BAB I
PENDAHULUAN

1.1 Latar Belakang

Kehidupan manusia dimulai pada zaman dahulu, dari yang sederhana hingga saat ini, semakin panjang rentang hidup manusia, semakin rumit teknologinya. Teknologi yang semakin berkembang tentunya banyak merubah tatanan hidup masyarakat. Menurut Michael Barama[1] "Satu sisi, kemajuan teknologi berdampak positif pada kehidupan manusia yang menjadi lebih efektif dan efisien, contohnya dengan adanya *e-commerce*,*e-banking,* serta layanan internet yang lainnya". Disisi lain, dengan adanya dampak positif pasti ada juga dampak negatif yang dirasakan akibat perkembangan teknologi yang semakin maju yaitu munculnya berbagai jenis kejahatan yang dilakukan didunia maya dengan memanfaatkan teknologi komputer dan jaringan internet yang biasa disebut sebagai *cyber crime.*

Cyber crime sendiri terbagi dalam beberapa jenis, yaitu:[2]

1. Pencurian Data
   Biasanya dilakukan untuk memenuhi kepentingan komersial karena ada pihak lain yang menginginkan informasi rahasia pihak lain. Tindakan ini tentu bersifat ilegal masuk ke dalam aktivitas kriminal karena bisa menimbulkan kerugian materil suatu lembaga atau perusahaan.

2. *Digital Terrorism*
   Cyber terorism merupakan tindakan digital yang sedang banyak diperangi oleh negara-negara besar di dunia, termasuk Indonesia. Pasalnya, aktivitas digital terorism kerap kali mengancam keselamatan

[1] Michael Barama, *Tindak Pidana Khusus*. Manado: Unsrat Press, 2016. h. 33.
[2] Ahmad Ramli, *Hukum Telematika*. Tangerang: Unoversitas Terbuka. 2017. h. 42.

warga negara atau bahkan partner yang mengatur jalannya pemerintahan

3. *Checking*
   Checking ialah istilah yang digunakan untuk menyebut penyalahgunaan informasi kartu kredit milik orang lain. Para carder (pelaku checking) biasanya menggunakan akses cartu credit orang lain untuk membeli barang belanjaan secara on the web. Kemudian, barang gratisan tersebut dijual kembali dengan harga murah untuk mendapatkan uang.
4. *Hacking*
   Tindakan berbahaya yang kerap kali dilakukan oleh para programer profesional ini biasanya secara khusus mengincar kelemahan atau celah dari sistem keamanan untuk mendapatkan keuntungan berupa materi atau kepuasan pribadi. Jika menilik dari kegiatan yang dilakukan, hacking sebenarnya tidak selalu memiliki konotasi buruk karena ada pula programmer positif yang menggunakan kemampuannya untuk kegiatan bermanfaat dan tidak merugikan.

Salah satu *cyber crime* yang sering ditemui dan sangat familiar dalam penggunaan teknologi adalah hacking. Mulanya, kegiatan hacking ini dilakukan orang dengan pengetahuan dan kemampuannya yang biasa disebut dengan seorang hacker untuk dapat menguji sistem serta mencari celah-celah yang terdapat pada sistem agar suatu sistem atau program dapat berkembang lebih baik lagi. Seiring dengan perkembangan jaman, banyak orang yang menyalahgunakan pengetahuan dan kemampuannya untuk melakukan perbuatan yang tidak bertanggung jawab untuk mendapatkan keuntungan pribadi. Muncul beberapa klasifikasi mengenai keberadaan hacker yang berkembang sampai saat ini yaitu:[3]

1. *White Hat Hacker*
   White hat hacker yaitu seseorang yang berpengetahuan dan berkemampuan lebih dibidang teknologi yang mengkhususkan dirinya dalam mekanisme untuk kemananan sistem dan jaringan sistem. Biasanya hal ini dilakukan untuk memperkuat mekanisme pada sistem tersebut. *White hat hacker* biasanya dipekerjakan dalam suatu perusahaan

[3] Bambang Hartono, *Hacker Dalam Perspektif Hukum Indonesia*, Universitas Bandar Lampung, 26, 2011, 23–30.

berbasis teknologi yang pastinya untuk meningkatkan keamanan sistem, sehingga hal ini dilakukan secara etis dan legal.

2. *Black Hat Hacker*
   Black hat hacker yaitu seseorang yang berpengetahuan dan berkemampuan lebih dibidang teknologi yang digunakannya untuk mengambil keuntungan pribadi secara *ilegal* atau dengan itikad tidak baik dengan meretas keamanan yang lemah pada suatu sistem atau program. *Black hat hacker* biasanya beraksi dengan mengahncurkan data atau mencegah mereka yang diijinkan untuk menggunakan jaringan tersebut.
3. *Grey Hat Hacker*
   Kelompok ini berubah-ubah dalam melakukan hacking. Terkadang memberikan perlindungan dan solusi terhadap masalah keamanan jaringan, namun dalam kesempatan yang lain dapat menjadi ancaman bagi pertahanan sistem jaringan. Pada umumnya seorang *grey hat hacker* yang beritikad baik melakukan peretasan tersebut untuk mengidentifikasi celah dalam suatu sistem atau program, apabila ditemukan suatu celah pada sistem tersebut, *grey hat hacker* umumnya akan menginformasikan kepada pemilik sistem.

Menurut Muhammad Azief and Ali Aslam *pada bukunya, "Hacke*r sengat sering dikenal dalam perspektif sebagai penjelajah berbagai situs dan "mengintip" data, tetapi tidak merusak sistem komputer, situs-situs orang atau lembaga lain disebut "hektivism".[4] Stigma yang terdapat di masyarakat selalu mengaitkan profesi ini dengan motivasi uang, yaitu dengan menggunakan data kartu kredit orang lain untuk belanja lewat internet. Cara mereka disebut "carder" beroleh data kartu kredit adalah dengan menadah data dari transaksi konvensional, misalnya pembayaran di hotel, biro wisata, restoran, toko dan lain-lain.

Kendati kejahatan ini kerap terjadi namun hingga sekarang belum ada pilar hukum paling ampuh untuk menangani kasus-kasusnya, bahkan perkembangan kejahatan di dunia cyber semakin dahsyat. Selain menggunakan piranti canggih, modus kejahatan *cyber* juga tergolong rapi.Begitu hebatnya kejahatan ini bahkan

[4] Muhammad Azief and Ali Aslam, *Cyber Crime Yang Dilakukan Oleh Hacker Dalam Tinjauan Hukum Kejahatan Internasional*, 2011. h. 2

dapat meresahkan dunia internasional.Dinamika *cybercrime* memang cukup rumit. Sebab, tidak mengenal batas negara dan wilayah.Selain itu, waktu kejahatannya pun sulit ditentukan.

Stigma *hacker* atau peretas ini sering didukung oleh beberapa kasus yang terjadi. Kasus yang akan menjadi sorotan dalam penelitian ini adalah maraknya tren pencurian aset dalam bentuk Bitcoin. Aksi pencurian para peretas tersebut menimbulkan kerugian sebesar lebih dari US$ 610 juta atau setara Rp 8,7 triliun. "Namun demikian, selang beberapa hari setelah peretasan terjadi, para peretas mengembalikan sebagian uang curian, yakni sebesar US$ 263 juta atau sekitar Rp 3,7 triliun".[5]

Poly Network mengatakan dalam sebuah posting blog bahwa para peretas berupaya menunjukkan bahwa terdapat lubang keamanan digital yang harus diperbaiki dan pencurian dana bermaksud untuk menjaganya tetap aman, dengan mengatakan bahwa memasukkan koin ke dalam "akun tepercaya" adalah cara untuk menyoroti *bug* tanpa memberi orang lain kesempatan untuk mengambilnya. "Pada akhirnya, Poly Network mengundang peretas untuk bertindak sebagai kepala penasihat keamanan perusahaan, Para peretas ini sebelumnya mengeksploitasi kerentanan Poly Network, sebuah platform yang terlihat menghubungkan berbagai blockchain sehingga mereka dapat bekerja sama".[6]

Kasus yang terjadi pada Poly Network dapat menjadi suatu kajian yang reflektif dalam perspektif hukum. Seandainya, permasalahan peretasan di atas

[5]https://www.cnbc.com/2021/08/23/poly-network-hacker-returns-remaining-cryptocurrency.html#:~:text=Poly%20Network%2C%20a%20platform%20in,funds%20to%20their%20own%20accounts. Diakses pada 6 Oktober 2021.

[6]https://www.theverge.com/2021/8/23/22638087/poly-network-600-million-stolen-crypto-hack-restored-defi diakses pada 6 oktober 2021

terjadi di Indonesia, terutama yang dilakukan oleh *grey hat hacker* yang melakukan peretasan dengan itikad baik dapat mendapatkan perlindungan hukumnya. Perlindungan hukum bagi para *grey hat hacker* tentunya akan menjadi momentum yuridis yang kelak dapat menjadi pondasi teknis yang kokoh dalam memberantas kejahatan *cyber*. Meskipun, tampaknya bahwa premis ini sangat menarik, nyatanya hukum Indonesia masih memandang semua *hacker* sebagai biang masalah.

Penyamarataan terma *hacker* di Indonesia sendiri terdapat pada pengaturan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya akan disebut dengan UU ITE). Pada pasal 30 UU ITE dengan jelas tertulis sebagai berikut:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Berdasarkan pasal di atas, maka *grey hat hacker* yang memang mengakses dengan sengaja dan tanpa hak, meskipun terdapat itikad baik dan tidak menimbulkan kerugian, tetap saja akan terkena pertanggungjawaban hukum keamanan elektronik. Pasal di atas menunjukkan terma *hacker* yang seharusnya lebih diatur dengan meninjau maksud dan itikadnya tidak terdapat. Sehingga, sekalipun

seorang peretas bermaksud melakukan peretasan dengan tujuan-tujuan yang baik, tetap saja akan terganjar oleh aturan hukum dalam UU ITE.

Hukum keamanan elektronik Indonesia tampak mengartikan kejahatan elektronik dalam perspektif yang sempit, asumsi ini tentu berbekal dari ketiadaan terma yang lebih luas mengenai *hacker*. Perspektif dan konsep mengenai *Cyber crime* dalam perkembangannya ternyata hukum di Indonesia masih banyak yang belum disesuaikan dengan perkembangan Iptek, terutama yang berkaitan dengan tindak pidana. "Harus diakui bahwa Indonesia belum mengadakan langkah-langkah yang cukup signifikan di bidang penegakan hukum (*law enforcement*) dalam upaya mengantisipasi *Cyber crime* seperti dilakukan oleh negara-negara maju di Eropa dan Amerika Serikat".[7] Kesulitan yang dialami adalah pada perangkat hukum atau undang-undang teknologi informasi dan telematika yang belum ada sehingga pihak kepolisian Indonesia masih ragu-ragu dalam bertindak untuk menangkap para pelakunya, kecuali kejahatan mayantara yang bermotif pada kejahatan ekonomi/perbankan. Perancangan hukum yang lebih aplikatif dan terbarukan, menurut Barda Nawari, seharusnya memegang pedoman sebagai berikut:[8]

a. Proses perencanaan dan legislasi nasional dilakukan melalui penelitian dan pengkajian secara mendalam yang meliputi aspek asas- asas, norma, institusi dan seluruh prosesnya yang dituangkan dalam suatu Naskah Akademik peraturan perundang-undangan. Naskah Akademik itu sendiri merupakan landasan dan pertanggungjawaban akademik untuk setiap asas dan norma yang dituangkan dalam rancangan undang-undang.

[7] Ahmad Ridha Kelrey and Aan Muzaki, *Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan*, Cyber Security Dan Forensik Digital, 2.2 (2019), h. 78 <https://doi.org/10.14421/csecurity.2019.2.2.1625>.

[8] Barda Nawawi Arief, Hasil Seminar Hukum Nasional VIII di Bali, 31 Mar 2003. Semarang, Pustaka Magister. h. 3.

b. Penyusunan legislasi harus harmonis secara horisontal dan tidak bertentangan dengan ketentuan yang lebih tinggi secara vertikal. Ketidakkonsistenan terhadap dua unsur tersebut akan berakibat timbulnya biaya tinggi, ketidakpastian hukum, dan konflik kewenangan antar institusi hukum.

c. Naskah akademik dan RUU yang harus dibuat melalui suatu penelitian dengan memperhatikan nilai-nilai ilmiah normatif dan praktik yang terjadi dan secara konsisten memperhatikan dan mendasarkan pada hierarki peraturan perundang-undangan. Oleh karenanya produk hukum harus sesuai dan konsisten dengan kaidah yang ada di dalam UUD 1945. Konsistensi semacam ini akan secara optimal memberikan maslahat bagi bangsa dan negara. Dengan kata lain, aspek filosofis, aspek yuridis dan aspek sosiologis yang disertai keajegan pada landasan filosofis dan konstitusi harus selalu diperhatikan secara cermat dalam pembuatan peraturan perundang-undangan.

d. Proses harmonisasi harus dimulai dari Naskah akademik, salah satu yang harus dimuat dalam naskah akademik adalah adanya pembahasan komparatif RUU yang akan dibuat dan keterkaitannya dengan hukum positif yang ada. Dengan demikian diperlukan adanya suatu regulasi yang mengatur tatacara dan proses pembahasan Naskah Akademik dalam rangka Program Legislasi Nasional.

e. Pembangunan hukum tidaklah terlepas dari sejarah, karena itu dengan telah dimulainya reformasi tidaklah berarti kita memulai segala sesuatunya dari nol. Semua hal yang baik yang ada dalam produk-produk hukum positif yang sudah ada harus menjadi modal pembangunan hukum, sementara yang tidak baik dan tidak sesuai lagi harus kita koreksi dan perbaiki. Pembangunan hukum adalah konsep yang berkesinambungan dan tidak pernah berhenti sehingga masalah keadilan, penegakan hukum dan sikap masyarakat terhadap hukum tidak boleh mengabaikan keadaan dan dimensi waktu saat hukum itu ditetapkan/berlaku, Selain tidak bijaksana, hal tersebut pada gilirannya juga akan berpotensi mengingkari asas dan kepastian hukum itu sendiri. Menafsirkan hukum dengan metode historis selain metode penafsiran lainnya seperti gramatikal dan sistematis adalah penting untuk dilakukan untuk memahami 'roh' hukum yang sesungguhnya.

f. Legislasi yang dilaksanakan dengan baik dapat menjadikan hukum berfungsi menjadi pemberi arah bagi masyarakat untuk menjadi masyarakat yang baik.

Kendati kejahatan ini kerap terjadi namun hingga sekarang belum ada pilar hukum paling ampuh untuk menangani kasus-kasusnya, bahkan perkembangan

kejahatan di dunia *cyber* semakin dahsyat. Selain menggunakan piranti canggih, modus kejahatan *cyber* juga tergolong rapi. Begitu hebatnya kejahatan ini bahkan dapat meresahkan dunia internasional. Dinamika *cybercrime* memang cukup rumit. Sebab, tidak mengenal batas negara dan wilayah.Selain itu, waktu kejahatannya pun sulit ditentukan. Lengkap sudah fenomena *Cyber Crime* untuk menduduki peringkat calon kejahatan terbesar di masa mendatang.

Penilaian itikad baik dalam meninjau kembali terma *grey hay hacker* merupakan tantangan yang besar bagi penegakan hukum Indonesia. "Pada satu sisi, keberadaan *grey hat hacker* masih berada pada posisi yang abu-abu, karena bisa jadi peretas tersebut ketika membobol sistem keamanan digital tidak berpegang pada itikad baik, sehingga situasi ini dapat disamakan dengan delik formil pencurian".[9] Namun, di sisi lain, pada kasus pencurian bit coin Poly Network yang menjadi studi kasus, terdapat itikad baik pada saat setelah perusahaan tersebut kehilangan aset. Maka berdasarkan latar belakang ini, maka penelitian ini akan menganalisis perlindungan hukum terhadap *Grey Hat Hacker* yang ditinjau dari Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

1.2. Rumusan Masalah

Berdasarkan penyusunan latar belakang masalah di atas, maka rumusan masalah yang terdapat dalam penelitian ini adalah sebagai berikut:

[9] Udit Kapadia, Samkit Kundalia, and Meghna M Kanade, *Grey Hat Hacking: Normative Ethical Theories-Based Opinion Piece/Report*, Analysis of Social Media: Ethical and Philosophical. View Project, April, 2020, h. 10.

1. Apakah kasus peretasan Bit Coin seperti pada Poly Network dengan klasifikasi *Grey Hat Hacker* masuk sebagai tindak pidana ITE?
2. Adakah pelindungan hukum bagi *Grey Hat Hacker* yang beritikad baik dalam UU ITE?

1.3. Tujuan Penelitian

Adapun tujuan dari penelitian yang dilakukan oleh peneliti adalah:

a. Tujuan Akademis

Penelitian ini dibuat untuk melengkapi dan merupakan salah satu syarat untuk memperoleh gelar Magister Hukum pada Fakultas Hukum Universitas Pelita Harapan Kampus Surabaya.

b. Tujuan Praktis

1. Untuk mengetahui landasan hukum yang mengacu pada kasus peretasan bitcoin yang termasuk dalam klasifikasi *grey hat hacker* dalam UU ITE.
2. Untuk mengetahui upaya perlindungan hukum *grey hat hacker* dalam UU ITE.

1.4. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat bagi berbagai pihak, yaitu:

1. Diharapkan dapat memberikan tambahan ilmu pengetahuan dan wawasan yang berupa tambahan bukti empiris bagi akademisi dan penelitian lain terkait dengan pengklasifikasian *Grey Hat Hacker* yang masuk sebagai tindak pidana ITE.

2. Diharapkan dapat digunakan sebagai gambaran, bahan pertimbangan dan masukan mengenai pelindungan hukum bagi *Grey Hat Hacker* yang beritikad baik dalam UU ITE.

1.5. Metode Penelitian

A. Tipe Penelitian

Tipe yang digunakan dalam penelitian ini adalah Tipe Yuridis Normatif yaitu suatu proses untuk menemukan suatu aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi dan dilakukan melalui studi pustaka.[10]

B. Pendekatan Masalah

Pendekatan masalah dalam penelitian ini menggunakan pendekatan konsep (*Conceptual approach*), pendekatan Undang-Undang (*Statute approach*), serta pendekatan studi kasus (*Case approach*). *Conceptual approach* adalah pendekatan yang berpatokan dari pandangan dan doktrin-doktrin yang didasarkan dari pendapat para ahli-ahli dan pakar-pakar hukum, yang diimplementasikan pada permasalahan yang sedang diteliti.[11] Kemudian *Statute approach* adalah pendekatan melalui pengkajian peraturan perundang-Undangan yang berkaitan dan diimplementasikan dengan permasalahan yang sedang diteliti.[12] Dan yang terakhir pendekatan secara *Case approach* merupakan pendekatan dengan cara melakukan telaah terhadap kasus yang berkaitan dengan isu yang beredar di masyarakat.

---

[10] Peter Mahmud Marzuki, *Penelitian Hukum,* Kencana, Jakarta, 2010, h.35

[11] Peter Mahmud Marzuki, *Penelitian Hukum,* Prenada Media Group, Jakarta, 2005 h.137

[12] *Ibid*, h. 96

Kajian pokok dalam pendekatan ini adalah perlindungan *grey hat hacker* dalam perundangan hukum telematika di Indonesia, terutama UU ITE.

C. Bahan / Sumber hukum

Bahan/sumber hukum yang digunakan dalam penelitian ini dapat dibedakan sebagai berikut :

1. **Bahan hukum primer,** Indonesia menganut Civil Law System dimana hukum positif seperti Peraturan Perundang-undangan yang digunakan sebagai bahan hukum primer dimana merupakan bahan hukum yang sifatnya mengikat, dalam hal ini yakni :
    a. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
    b. Kitab Undang-Undang Hukum Pidana
    c. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2. **Bahan hukum sekunder,** yang erat kaitannya dengan bahan hukum primer karena sifatnya menjelaskan bahan hukum primer, antara lain yurisprudensi dan asas-asas yang dapat ditemukan dalam literatur tentang bentuk tindakan pengkalsifikasian dan perlindungan hukum terhadap *grey hat hacker.*

D. Langkah Penelitian

a. Pengumpulan Bahan Hukum

Pengumpulan bahan hukum dilakukan dengan inventarisasi, klasifikasi, dan sistematisasi. Langkah inventarisasi dilakukan dengan mengumpulkan bahan hukum terkait melalui pustaka. Bahan-bahan itu diklasifikasikan berdasarkan kebutuhan untuk

menganalisis rumusan masalah. Untuk mempermudah memahami, bahan tersebut disusun secara sistematis.

b. Analisis Atau Pembahasan

Mengingat tipe penilitan menggunakan yuridis normative maka, langkah Analisis menggunakan metode silogisme deduksi, dalam hal ini adalah ketentuan perundang-undangan yang berawal dari pengetahuan yang bersifat umum yang diperoleh dari ketentuan Peraturan Perundang-undangan, yang kemudian diimplementasikan pada rumusan masalah yang kemudian menghasilkan jawaban khusus. Untuk memperoleh jawaban yang benar, akurat, dan logis digunakan beberapa penafsiran, antara lain penafsiran sistematis dan penafsiran otentik. Penafsiran sistematis adalah penafsiran dengan cara melihat/memperhatikan susunan pasal yang berhubungan antara pasal yang satu dengan pasal-pasal yang lainnya, yang ada di dalam undang undang itu sendiri maupun dengan pasal-pasal dari Undang-undang yang lain untuk memperoleh pengertian yang lebih spesifik. Penafsiran otentik adalah penafsiran yang pasti terhadap arti kata yang ditentukan dalam Peraturan Perundang-undangan itu sendiri.

1.6 Pertanggung jawaban Sistematika

Pertanggungjawaban Sistematika dari penelitian skripsi ini terdiri dari IV (empat) bab yang dimana setiap bab dibagi menjadi beberapa sub bab sebagai berikut:

BAB I. PENDAHULUAN. Bagian ini merupakan awal dari penelitian ini dengan mengemukakan latar belakang masalah; berangkat dari studi kasus peretasan Poly Network, maka perlindungan hukum terhadap *Grey Hat Hacker* yang ditinjau dari Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik patut dikaji lebih mendalam. Pada bab ini juma menampilkan rumusan masalah, metode penelitian, hingga sistematika penelitian.

BAB II. PERETASAN *GREY HAT HACKER* MENURUT UNDANG-UNDANG DI INDONESIA. Bab ini terbagi dalam dua sub bab. Dalam sub bab 2.1 Kajian Hacker dan Aktivitasnya dalam Perundangan di Indonesia. Bab ini mengemukakan hacker dan sejumlah kajian mengenai aktivitasnya sesuai dengan perundangan di Indonesia. Hacker memiliki beberapa penjelasan secara definitif yang nantinya akan mempengaruhi klasifikasi jenis dan modus operandinya. Masing-masing klasifikasi tersebut kemudian akan dihubungkan dengan sejumlah perundangan, terutama UU ITE. Pada sub bab 2.2 Kasus Peretasan Bit Coin Poly Network menurut UU ITE. Pada sub bab ini memahami kasus peretasan bit coin pada Poly Network sesuai dengan UU ITE,.

BAB III. ANALISIS PERLINDUNGAN HUKUM PADA *GREY HAT HACKER* YANG BERITIKAD BAIK DALAM UU ITE. Bab ini terdiri dari 2 (dua) sub bab. Pada sub bab 3.1 Analisis Tindak Pidana Cyber dalam Perundangan di Indonesia. Pada sub bab ini menguraikan secara sistematis

tindak pidana cyber sesuai dengan kaidah dalam perundangan di Indonesia, sehingga didapatkan pandangan atau landasan yuridis mengenai aktivitas tersebut di Indonesia. Pada sub bab 3.2 Analisis Perlindungan Grey Hat Hacker dalam UU ITE. Sub bab ini menganalisis mengenai ketersediaan perlindungan hukum bagi *grey hat hacker* yang memiliki itikad baik dalam perundangan di Indonesia. Sub bab ini merupakan upaya menjawab rumusan masalah sesuai ketentuan-ketentuan hukum yang khusus diadakan dan wajib dalam dunia telematika di Indonesia.

BAB IV. PENUTUP. Bab ini terdiri atas Kesimpulan dan Saran. Kesimpulan adalah hasil jawaban singkat atas rumusan masalah yang dikemukakan di atas. Saran adalah masukan yang berguna untuk menyelesaikan kasus-kasus yang sejenis dalam memberikan putusan/vonis yang sesuai. Mengingat ilmu hukum bersifat preskriptif yang selalu membutuhkan masukan, khususnya kepada para penegak hukum.