendekatan sosial budaya-etika, dan ketiga pendekatan hukum.

⁵ Agus Tri P.H. *Cyber Crime dalam Perspektif Hukum Pidana*, Skripsi, Surakarta: UMS, 2010, Hlm. 10.

⁶ Barda Nawawi Arief, *Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: Rajawali Pers, 2006), hlm 25.

⁷ Lihat pada pasal 35 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, atau diakses secara ilegal dan tanpa hak.

Melihat fakta hukum sebagaimana yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga *cyber crime* yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya. Dikatakan teramat penting karena dalam penegakan hukum pidana dasar pembenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana, di samping perbuatannya dapat dipersalahkan atas kekuatan undang-undang yang telah ada sebelumnya (asas legalitas), juga perbuatan mana didukung oleh kekuatan bukti yang sah dan kepadanya dapat dipertanggungjawabkan (unsur kesalahan). Pemikiran demikian telah sesuai dengan penerapan asas legalitas dalam hukum pidana (KUHP) kita, yakni sebagaimana dirumuskan secara tegas dalam Pasal 1 ayat (1) KUHP "*Nullum delictum nulla poena sine praevia lege poenali*" atau dalam istilah lain dapat dikenal, "tiada tindak pidana, tidak ada pidana, tanpa adanya aturan hukum pidana terlebih dahulu"

Perkembangan teknologi yang sangat pesat, membutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan teknologi

tersebut. Sayangnya, hingga saat ini banyak negara belum memiliki perundang-undangan khusus di bidang teknologi informasi (TI), baik dalam aspek pidana maupun perdatanya.

Jika dilihat dari pidananya, Soedjono Dirdjosisworo menyatakan bahwa⁸ :

“Perubahan dan penyesuaian sosial serta perkembangan teknologi selama setengah abad sejak 1985 (UU No.73/58) demikian pesatnya, dan kepesatan perkembangan sosial dan teknologi serta semakin berpengaruhnya globalisasi yang terus didorong oleh teknologi informasi dan komunikasi sangatlah terasa bahwa Kitab-Kitab Hukum Pidana sudah sejak lama tidak mampu secara sempurna mengakomodasi dan mengantisipasi kriminilitas yang meningkat, naik kualitatif, maupun kuantitatif dengan jenis, pola dan modus operandi yang tidak terdapat dalam Kitab Undang-Undang Hukum Pidana (contoh menonjol adalah *Cyber Crime*)”.

Banyak kasus yang membuktikan bahwa perangkat hukum di bidang TI masih lemah, hal ini bisa dilihat dari kendala yuridis dan kendala non yuridis. Kendala yuridisnya yaitu masih belum diakuinya dokumen elektronik secara tegas sebagai alat bukti oleh KUHAP.

Hal tersebut dapat dilihat pada Undang-Undang Nomor 8 Tahun 1981 Pasal 184 ayat (1) bahwa undang-undang ini secara definitif membatasi alat-alat bukti hanya sebagai keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa saja, dan belum adanya kewenangan penyidik untuk menggeledah sistem komputer yang diduga menjadi alat atau sasaran kejahatan.

⁸ Soedjono Dirjosisworo, *Respon Terhadap Kejahatan, Introduksi Hukum Penanggulangan Kejahatan (Introduction to The Law of Crime Prevention)*, (Bandung: STHB Press, 2002), hlm 104.

Sementara itu, kendala non yuridis, yaitu Keterbatasan kemampuan dan jumlah anggota polri yang menguasai bidang teknologi komputer, barang bukti dalam *cyber crime* mudah dihilangkan atau dihapus, adanya kesulitan untuk mendeteksi kejahatan dibidang perbankan yang menggunakan sarana komputer. Kesulitan pendeteksian kejahatan tersebut disebabkan oleh kurang tersedianya peralatan yang memadai, keengganan dari beberapa korban untuk melapor kepada polisi, sistem keamanan dari pemilik aset/sistem yang relatif lemah, sulit melacak keberadaan/domisili pelaku kejahatan.⁹

Berkaitan dengan hal tersebut maka Polri membentuk suatu satuan khusus di tingkat Mabes Polri yang dinamakan Direktorat Tindak Pidana Siber (Ditpidasiber) yang diawaki oleh personel terlatih untuk menangani kasus-kasus semacam ini, tidak hanya dalam teknik penyelidikan dan penyidikan, tapi juga menguasai teknik khusus untuk pengamanan dan penyitaan bukti-bukti secara elektronik. Akan tetapi kemampuan hukum untuk menanggulangi kejahatan mengalami penurunan, hal ini dikarenakan struktur hukum dengan fungsi hukum tidak berkembang secara paralel sehingga penegakan hukum cenderung terus melemah.¹⁰ Sebelum lahirnya Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE), maka

⁹ Aman Nursusila, *Implementasi Penegakan Hukum Terhadap Kejahatan diBidang Komputer*, Malang: Tesis, Program Pasca Sarjana Universitas Brawijaya, 2003, hlm 45.

¹⁰ Mahfud M.D, *Poitik Hukum Nasional*, Bandung: Alumni , 2000, hlm 35

mau tidak mau Polri harus menggunakan pasal-pasal di dalam KUHP, namun saat ini dengan adanya Undang-undang tersebut menjadi dasar hukum Polri untuk menjerat pelaku tindak pidana kejahatan siber.

Polri dalam menindaklanjuti proses hukum tindak pidana kejahatan siber pada tingkat pengadilan tentunya harus disertai pembuktian-pembuktian yang kuat agar dapat menyakinkan hakim sehingga pelaku tidak dengan mudah bebas begitu saja. Pembuktian adalah bagian yang sangat strategis dalam menyelesaikan suatu perkara pidana dan merupakan inti persidangan pidana.

Eddy Hiariej menerangkan bahwa arti penting dari pembuktian pidana adalah terkait dengan mencari kebenaran suatu peristiwa hukum, dan terkait dengan pidana berarti mencari kebenaran yang sesungguhnya atau kebenaran materiil.¹¹ Sistem pembuktian pidana yang dianut dalam acara pidana di Indonesia adalah *negatief wettelijk bewijstheorie*. Teori pembuktian ini dalam menjatuhkan putusan, hakim harus memperoleh keyakinan yang timbul dari alat bukti yang diatur dalam undang-undang.¹² Seperti yang diatur dalam Pasal 183 Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana yang selanjutnya disebut sebagai KUHP bahwa dalam menjatuhkan putusan hakim harus mendasarkan pada minimal sekurang-kurangnya dua alat bukti yang sah dan memperoleh keyakinan tentang peristiwa

¹¹ Eddy O.S. Hiariej, *Teori & Hukum Pembuktian*, (Jakarta, Penerbit Erlangga, 2012, hlm 7.

¹² *Ibid*, hlm 17

tersebut. Teori pembuktian ini juga menjadi acuan hukum acara pidana khususnya pembuktian perkara pidana yang diatur diluar KUHP.

Dalam dunia keamanan komputer pun terjadi perkembangan. Bukti digital yang mulai dijadikan sebagai bukti mulai memunculkan permasalahan yang cukup kompleks. Namun masalah yang paling mendasar dari bukti digital ini adalah tentang keaslian dan integritas bukti digital itu sehingga bukti digital tersebut dapat dipercaya. Untuk dapat mewujudkan hal tersebut muncul sebuah proses investigasi bukti digital yang dikenal dengan forensik digital. Forensik digital adalah metode investigasi dengan pengaplikasian ilmu pengetahuan dan teknologi untuk memeriksa dan menganalisis suatu bukti digital. Ilmu yang merupakan salah satu bagian dari dunia keamanan komputer ini berkembang dengan cepat mengikuti teknologi yang juga berkembang. Proses forensik digital ini akan menemukan suatu bukti digital dari suatu sistem elektronik yang selanjutnya akan dianalisis agar dapat dijadikan bukti yang terpercaya. Output dari proses forensik digital tersebut adalah *digital evidence* itu sendiri serta hasil uji forensik digital.

Berdasarkan uraian tersebut diatas penulis tertarik untuk mengkaji lebih lanjut kedalam bentuk Tesis yang diberi judul **“ANALISIS HUKUM PEMBUKTIAN *DIGITAL FORENSIC* DALAM MENGUNGKAP TINDAK PIDANA *CYBER CRIME*”**

B. Rumusan Masalah

1. Bagaimana Analisis Hukum Pembuktian *Digital Forensic* dalam mengungkap Tindak Pidana *Cyber Crime*?
2. Bagaimana kekuatan alat bukti dalam Tindak Pidana *Cyber Crime*?

C. Tujuan dan Kegunaan Penelitian

1. Tujuan Penelitian

- a. Untuk mengetahui dan menganalisis hukum pembuktian *digital forensic* dalam mengungkap tindak pidana *cyber crime*.
- b. Untuk mengetahui dan menganalisis kekuatan alat bukti dalam tindak pidana *cyber crime*.

2. Kegunaan Penelitian

a. Secara Teoritis

- 1) Memberikan sumbangan ilmu pengetahuan pada umumnya dan ilmu hukum pada khususnya.
- 2) Untuk menambah ilmu pengetahuan mengenai hal-hal yang berkaitan dengan Tindak Pidana *Cyber Crime* yang terjadi di Indonesia.
- 3) Untuk menambah referensi dan bahan masukan untuk penelitian selanjutnya.

b. Secara Praktis

Hasil penelitian ini diharapkan dapat digunakan sebagai ilmu tambahan dan masukan bagi pemerintah khususnya aparat

penegak hukum, mahasiswa, masyarakat umum dan khususnya bagi penulis sendiri.

D. Landasan Teori

1. Teori Pembuktian

Pembuktian berasal dari kata “bukti” yang berarti suatu hal (peristiwa dan sebagainya) yang cukup untuk memperlihatkan kebenaran suatu hal (peristiwa tersebut). Pembuktian adalah perbuatan membuktikan. Adapun dikaji dari makna leksikon, “pembuktian” adalah suatu proses, cara, perbuatan membuktikan, usaha menunjukkan benar atau salahnya terdakwa dalam sidang pengadilan. Sedangkan dikaji dari persektif yuridis, pembuktian juga merupakan titik sentral hukum acara pidana.

Hal ini dapat dibuktikan sejak awal dimulainya tindakan penyelidikan, penyidikan, prapenuntutan, pemeriksaan tambahan, penuntutan, pemeriksaan di sidang pengadilan, putusan hakim bahkan sampai upaya hukum, masalah pembuktian merupakan pokok bahasan dan tinjauan semua pihak dan pejabat yang bersangkutan pada semua tingkat pemeriksaan dalam proses peradilan, terutama bagi hakim. Proses pembuktian pada hakikatnya memang lebih dominan pada sidang di pengadilan guna

menemukan kebenaran materil akan peristiwa yang terjadi dan memberikan putusan seadil mungkin¹³.

Proses pembuktian ada empat sistem pembuktian yaitu sebagai berikut:¹⁴

a. Pembuktian berdasarkan keyakinan belaka (*conviction in time*)

Bersalah atau tidaknya terdakwa menurut teori pembuktian ini semata-mata ditentukan oleh keyakinan hakim. Keyakinan tersebut diambil dan disimpulkan oleh hakim berdasarkan pada alat-alat bukti yang diberikan di persidangan

atau hanya dengan mendengarkan keterangan terdakwa.

b. Pembuktian menurut keyakinan hakim atas alasan yang logis (*conviction raisonee*).

Keyakinan dalam teori pembuktian ini memegang peran penting dalam menentukan salah tidaknya terdakwa, namun keyakinan hakim tersebut harus berdasarkan pada alasan-alasan yang dapat diterima akal dan logis .

c. Pembuktian menurut Undang-Undang secara positif (*positief wettelijk*)

Teori pembuktian ini berpedoman pada prinsip pembuktian dengan alat-alat bukti yang ditentukan oleh Undang-Undang, yang artinya untuk membuktikan terdakwa

¹³ Andi Hamzah, *Hukum Acara Pidana*. (Jakarta : Sinar Grafika: 2001), hlm 247-253

¹⁴ Ibid, hlm 254

bersalah atau tidaknya dengan melihat pada alat-alat bukti yang sah yang telah ditentukan dalam Undang-Undang.

- d. Pembuktian menurut Undang-Undang secara negatif (*negatief wettelijk*)

Teori pembuktian menurut Undang-Undang secara negatif merupakan gabungan dari teori pembuktian menurut Undang-Undang secara positif dengan teori pembuktian dengan keyakinan belaka.

2. Teori Kejahatan Cyber¹⁵

Setiap hukum tujuannya adalah untuk mewujudkan keadilan. Demikian pula dengan hukum cyber. Terdapat beberapa teori untuk memberikan dasar hukum kepada negara dalam kejahatan cyber. Adapun teori-teori tersebut adalah sebagai berikut.

- a. *The Theory of the Uploader and the Downloader*

Berdasarkan teori ini, suatu negara dapat melarang dalam wilayahnya, kegiatan *uploading* dan *downloading* yang diperkirakan dapat bertentangan dengan kepentingannya. Misalnya, suatu negara dapat melarang setiap orang untuk *uploading* kegiatan perjudian atau kegiatan perusakan lainnya dalam wilayah negara, dan melarang setiap orang dalam wilayahnya untuk *downloading* kegiatan perjudian tersebut.

¹⁵ Barda Nawawi Arief, *Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: Rajawali Pers, 2006), hlm 80.

b. Teori Individualisasi

Barda Nawawi berpendapat, individualisasi pemidanaan dibangun berdasarkan ide keseimbangan dalam pemidanaan, yaitu mencakup 4 hal sebagai berikut :

- 1) Keseimbangan monodualistik antara kepentingan umum atau masyarakat dengan kepentingan individu atau perorangan. Dalam ide keseimbangan tersebut, kepentingan umum dan kepentingan individu tersebut tercakup ide perlindungan/kepentingan korban, dan ide individualisasi

pemidanaan.

- 2) Keseimbangan antara unsur objektif (yaitu perbuatan atau lahiriah) dengan unsur subjektif (batiniah atau sikap batin), dan *ide daatdaader strafrecht*.

- 3) Keseimbangan antara kriteria formil dan materiil.

- 4) Keseimbangan antara kepastian hukum dengan kelenturan atau elastisitas atau fleksibilitas dan keadilan.¹⁶

c. Teori Pemidanaan integratif

Berdasarkan hasil penelitian Muladi yaitu teori pemidanaan integratif dikatakan bahwa teori ini mempunyai tujuan yaitu perlindungan masyarakat, pemeliharaan solidaritas

¹⁶ Barda Nawawi Arief, *op cit*, 1998, hlm102

masyarakat, pencegahan umum dan khusus, dan pengimbalan atau pengimbangan.¹⁷

E. Metode Penelitian

1. Jenis Penelitian

Menggunakan jenis penelitian hukum normatif. Penelitian hukum normatif merupakan penelitian yang dilakukan atau berfokus pada norma hukum positif berupa peraturan perundang-undangan.¹⁸

2. Pendekatan penelitian

Metode pendekatan yang diterapkan dalam penelitian ini adalah yuridis empiris. Pendekatan ini mengkaji konsep normatif atau yuridis mengenai proses dan prosedur pembuktian *digital forensics* oleh Polri sesuai dengan peraturan perundang-undangan.¹⁹

3. Sumber Data

Pada penelitian hukum normatif ini, bahan-bahan hukum yang penulis gunakan adalah merupakan data sekunder, yang terdiri dari:

¹⁷ Muladi, *op, Cit*, 1992, hlm 11

¹⁸ Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Cetakan ke – 11. (Jakarta : PT Raja Grafindo Persada, 2009), hlm. 13–14.

¹⁹ *Ibid*

a. Bahan Primer

Berupa peraturan perundang-undangan yang tata urutannya sesuai dengan Tata Cara Pembentukan Peraturan Perundang-Undangan. Bahan hukum primer terdiri atas:

1) Undang-Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana, Pasal 184 ayat (1), perihal alat bukti yang sah, Pasal 39 ayat (1), perihal benda yang dikenakan penyitaan;

2) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan

Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Pasal 44 huruf b, perihal alat bukti lain dalam Undang-Undang Nomor 11 Tahun 2008;

3) Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2016 Tentang Administrasi Penyidikan dan Penindakan Tindak Pidana di Bidang Teknologi Informasi dan Transaksi Elektronik, Pasal 45 ayat (1), perihal bantuan teknis pemeriksaan barang bukti, Pasal 46 tentang pemeriksaan barang bukti dengan pengujian forensik sistem elektronik;

4) Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 10 Tahun 2009 Tentang Tata Cara Dan Persyaratan Permintaan Pemeriksaan Teknis Kriminalistik Tempat Kejadian Perkara dan Laboratoris Kriminalistik Barang Bukti

Kepada Laboratorium Forensik Kepolisian Negara Republik Indonesia;

- 5) Surat Edaran Kejaksaan Agung Republik Indonesia Nomor B-1179|E|EJP/O7/2008 Tentang Pola Penanganan Perkara Tindak Pidana Informasi dan Transaksi Elektronik.

b. Bahan Sekunder

Pendapat hukum yang diperoleh dari buku, jurnal, internet, doktrin, artikel dan asas-asas hukum. Pendapat hukum juga diperoleh melalui beberapa narasumber yaitu ahli forensik

digital Laboratorium Forensik Digital Direktorat Tindak Pidana Siber Bareskrim Polri, Jaksa yang pernah menggunakan hasil uji forensik digital dalam pembuktian dan ahli hukum pidana khususnya tentang pembuktian pidana.

c. Bahan Tersier

Merupakan bahan hukum yang bersifat menunjang bahan-bahan hukum primer dan bahan hukum sekunder seperti KUHAP, kamus hukum, kamus besar Bahasa Indonesia, ensiklopedia, dan lain-lain.²⁰

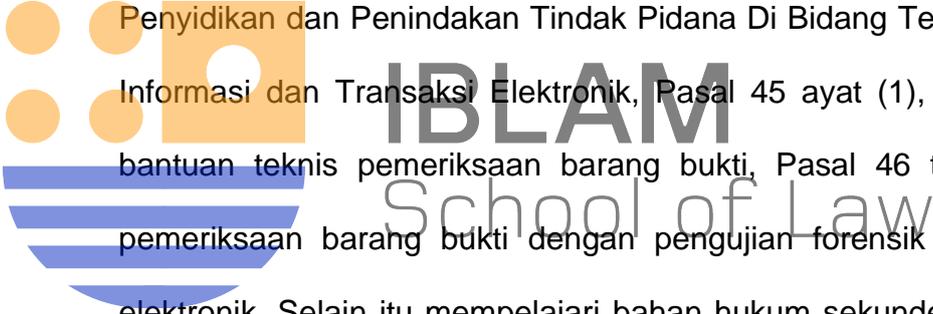
4. Teknik Pengumpulan Data

a. Studi Kepustakaan

Pengumpulan data dengan mempelajari bahan hukum primer yang terdiri atas peraturan perundang-undangan yaitu

²⁰ Syafrinaldi, dkk., *Buku Panduan Penulisan Skripsi*, (Pekanbaru: UIR Press, 2012), hlm 17

ketentuan Pasal 184 ayat (1) KUHP tentang alat bukti peradilan pidana umum dan Pasal 39 ayat (1) tentang benda yang dikenai penyitaan karena terkait juga dengan barang bukti tindak pidana. Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Pasal 44 huruf b, perihal alat bukti lain dalam Informasi dan Transaksi Elektronik dan mengenai bukti elektronik. Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2016 Tentang Administrasi



Penyidikan dan Penindakan Tindak Pidana Di Bidang Teknologi Informasi dan Transaksi Elektronik, Pasal 45 ayat (1), perihal bantuan teknis pemeriksaan barang bukti, Pasal 46 tentang pemeriksaan barang bukti dengan pengujian forensik sistem elektronik. Selain itu mempelajari bahan hukum sekunder yang terdiri atas buku, jurnal, internet, dan dokumen yang berkaitan dengan hasil uji forensik digital, bukti elektronik, dan ahli forensik digital.

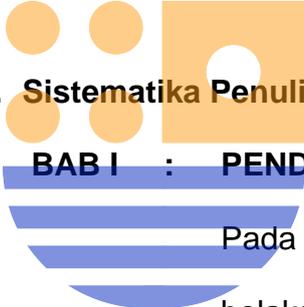
b. Wawancara dengan narasumber

Untuk memperoleh data yang diperlukan maka peneliti telah mengadakan wawancara langsung dengan narasumber yaitu ahli forensik digital Laboratorium Forensik Digital Direktorat Tindak Pidana Siber Bareskrim Polri dan Jaksa dari Kejaksaan Tinggi DKI Jakarta. Wawancara yang dilakukan

berdasarkan pedoman wawancara yang sudah dipersiapkan sebelumnya. Pedoman wawancara yang digunakan adalah pedoman wawancara secara terbuka.

5. Analisis Data

Analisis data yang digunakan dalam penelitian ini adalah analisis secara kualitatif yaitu analisis yang dilakukan dengan cara memahami dan merangkai data-data yang dikumpulkan secara sistematis sehingga diperoleh gambaran mengenai permasalahan yang diteliti.²¹



F. Sistematika Penulisan

BAB I : PENDAHULUAN

Pada bab ini, penulis menjelaskan mengenai latar belakang, rumusan masalah, tujuan dan kegunaan penelitian, landasan teori, metode penelitian serta sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Dalam bab ini dibahas mengenai tinjauan umum mengenai Sistem Pembuktian Perkara pidana, Forensik Digital, Alat bukti, Tindak Pidana *Cyber Crime*.

²¹

Ibid

**BAB III : ANALISIS HUKUM PEMBUKTIAN *DIGITAL FORENSIC*
DALAM MENGUNGKAP TINDAK PIDANA *CYBER*
*CRIME***

Dalam bab ini dibahas dan dianalisis mengenai pembuktian *digital forensic*.

**BAB IV : KEKUATAN ALAT BUKTI DALAM TINDAK PIDANA
*CYBER CRIME***

Dalam Bab ini akan dibahas mengenai kekuatan alat bukti.

BAB V : PENUTUP

Bab ini berisi kesimpulan dan saran.



IBLAM
School of Law