BAB 1

PENDAHULUAN

A. Latar Belakang Masalah

Kemajuan Teknologi sudah mulai berkembang pesat dan perkembangan teknologi tidak dapat dipisahkan dari kemajuan teknologi informasi. Bila menelaah tentang kemajuan Teknologi informasi di zaman sekarang, maka tidak dapat dipisahkan dari perkembangan Teknologi yaitu internet. Internet merupakan penemuan yang mengagumkan merupakan awal dari pencapaian yang telah manusia rasakan untuk saat ini[1] . Karena internet sudah menjadi kebutuhan untuk mencari informasi, dapat di akses kapan pun dan tanpa batas (*Bordeless*). Dimana semua orang berhak menggunakan dan mengakses informasi seluas-luasnya, tidak hanya dari kalangan pelajar, mahasiswa, orang kantoran saja bahkan untuk ibu rumah tangga, pedagang dan sebagainya, juga bisa menggunakannya. Internet berperan besar untuk kehidupan manusia saat ini, karena hampir segala informasi dapat di akses melalui internet. Dari internet kita dapat mengakses hal apapun seperti ilmu pengetahuan, info berita, menu masakan dan sebagainya. Kemajuan teknologi informasi khususnya internet menimbulkan dampak positif bagi kemajuan hidup manusia. Di balik kemudahan yang ditawarkan oleh internet ternyata memiliki sisi gelap.Seperti pada contoh kasus Ahmad Hanafi.Yang awalnya pada sekitar bulan Juni 2011 diajak oleh

[1] Budi Agus Riswandi, " *Hukum dan internet di Indonesia",* (Yogyakarta: UII Press. April 2003) hlm 1.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Fachrizal Ahmad Sumardjo Alias Rizal Dua Gebe/Rizal 2GB (terdakwa yang diajukan dalam penuntutan terpisah) untuk pentest (*Penetration Test*) server Telkomsel. Adapun tugas terdakwa adalah memilah data-data yang biasa dipergunakan dan dimanfaatkan untuk mencari internet gratis, mencari perintah untuk pengisian pulsa serta menjual pulsa. Terdakwa selanjutnya diberi akses berupa internet gratis melalui VPN (*Virtual Private Network*) yang langsung menuju server OVO milik PT Telkomsel dan setelah Fachrizal Ahmad Sumardjo Alias Rizal Dua Gebe/ Rizal 2GB menemukan URL (*Uniform Resource Locator*) Recharge untuk pengisian pulsa secara illegal, kemudian oleh terdakwa digunakan untuk melakukan pengetesan melalui browser internet. Terdakwa selanjutnya tanpa persetujuan PT Telkomsel dengan memakai peralatan PC (*Personal Computer*) rakitan, Harddisk External, kartu AS Telkomsel sebagai modem, Laptop Merk DELL berhasil masuk ke jaringan internal PT Telkomsel dengan mengunakan koneksi APN MMS melakukan tunnelling koneksi ke server F5 (*BigIP*) kemudian menuju ke server OVO dan selanjutnya terdakwa dapat melakukan koneksi ke seluruh server milik PT Telkomsel. Berdasarkan Berita Acara Pemeriksaan Laboratoris Kriminalistik Bukti Digital No.Lab : 14/I/2012/Cyber tanggal 2 Pebruari 2012 yang dilakukan oleh Aditya Cahya S.S.Kom, dari peralatan yang dipergunakan oleh terdakwa diperoleh hasil bahwa terdakwa telah menguasai beberapa dokumen/informasi elektronik milik PT Telkomsel yang bersifat rahasia diantaranya dokumen/informasi elektronik user VOC atau Vasconfig.xlsx, dokumen/informasi elektronik Smaf Server Adress.xlsx dan dokumen/informasi elektronik smaf_code_ref.xlsx. Bahwa

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Terdakwa berhasil masuk ke beberapa server PT Telkomsel untuk dapat terhubung pada server regae dan URP (*Universal Recharge Platform*) dan berhasil melakukan pengisian pulsa milik PT Telkomsel tanpa harus melakukan pembayaran kepada PT Telkomsel. Selanjutnya Terdakwa dengan mengunakan beberapa pesawat handphone, beberapa modem dan beberapa simcard telkomsel. Dengan kejahatan yang dilakukan oleh terdakwa tersebut bisa di kategorikan kejahatan cyber crime.

Menurut Kepolisian Inggris, Cyber Crime adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.[2] Kejahatan dunia maya merupakan istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan menjadi alat, sasaran, atau tempat terjadinya kejahatan. Termasuk ke dalam kejahtan dunia maya, anatara lain adalah penipuan online, pemalsuan cek, penipuan kartu kredit/carding, confidance fraud, penipuan identitas, pornografi anak, dan sebagainya. Namun istilah ini juga digunakan untuk kegiatan kejahatan tradisional di mana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.

Indra Safitri mengemukakan bahwa kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi

---

[2] Abdul Wahid dan Mohammad Labib, ”*Kejahatan*" ,hlm 4

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

yang mengandalakan kepada tingkat keamanan yang tinggi dan kredabilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.[3]

Hacking adalah salah satu bentuk kejahatan komputer yang sering di temukan adalah hacking atau cracking. Kejahatan ini dapat dilakukan dari dalam dan luar negeri. Hacking adalah salah satu kegiatan yang bersifat negatif, meskipun pada awalnya memiliki tuduhan yang mulia yaitu untuk memperbaiki sistem keamanan yang telah di bangun dan memperkuatnya, tetapi dalam perkembangannya hacking digunakan untuk keperluan-keperluan lain yang bersifat merugikan. Dalam perkembangannya dengan di undangkannya UU ITE maka perbuatan hacking di atur dalam pasal 30 yang menentukan :[4]

a. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Eletronik milik orang lain dengan cara apapun.

b. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.

c. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan melanggar, menerobos, melampaui, dan menjebol sistem keamanan.

---

3 Indra Safitri, *" Tindak Pidana di Dunia Cyber"* dalam insider, Legal Journal From Indonesian Capital & Investmen Market.,dalam http://business.fortunecity.com/buffet/842/art18099_tindakpidana.htm.

4 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik,pasal 30

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Adapun sanksi yang di kenakan dari perbuatan hacking ini di atur dalam pasal 46, dimana menentukan :

a. Setiap orang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6(enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)
b. Setiap orang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (2) di pidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah).
c. Setiap orang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (3) dipidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00.

Tabel Kasus Hacking

NO	KASUS HACKING
1	Pada tahun 1983,pertama kalinya FBI menangkap kelompok kriminal komputer The 414s (414 merupakan kode area lokal mereka) yang berbasis di Milmaukee AS. Kelompok yang yang kemudian disebut hacker tersebut melakukan pembobolan 60 buah komputer, dari komputer milik Pusat Kanker Memorial Sloan-Kettering hingga komputer milik Laboratorium Nasioanal Los Alamos. Salah seorang dari antara pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan
2	Digigumi (grup digital) adalah sebuah kelompok yang mengkhususkan diri bergerak dalam bidang game dan komputer dengan menggunakan teknik hexademical untuk mengubah teks yang terdapat di dalam game. Contohnya game chrono trigger berbahasa inggris dapat diubah menjadi bahasa Indinesia, oleh karena itu, status digigumi adalah hacker, namun bukan sebagai perusak.
3	Pada hari sabtu,17 april 2004, Dani Firmansyah, konsultan Teknologi Informasi PT Danareksa di Jakarta berhasil membobol situs milik KPU di http://tnp.kpu.go.id dan mengubah nama-nama partai di dalamnya

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

	menjadi nama-nama unik, seperti partai kolor ijo, partai mbah jambon, partai jambu, dan lain sebagainya. Dani menggunakan teknik SQL Injection(pada dasarnya teknik tersebut adalah dengan cara mengetikkan string atau perintah tertentu di address bar browser) untuk menjebol situs KPU. Kemudian Dani tertangkap pada hari kamis, 22 april 2004.

Bisa diketahui bahwa kalau dilihat perspektif hukum pidana islam (*fiqh jinayah*), cyber crime paling tidak terbagi menjadi dua bagian, yaitu sebagai berikut.

1. Kasus carding di mana pelaku mencuri nomor kartu kredit pemiki orang lain walaupun tidak secara fisik karena hanya nomor kartunya yang diambil dengan menggunakan software card generator di Internet untuk melakukan transaksi di-*e-commerce*. Selanjutnya, kasus permainan judi secara online di internet
2. Masalah penipuan di website, kasus pengancaman dan pemerasan melalui e-mail, pencemaran nama baik dengan menggunakan media internet seperti e-mail, mailing list, penyebaran pornografi di website, penyebaran foto atau film pribadi yang vulgar di internet, kasus deface atau hacking yang membuat sistem milik orang tidak berfungsi. Dalam kasus ini bisa kategorikan pada jarimah ta'zir. Dari berbagai paparan di atas, maka dapat di pahami bahwa kejahatan apapun bentuknya, baik konvesional maupun kejahatan yang dilakukan melaui media internet atau cyber crime tidak akan lepas dari hukuman, karena mengganggu ketertiban umum yang sangat dipelihara oleh islam. Seiring dengan itu di dalam hukum positif dikenal dengan adagium " (*aut punere aut de dere, nullum crimen sine poena*).

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Dengan demikian , cyber crime atau kejahatan dunia maya masuk dalam ranah jarimah ta;zir bukan jarimah qishash dan hudud. Sebab bisa dipastikan bahwa di zaman Rasulullah belum diketemukan teknologi komputer dan internet seperti zaman ini. Maka dari itu tidak ada satu ayat atau hadis pun yang menyebutkan secara eksplisit eksistensi kejahatan dunia maya seperti yang ada di zaman sekarang ini.

Jarimah ta'zir adalah kejahatan-kejahatan yang bentuknya yang ditentukan oleh Ulul Amri tetapi sesuai atau tidak bertentangan dengan nilai-nilai, prinsip-prinsip dan tujuan syariah, seperti peraturan lalu lintas pemeliharaan lingkungan hidup dan memberi sanksi kepada aparat pemerintah yang tidak disiplin. Hukuman ta'zir ialah hukuman yang dijatuhkan atas jarimah-jarimah yang tidak dijatuhi hukuman yang telah ditentukan oleh hukum syariat, yaitu jarimah-jarimah hudud dan qiyas-diyat. Hukuman-hukuman tersebut banyak jumlahnya, yang mulai dari hukuman yang paling ringan samapai paling terberat. Hakim diberi wewenang untuk memilih di antara hukuman-hukuman tersebut, yaitu hukuman yang sesuai dengan keadaan jarimah serta diri pembuatnya.[5]

Pada penelitian ini, penulis memfokuskan pembahasan dalam satu aktivitas dalam dunia maya yaitu hacking/hacker jika di artikan secara sempit yaitu mengakses atau menyusup ke sistem komputer dan sistem elektronik tanpa hak.Hacking sebagai sebuah bentuk telah ada dan berkembang bersama perkembangan teknologi komputer dan internet. Kemajuan teknologi komputer

[5] Ahmad Hanafi, "Asas-asas Hukum Pidana Islam", (Jakarta: Bulan Bintang, 1990),hlm 299.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

dan internet saat ini tidak akan lepas dari Hacking. Sebab awal mulanya hacking merupakan suatu bentuk kegiatan seorang hacker (pelaku hacking biasa disebut hacker) untuk meningkatkan performa, menguji sistem atau mencari bug suatu program komputer dan internet.

Oleh karena itu, hacker diperlukan dengan mengoprek, mengubah-ubah, bongkar-pasang sistem, software atau hardware komputer yang telah dimiliki. Lebih jauh, ternyata budaya hacking di kalangan *geek* (sebutan orang bagi penggila teknologi) ini memberikan manfaat, sebab dengan hacking dapat diketahui kelemahan sistem atau produk software maupun hardware. Sehingga tidak heran jika pengusaha besar komputer mulai melirik orang-orang yang memiki keahlian hacking untuk direkrut. Merekrut hacker bukan tanpa tujuan, melainkan untuk menguji sistem, meningkatkan kwalitas produk dan lain sebagainya dari perusahaan bersangkutan. Inilah sejarah awal munculnya sekolah-sekolah hacker.

Dari penjelasan di atas dapat disimpulkan, hacker bisa berbentuk invidual atau komunitas yang terorganisir. Lambat laun, dengan semakin berkembangnya teknologi komputer dan internet semakin mudah orang mempelajari teknologi informasi, memberi dampak munculnya hacker-hacker baru yang tidak boleh diremehkan keahliannya, walaupun sebagian besar hacker belajar secara otodidak.

Dari sekian hacker, tidak semuanya memiliki niat mulia, ada yang menyertakan kode-kode berbahaya pada suatu software, menyusup ke sistem orang lain dengan niat sekedar iseng hingga yang memiliki maksud tertentu. Di

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

sinilah awal mula bencana, komputer yang dihubungkan oleh internet (jaringan yang terhubung secara global).

B. Identifikasi dan Batasan Masalah

1. Identifikasi Masalah

Berdasarkan latar belakang di atas, maka identifikasi masalah yang muncul adalah :

a. Analisis fiqh jinayah terhadap sanksi pidana hacking menurut UU No 11 Tahun 2008 tentang informasi dan transaksi elektronik (ITE).
b. Penetapan sanksi pidana hacking UU No 11 Tahun 2008 tentang informasi dan transaksi elektronik (ITE).
c. Pertimbangan Hakim dalam Putusan No. 133 / Pid. B / 2012 / PN. Pwk.

2. Batasan Masalah

a. Pertimbangan Hakim dalam Putusan No. 133 / Pid. B / 2012 / PN. Pwk tentang sanksi pidana hacker milik PT Telkomsel?
b. Bagaimana analisis Fiqh Jinayah terhadap sanksi pidana hacker dalam UU no 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) terhadap Putusan No. 133 / Pid. B / 2012 / PN. Pwk?

3. Rumusan Masalah

Dari pemaparan latar belakang dan identifikasi masalah di atas, maka rumusan masalah yang akan dijawab dalam penelitian ini adalah:

1. Bagaimana dasar hukum Pertimbangan Hakim Pengadilan Negeri Purwokerto terhadap Putusan No. 133 / Pid. B / 2012 / PN. Pwk

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Tentang sanksi pidana dalam UU No. 11 Tahun 2008 tentang ITE milik PT TELKOMSEL ?

2. Bagaimana analisis Fiqh Jinayah terhadap dasar hukum Pertimbangan Hakim Pengadilan Negeri Purwokerto Terhadap Putusan No. 133 / Pid. B / 2012 / PN. Pwk Tentang sanksi pidana Hacker milik PT TELKOMSEL ?

4. Kajian Pustaka

Dari hasil telaah kajian pustakaan terhadap hasil penelitian sebelumnnya, penulis tidak menjumpai judul penelitian sebelumnya yang sama yang dilakukan oleh mahasiswa UIN Sunan Ampel Surabaya. Tetapi penulis mendapatkan beberapa hasil penelitian yang sedikit memiliki relevansi terhadap penelitian yang akan penulis lakukan, sebagai berikut:

Pertama ialah yang dilakukan oleh Desi Tri Astutik mahasiswi fakultas Syari'ah program studi Siyasah Jinayah IAIN Sunan Ampel dalam skripsinya yang berjudul "*Tindak Pidana Kejahatan Dunia Mayantara (CyberCrime) Dalam Perspektif Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Fiqih Jinayah*". Penelitian ini dilakukan pada tahun 2008. Didalam skripsinya memaparkan tentang cybercrime pada dasarnya merupakan kejahatan dunia mayantara yang dilakukandengan melalui jaringan internet dengan menggunakan fasilitas komputer. Dalam perspektif hukum pidana Islam (*Fiqh Jinayah*) pemberlakuan UU ITE dapat dikatakan sebagai ketentuan aturan hukum yang menjerat

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

pelaku kejahatan dunia mayantara (*cyber crime*), karena di dalam undang-undang tersebut telah memenuhi unsur-unsur yang ada dalam aturan Fiqh Jinayah.Adapun unsur-unsur tersebut yaitu unsur umum yang terdiri dari (*unsur formil, unsur materil, dan unsur moral*) dan unsur khusus. Penerapan sanksi yang diberikan kepada pelaku cyber crime yaitu dikenakan sanksi ta'zir,dimana sanksi ta'zir meripakan hukuman yang diserahkan kepada Ulil Amri dengan tujuan memberikan rasa jera kepada pelaku jarimah.[6]

Yang kedua ialah oleh khairul anam mahasiswa UIN Sunan Kalijaga, dalam skripsinya yang berjudul "*Hacking menurut Perspektif Hukum Positif dan Hukum Islam*"Penelitian ini dilakukan pada tahun 2009. Didalam skripsinya memaparkan tentang hacking tidak bisa dikategorikan kegiatan terlarang, meskipun memiliki sisi negatif. Dalam hal ini, UU ITE harus merubah perspektif atau lebih tepatnya perlu merombak pasal-pasal yang menentukan kegiatan hacking (termasuk penggunaan tool hacking) harus melalui atau atas izin lembaga tertentu. Sedangkan hukum Islam lebih fleksibel dalam melihat aktivitas hacking, yaitu, dengan tidak mengikat hacker dalam melakukan hacking pada otoritas tertentu (lembaga pemerintah), serta hacking dibolehkan untuk mencapai kemaslahatan yang lebih besar (*saddu az-zari ah*). Mendasarkan pada hal tersebut sangat

---

[6] Desi Tri Astutik,. "*Tindak Pidana Kejahatan Dunia Mayantara (CyberCrime)Dalam Perspektif Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Fiqih Jinayah*", 2008.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

mendesak bagi lembaga terkait untuk mengkaji pasal-pasal dalam UU ITE yang terkait hacking karena sudah tidak relevan lagi. Sedangkan dilihat dari segi studi hukum Islam sudah dapat dikatakan cukup relevan dalam menjawab permasalahan dalam penelitian ini. Namun demikian tetap perlu digalakkan kembali, penelitian terhadap bidang yang sama. Agar hukum Islam dapat lebih menjawab permasalahan kontemporer secara lebih komprehensif dan dapat dijadikan sebagai pembanding bagi hukum positif.[7]

5. Tujuan Penelitian

Adapun tujuan penelitian ini adalah antara lain:

1. Untuk mengetahui dasar pertimbangan hukum Hakim Pengadilan Negeri Purwokerto perkara tentang sanksi pidana Hacker milik PT Telkomsel dalam Putusan Nomor: 133 / Pid. B / 2012 / PN. Pwk.
2. Untuk mengetahui pandangan Fiqh Jinayah dan UU ITE No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terhadap putusan Pengadilan Negeri Purwokerto perkara tentang sanksi pidana Hacker milik PT Telkomsel dalam Putusan Nomor: 133 / Pid. B / 2012 / PN. Pwk.

6. Kegunaan Hasil Penelitian

Kegunaan penelitian ini terdapat dua macam yaitu:

1. Secara Teoritis

[7] Khairul Anam, " Hacking menurut Perspektif Hukum Positif dan Hukum Islam", 2009.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Adapun manfaat dari penelitian ini adalah untuk mengembangkan penelitian terhadap hukum dan *Hacker/Hacking*, yang mampu memperkaya *khazanah* ilmu hukum.Selain itu, manfaat dari penelitian ini adalah untuk memperluas cakupan tidak pidana atau jarimah dalam keilmuan hukum pidana Islam atau mengembangkan sistem hukuman dalam Hukum Pidana Islam.

2. Secara Praktis

Riset ini mampu memberikan solusi alternatif dalam memberikan hukuman yang sesuai bagi pelaku *Hacker/Hacking*yang mengakibatkan cacat fisik maupun gangguan kejiwaan terhadap korban *hacker/hacking* dan memberikan daya pencegahan *hacker/hacking*.

7. Definisi Operasional

Demi mendapatkan pemahaman dan gambaran yang jelas tentang judul dalam penulisan skripsi ini, maka penulis akan menjelaskan beberapa unsur istilah yang terdapat dalam judul skripsi ini, diantaranya:

1. Fiqh Jinayah adalah segala ketentuan hukum mengenai tindak pidana atau perbuatan kriminal yang dilakukan oleh orang-orang mukallaf (orang yang dapat dibebani kewajiban), sebagai hasil dari pemahaman atas dalil-dalil hukum yang terperinci dari Al-Qur'an dan hadis. [8]Dalam penulisan skripsi ini, fiqh jinayah diartikan hukum Islam yang memuat masalah-masalah kejahatan, pelanggaran yang dikerjakan manusia, dan hukuman yang

[8] Zainuddin Ali," *Hukum Pidana Islam"*, (Jakarta: Sinar Grafika, 2009), 1.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

diancamkan kepada pelaku perbuatan tersebut. Dalam istilah ini berupa pendapat ulama tentang konsep uqūbah qisas dan diyat.

2. Sanksi Pidana Hacker dalam Pasal 30 ayat (1-3) yang tercantum dalam Undang-Undang ITE adalah Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Eletronik milik orang lain dengan cara apapun.Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan melanggar, menerobos, melampaui, dan menjebol sistem keamanan.

8. Metode Penelitian

Penelitian ini dapat digolongkan dalam jenis penelitian kualitatif dengan prosedur penelitian yang akan menghasilkan data deskriptif berupa data tertulis dari dokumen, Undang-Undang dan artikel yang dapat ditelaah. Untuk mendapatkan hasil penelitian akurat dalam menjawab beberapa persoalan yang diangkat dalam penulisan ini, maka menggunakan metode:

A. Jenis penelitian

Jenis penelitian ini adalah penelitian Normatif yaitu metode penelitian hukum yang dilakukan dengan meneliti bahan pustaka. Dalam hal ini penelitian ini dilakukan untuk mengidentifikasi konsep sanksi pidana Hacker dalam putusan Pengadilan Negeri Purwokerto Nomor: 133/Pid.B/2012/PN.Pwk. Metode berfikir yang digunakan adalah metode

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

berfikir deduktif (cara berfikir dalam penarikan kesimpulan yang ditarik dari sesuatu yang sifatnya umum yang sudah dibuktikan bahwa dia benar dan kesimpulan itu ditujukan untuk sesuatu yang sifatnya khusus). Dalam kaitannya dengan penelitian normatif disini akan digunakan beberapa pendekatan, yaitu pendekatan perundang-undangan dan pendekatan konsep (*conceptual approach*).

B. Teknik pengumpulan data

Jenis penelitian ini adalah *Library Research* atau studi kepustakaan. Studi kepustakaan merupakan suatu kegiatan yang tidak dapat dipisahkan dari suatu penelitian. Teori-teori yang mendasari masalah dan bidang yang akan diteliti dapat ditemukan dengan melakukan studi kepustakaan. Melalui studi kepustakaan juga dapat diperoleh informasi tentang penelitian-penelitian sejenis atau yang ada kaitannya dengan penelitian, ataupun penelitian yang telah dilakukan sebelumnya, sehingga dapat memanfaatkan semua informasi dan pemikiran-pemikiran yang relevan dengan penelitian yang akan dilakukan.

Karena jenis penelitian ini adalah library research, maka pada tahap pengumpulan data menggunakan bahan-bahan pustaka tentang sanksi pidana Hacker yang relevan dan representatif.

Sebagai data primer adalah putusan Pengadilan Negeri Purwokerto Nomor: 133/Pid.B/2012/PN.Pwk. Sedangkan data sekunder dalam penelitian ini adalah al-Qur'an dan al-Hadits yang merupakan sumber

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Hukum Islam, kitab-kitab Fiqh Jinayah, dan Undang-Undang ITE No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta beberapa buku literatur tentang cyber crime (hacker) sebagai sumber Hukum Positifnya.

C. Data yang dikumpulkan

Agar dalam pembahasan skripsi ini nantinya bisa dipertanggungjawabkan dan relevan dengan permasalahan yang diangkat, data penelitian ini adalah tentang Putusan Pengadilan Negeri Purwokerto Nomor: 133/Pid.B/2012/PN.Pwk.

D. Sumber data

1. Data primer

   Sumber Data Primer : yaitu dokumen yang menguatkan konsep teori dari penulisan skripsi ini adalah dengan memakai dokumen putusan Pengadilan Negeri Purwokerto Nomor: 133/Pid.B/2012/PN.Pwk serta Undang-Undang ITE No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

2. Data sekunder

   Sumber Data Sekunder : adalah data yang digunakan dalam penelitian ini yaitu berangkat dari literatur sebagai konsep teori dari skripsi pertanggungjawaban pidana anak dibawah umur ini, yang berkaitan dengan segala sumber yang memuat informasi tentang obyek penelitian ini. Literatur yang digunakan adalah seperti kitab-kitab fiqh, buku-buku

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

pengetahuan, ensiklopedia, artikel-artikel hukum dan lain sebagainya Teknik pengumpulan data

C. Teknik Pengolahan Data

Penulis akan memaparkan dan mendeskripsikan semua data yang penulis dapatkan dengan tahapan sebagai berikut:

a. *Organizing*: Suatu proses yang sistematis dalam pengumpulan, pencatatan, dan penyajian fakta untuk tujuan penelitian.[9]
b. *Editing* : Kegiatan memperbaiki kualitas data (mentah) serta menghilangkan keraguan akan kebenaran/ketepatan data tersebut.[10]
c. *Coding* : Mengklasifikasi data-data. Maksudnya data-data yang telah diedit tersebut diberi identitas sehingga memiliki arti tertentu pada saat analisis.[11]

D. Teknik Analisis Data

Penulisan ini menggunakan teknik deskriptif, yaitu membuat deskripsi, gambaran, atau menjelaskan secara sistematis atas data yang berhasil dihimpun terkait dengan pembahasan.. Metode yang digunakan dalam menganalisis data dalam skripsi ini menggunakan metode deduktif, yaitu data-data yang diperoleh secara umum yang kemudian dianalisis untuk disimpulkan secara khusus.[12]

9. Sistematika Pembahasan

---

[9] Sonny Sumarsono, "*Metode Riset Sumber Daya Manusia"*, (Yogyakarta: Graha Ilmu, 2004), 66.
[10] Ibid., 97.
[11] Ibid., 99.
[12] M. Arhamul Wildan, "*Metode Penalaran Deduktif dan Induktif"*, dalam arhamulwildan. blogspot.com, diakses pada 12 Maret 2015

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Secara keseluruhan, skripsi ini secara sistematis terbagi menjadi lima bab:

Bab Pertama pendahuluan yang berisi gambaran umum yang berfungsi sebagai pengantar dalam memahami pembahasan bab berikutnya. Bab ini memuat pola dasar penulisan skripsi, untuk apa dan mengapa penelitian ini dilakukan. Oleh karena itu, pada Bab I ini pada dasarnya memuat sistematika pembahasan yang meliputi : latar belakang masalah, identifikasi dan batasan masalah, rumusan masalah, kajian pustaka, tujuan penelitian, kegunaan hasil penelitian, definisi operasional, metode penelitian, dan sistematika pembahasan.

Bab Kedua Berisi tentang kerangka teoritis secara umum sebagai penyorot terhadap obyek bahasan yang didalamnya: sekilas tentang hukum pidana islam, unsur-unsur dalam islam, macam-macam hukuman, tindak pidana hacker, hacker menurut hukum islam dan sanksi pidana hacker dalam fiqh jinayah.

Bab Ketiga Membahas tentang putusan Pengadilan Negeri Purwokerto Nomor: 133/Pid.B/2012/PN.Pwk tentang sanksi pidana hacker milik PT Telkomsel

Bab Keempat Berisi ''Analisis terhadap Putusan Pengadilan Negeri Purwokerto Nomor: 133 / Pid. B / 2012 / PN. Pwk tentang sanksi pidana hacker milik PT Telkomsel menurut fiqh jinayah.

Bab Kelima Merupakan bab penutup yang berisi tentang kesimpulan hasil penelitian dan saran yang diberikan oleh penulis.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id