MENGENAL HACKING SEBAGAI SALAH SATU KEJAHATAN DI DUNIA MAYA

Indah Sari
indah.alrif@gmail.com
Universitas Dirgantara Marsekal Suryadarma

Abstract

Hacking categorized as one of the cybercrime because hacker is a person specialized in programming that can hack a security system in computer or network for a certain purpose. A hacker generally have the knowledge about computer, programming, network, and also hardware. In a cyberworld, hacker is someone which can perform hacking to any device like computer, webcam, smartphone, and router. A hacking that can cause damage to someone is considered as a criminal activity. From this background, the writer elevates two problem from this case. First, why hacking categorized as a cybercrime? Second, how Public Law see hacking as a cybercrime? The kind of typing that the writer uses in this research is descriptive research (describing an object and taking simple conclusion from it) with secondary data and use statute approach, case approach, and conceptual approach. This kind of technique is collected by library research and the data will be analyzed qualitatively. As for the study result, it consists of: the writer found how to distinguish hacking criteria that can be categorized as cybercrime dan see hacking from Public Law perspective

Keywords: *Hacking, Hacker, Cybercrime, and Public Law*

PENDAHULUAN

Hacking merupakan salah satu kegiatan yang bersifat negatif, meskipun awalnya *hacking* memiliki tujuan mulia yaitu untuk memperbaiki sistem keamanan yang telah dibangun dan memperkuatnya.

Tetapi dalam perkembangannya *hacking* digunakan untuk keperluan-keperluan lain yang bersifat merugikan. Hal ini tidak lepas dari pengguna internet yang semakin meluas sehingga penyalahgunaan kemampuan *hacking* juga mengikuti luasnya pemanfaatan internet.

Beberapa tahap *hacking* yang selanjutnya akan digunakan sebagai langkah untuk menentukan tahap-tahap *hacking* yang dapat dikategorikan sebagai kejahatan. Tahap-tahap h*acking* seperti yang dimaksud adalah:

a. Mengumpulkan dan mempelajari informasi yang ada mengenai sistem operasi komputer atau jaringan komputer yang dipakai pada target sasaran.
b. Menyusup atau mengakses jaringan komputer target sasaran.
c. Menjelajahi sistem komputer dan mencari akses yang lebih tinggi.
d. Membuat *backdoor* dan menghilangkan jejak.

Hacker harus memiliki pengetahuan dan kemampuan menguasai serta mengaplikasikan bahasa pemrograman. Pengetahuan dan kemampuan itu dapat diperoleh dengan berbagai cara diantaranya dengan belajar pada ahlinya atau belajar sendiri secara otodidak (Awaludin & Wahono, 2015). Bahasa pemrograman merupakan bahasa teknis, sehingga orang yang benar-benar tidak mempunyai kemampuan teknis akan kesulitan untuk memahami bahasa teknis ini.

Setiap sistem operasi mempunyai kelemahan. Kelemahan itu lambat laun akan diketahui oleh para *hacker* melalui berbagai cara, diantaranya adalah mem-

pelajari sistem operasi tersebut, diskusi dengan sesama *hacker* melalui *mailing list*, *newsgroup* maupun mengambil informasi dari sebuah situs di internet yang menyajikan informasi mengenai kelemahan-kelemahan sistem operasi komputer (Awaludin & Yasin, 2020). Kemudahan memperoleh informasi mempermudah *hacker* dapat mengetahui kelemahan sistem operasi tersebut.

Langkah *hacker* setelah mengetahui sistem operasi apa yang dipakai pada target sasaran adalah menyusup atau mengakses jaringan komputer target sasaran itu. Menyusup atau mengakses jaringan komputer target sasaran ini dilakukan dengan mengeksploitasi kelemahan yang ada pada sistem operasi tersebut. Dengan kata lain *hacker* memasuki situs orang lain tanpa izin. *Hacker* dengan kemampuannya dapat masuk dan berjalan-jalan dalam situs orang lain meskipun situs itu telah dilengkapi dengan sistem keamanan. Tantangan bagi para *hacker* adalah membongkar sistem yang digunakan oleh pemilik situs tersebut.

Jika langkah ini dapat dilakukan, maka merupakan kebanggaan tersendiri bagi *hacker*, setidak-tidaknya merupakan modal untuk mendapat pengakuan mengenai status dirinya dengan sesama *hacker*.

Hacker yang sudah bisa memasuki situs orang lain merupakan kejahatan *cyber crime* karena situs merupakan ruang privat orang yang membuat situs tersebut. Dengan mengacak-acak tampilan yang jauh dari aslinya dan menghapus file-file yang ada di situs tersebut sudah bukan rasa keingintahuan biasa yang dimiliki orang hal ini sudah termasuk dalam kejahatan.

Bertolak dari uraian diatas, maka menarik bagi penulis untuk meneliti lebih lanjut *hacking* sebagai salah satu kejahatan di dunia maya, akhirnya penulis merumuskan dua rumusan masalah sebagai seberikut:

1. Mengapa *hacking* dikategorikan ke dalam salah satu kejahatan di dunia maya?
2. Bagaimana persfektif Hukum Pidana Nasional melihat *hacking* sebagai salah satu kejahatan di dunia maya?

Adapun tujuan dari penulisan ini adalah: *pertama,* untuk mengkaji dan menganalisis lebih dalam lagi mengenai *hacking* sebagai salah satu kejahatan di dunia maya *kedua*, untuk mengetahui dan menjelaskan sejauhmana persfektif Hukum Pidana Nasional melihat *hacking* sebagai salah satu kejahatan di dunia maya

Adapun kegunaan dari penulisan ini adalah:

a. Dapat memberikan wawasan dan pengetahuan bagi dosen, mahasiswa, civitas akademika, praktisi hukum, praktisi sistem informasi mengenai batasan *hacking* sebagai salah satu kejahatan di dunia maya
b. Tulisan ini dapat mendorong penelitian lebih lanjut untuk dapat mengembangkan kajian dan pengetahuan tentang kriteria *hacking* sebagai salah satu kejahatan di dunia maya dan meneliti lebih lanjut juga hacking dalam persfektif Hukum Pidana Nasional.

Adapun sistematika penulisan sebagai berikut: *pertama*, Pendahuluan yang berisikan latar belakang penulisan, rumusan masalah, tujuan penulisan, kegunaan penulisan serta sistematika penulisan, *kedua,* dimana penulis memaparkan kajian-kajian literatur yang mterdiri dari kejahatan, kejahatan di dunia maya,

hacking, hacker dan hukum pidana, *ketiga,* Metode Penelitian yang berisikan jenis penelitian, pendekatan penelitian, jenis data, teknik pengumpulan data, serta metode analisis data. *Keempat*, Pembahasan. Adapun di dalam pembahasan akan di paparkan; bentuk-bentuk *cyber crime*, *hacking* sebagai salah satu kejahatan di dunia maya, *hacking* yang pernah terjadi di dunia, *hacking* yang pernah terjadi di Indonesia, *hacking* dalam persfektif Hukum Pidana Nasional. *Kelima*, Simpulan yang akan menjawab dua rumusan permasalahan yang diangkat dalam penulisan ini.

Berdasarkan uraian di atas akhirnya penulis tertarik untuk mengkaji dan mendalami mengenai "**MENGENAL HACKING SEBAGAI SALAH SATU KEJAHATAN DI DUNIA MAYA**

KAJIAN LITERATUR

Kejahatan

Secara empiris definisi kejahatan dapat dilihat dari dua persfektif, *pertama* adalah kejahatan dalam persfektif yuridis, kejahatan di rumuskan sebagai perbuatan yang oleh negara diberi pidana. Pemberian pidana ini dimaksudkan untuk mengembalikan keseimbangan yang terganggu akibat perbuatan itu (B. Simanjuntak, 1981:70). Perbuatan atau kejahatan yang demikian itu dalam ilmu hukum pidana biasa disebut dengan tindak pidana (*straftbaarfeit*). *Kedua*, kejahatan dalam arti (persfektif) sosiologis (kriminologis) merupakan suatu perbuatan yang dari sisi sosiologis merupakan kejahatan sedangkan dari yuridis (hukum posistif) bukan merupakan suatu kejahatan (B.Simanjuntak, 1982:70). Artinya perbuatan tersebut oleh negara tidak dijatuhi pidana. Perbuatan ini dalam ilmu hukum pidana disebut dengan *strafwaardig*, artinya perbuatan tersebut patut atau pantas dipidana. Ini dikarenakan penjatuhan pidana merupakan upaya untuk mengembalikan keseimbangan yang terganggu akibat perbuatan (kejahatan) tersebut.

Batasan kejahatan menurut Bonger adalah perbuatan yang sangat anti sosial yang memperoleh tantangan dengan sadar dari negara berupa pemberian penderitaan (hukuman atau penderitaan). selanjutnya Bonger mengatakan "Kejahatan merupakan sebagian dari perbuatan immoral. Oleh sebab itu maka perbuatan immoral adalah perbuatan anti sosial. Namun demikian haruslah dilihat juga bentuk tingkah lakunya dan masyarakat, sebab perbuatan seseorang tidaklah sama dan suatu perbuatan immoral belum tentu dapat dihukum" (B. Simandjuntak & I.L. Pasaribu, 1984: 45).

Van Bammelen merumuskan, kejahatan adalah tiap kelakuan yang bersifat tidak susila dan merugikan, dan menimbulkan begitu banyak ketidaktenangan dalam suatu masyarakat tertentu, sehingga masyarakat itu berhak untuk mencelanya dan menyatakan penolakannya atas kelakuan itu dalam bentuk nestapa dengan sengaja diberikan karena kelakuan tersebut (B. Simandjuntak, 1981: 72).

Sebuah kejahatan pastilah mengandung unsur Perbuatan Melawan Hukum (PMH). Di dalam Hukum Pidana Perbuatan Melawan Hukum (PMH) dicirikan: *pertama*, perbuatan melawan hukum pidana sering disebut *Wederrechttelijk, kedua*, dasar hukum pengaturannya terdapat pada Kitab Undang-Undang Hukum Pidana (KUHP), *ketiga*, sifat melawan hukum pidana bersifat publik artinya ada kepentingan umum yang dilanggar (disamping juga kepentingan individu), *keempat*, unsur-unsur perbuatan melawan hukum dalam hukum pidana adalah perbuatan yang melanggar undang-undang, perbuatan yang dilakukan

di luar batas kewenangannya atau kekuasaannya dan perbuatan yang melanggar asas-asas umum yang berlaku di lapangan hukum.

Kejahatan di dunia maya

Kejahatan di dunia maya atau *Cyber Crime* adalah tindak pidana kriminal yang dilakukan pada teknologi internet (*Cyber Space*), baik yang menyerang fasilitas umum maupun kepemilikan pribadi. Secara teknik dapat dibedakan menjadi *offline crime*, *semi online crime*, dan *cyber crime*. Contoh dari *offline crime* adalah dengan cara yang sederhana misal mencuri dompet seseorang untuk kemudian diambil kartu kreditnya, atau bekerjasama dengan kasir untuk mencatat nomor kartu kredit seseorang kemudian menduplikatnya. Contoh teknik *semi online crime* adalah memasang *skimming* di mesin ATM untuk mencuri informasi kartu debit korban. Sedangkan untuk *cyber crime* orang pelaku dan korban tidak perlu bertatap muka, dan bersentuhan, yaitu dengan menggunakan teknologi yang canggih, seperti penggunaan situs palsu klik BCA, dll. Masing-masing teknik memiliki karakter tersendiri, namun perbedaan utama diantara ketiganya adalah keterhubungan dengan jaringan informasi publik (internet).

Cyber crime dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi. *The Prevention of Crime and The Treatment of Offlenderes* di Havana, Cuba pada Tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada 2 istilah yang dikenal:

1. *Cyber crime* dalam arti sempit disebut *computer crime*, yaitu perilaku illegal/melanggar yang secara langsung menyerang sistem keamanan komputer dan/atau data yang diproses dari komputer.
2. *Cyber crime* dalam arti luas disebut *computer related crime*, yaitu perilaku illegal/melanggar yang berkaitan dengan sistem komputer atau jaringan.

Dalam Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders yang diselenggarakan di Vienna, 10-17 April 2000, dibahas kategori *cyber crime*. *Cyber crime* dapat dilihat secara sempit maupun secara luas, yaitu:

a. *Cyber crime in a narrow sense ("computer crime"): any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them;*
b. *Cyber crime in a broader sense ("computer-related crime"): any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.*

Dari penjelasan-penjelasan tersebut, *cybercrime* dapat berupa kejahatan baru yang tidak diatur dalam undang-undang pidana konvensional, dan juga dapat berupa kejahatan konvensional yang menggunakan sarana komputer atau sistem komputer.

Dari beberapa pengertian di atas, *cyber crime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

Hacker

Hacker merupakan orang yang menguasai pemprograman yang dapat melakukan *hacking* atau peretasan sistem keamanan pada komputer atau jaringan dengan tujuan tertentu. Seorang *hacker* umumnya memiliki pemahaman tentang komputer, pemprograman, jaringan, dan juga perangkat keras lebih lanjut. Dengan memahami apa sebenarnya *hacker* atau peretas tentu akan menjadi paham bahwa peretas atau kegiatan peretasan tidak selalu dihubungkan dengan kejahatan dunia maya. Di dalam dunia *Cyber*, peretas merupakan orang yang dapat melakukan peretasan perangkat misal seperti komputer, webcam, ponsel, sampai router. Tindakan peretasan yang menimbulkan kerugian suatu pihak merupakan kegiatan kriminal. Seorang *hacker j*uga memiliki arti lain yaitu seseorang dengan keahlian komputer di atas rata-rata dan punya ketertarikan besar terhadap sistem keamanan dan pertahanan komputer. Seorang *hacker* memiliki kemampuan membuat *software* atau bisa dibilang seorang *software developer.*

Jenis-Jenis *Hacker*

1. *Hacker* Topi Hitam
   Hacker topi hitam ini merupakan hacker atau peretas yang bisa dibilang ilegal. Umumnya hacker topi hitam mengirim ancaman kepada korban atau suatu perusahaan yang akan diretas sistemnya. Hacker ini akan sengaja mengakses sistem keamanan secara ilegal seperti jaringan atau sistem keamanan. Dengan maksud jahat, hacker topi hitam akan melakukan kejahatan seperti mencuri data, menyebarkan malware, dan juga mengambil keuntungan secara pribadi dengan penggunaan ransomware. Selain itu mereka juga melakukan perusakan sistem dengan tujuan untuk mendapatkan nama tenar.
2. *Hacker* Topi Putih
   Hacker satu ini merupakan hacker yang dapat dibilang resmi yang biasanya melakukan kegiatan peretasan dengan seizin pemilik sistem. Dia akan melakukan pengujian atau pengetesan keamanan sistem. Di Indonesia sendiri terdapat kelompok hacker topi putih yaitu ethical hacking Indonesia yang memiliki tujuan baik dengan memperbaiki celah sistem keamanan.Perusahaan, organisasi, atau software developer umumnya menggunakan jasa dari hacker topi putih untuk melakukan pengujian kekuatan keamanan sistem yang mereka gunakan atau mereka buat. Apabila masih ada celah atau ada bagian yang dapat diretas, maka hacker topi putih akan memberikan penjelasan dan meningkatkan sistem keamanannya.
3. *Hacker* Topi Abu-abu
   Untuk hacker topi abu-abu ini bisa dibilang berada di tengah-tengah antara hitam dan juga putih. Motif awal hacker ini memiliki kesamaan seperti topi hitam dan putih. Walaupun umumnya hacking topi abu-abu ini tidak memiliki motivasi untuk mendapatkan tenar atau uang, tetapi mereka akan menawarkan korban untuk memperbaiki sistem yang masuk lemah.Akan tetapi kadang peretas topi abu-abu juga mencari keuntungan ilegal dengan memanfaatkan celah sistem dari korban dan mengeksploitasi kerentanan tersebut untuk bisa mendapatkan keuntungan pribadi.
4. *Hacker* Topi Merah
   Hacker satu ini dapat dibilang hacking bermata elang atau umumnya melakukan peretasan yang main hakim sendiri seperti peretas etis. Tujuan peretasan yang dilakukan

kelompok topi merah adalah menghentikan serangan ilegal dari pelaku peretasan. Secara umum kelompok topi merah punya niatan yang sama dengan hacker etis yang mana membantu korban yang mendapat ancaman peretasan. Tetapi cara yang dilakukan cukup ekstrim dengan menyebar serangan ke sistem lawan atau peretas lain yang melakukan ancaman kepada korban.

5. *Hacktivits*
   Jenis hacker satu ini merupakan hacker yang melakukan peretasan dengan tujuan menyerang serangan untuk mempengaruhi perubahan politik. Tujuannya adalah dengan menarik perhatian banyak publik yang dinilai merupakan pelanggaran etika. Hacktivits akan membocorkan bukti kesalahan dan juga mempublikasikan bukti seperti gambar, informasi, dan komunikasi pribadi.
6. *Script Kiddies*
   Hacker satu ini merupakan seorang hacker amatir dan tidak memiliki banyak pengalaman yang mencoba menggunakan suatu skrip. Umumnya hacker ini merupakan seorang penggemar hacker terkenal yang mencoba meniru idolanya dengan melakukan peretasan yang sedikit menimbulkan kerusakan.

Jenis-Jenis Serangan *Hacking* adalah:

1. Phising
   Peretasan satu ini cukup sering kita jumpai, khususnya di banyak sosial media. Phising merupakan peretasan dengan tujuan mencuri data email korban dengan membuat suatu website yang tampaknya resmi dan berasal dari organisasi sah.Korban secara tidak sadar atau dengan paksaan mengisi data-data pribadi seperti email, password email, tanggal lahir, detail kartu kredit, nomor Jaminan Sosial, dan masih banyak lagi.
2. Dos dan DdoS
   Hacking satu ini membuat korban tidak dapat mengakses sistem, jaringan, atau TI lainnya yang mereka miliki. Seorang peretas ilegal atau kriminal umumnya menggunakan teknik serangan ini dengan tujuan merusak sistem, server web, dan juga mengganggu lalu lintas jaringan korban dengan serangan DDOS.
3. DNS Spoofing
   Jenis peretasan satu ini umumnya dilakukan dengan cara mengeksploitasi DNS dan server web client dengan membuat laju internet menuju ke server palsu.
4. Injeksi Keylogger
   Keylogging program umumnya disuntikan atau disebarkan menggunakan hacking tools ke korban sebagai malware yang bisa memantau atau merekam semua ketikan yang dilakukan korban. Hal ini tentu bisa memberikan banyak informasi penting kepada hacker dan bisa melakukan pencurian data pribadi seperti kredensial login, data perusahaan, dan masih banyak lagi.
5. Serangan Brutal
   Jenis peretasan satu ini umumnya memanfaatkan alat yang digunakan untuk menebak berbagai kombinasi seperti nama pengguna, kata sandi, maupun kode kombinasi lainnya dengan benar untuk tujuan pembobolan sistem.
7. Perbaikan UI
   Peretas satu ini bisa juga dikenal dengan clickjacking, dimana hacker akan membuat IU atau tautan palsu di dalam sebuah website resmi. Tujuannya adalah agar pengunjung website mengklik tautan palsu tersebut, sehingga hacker bisa mengakses komputer korban tanpa diketahui.

Hacking

Hacking adalah kata yang mengacu pada aktivitas yang berupaya menyusupi perangkat digital, seperti komputer, smartphone (ponsel cerdas), tablet, dan bahkan seluruh jaringan. Ini berarti peretasan (dalam bahasa Indonesia) dan mungkin tidak selalu digunakan untuk tujuan jahat. Walaupun saat ini sebagain besar referensi tentang *hacking* (peretasan) dan *hacker* (peretas), mencirikan mereka sebagai aktivitas yang melanggar hukum. Ini biasanya dilakukan karena dimotivasi oleh keuntungan finansial, protes, pengumpulan informasi (mata-mata), dan bahkan hanya untuk kesenangan atau hobi dari tantangan tersebut. Dalam dunia teknologi, *hacking* atau meretas juga berarti membobol komputer seseorang secara ilegal. Kata *hack* atau retas berasal dari kata Inggris kuno yaitu adalah "haccian" yang berarti dipotong-potong, tetapi *hack* (retas) juga berarti sering diartikan batuk. Dahulu kala *hack* ini digunakan singkatan "kuda biasa" dan sekarang menjadi sebuah kata yang mengacu pada kejahatan walaupun tidak 100 % seperti itu.

Hukum Pidana

Beberapa pendapat pakar hukum dari barat (Eropa) mengenai Hukum Pidana antara lain sebagai berikut:

1. POMPE, menyatakan bahwa Hukum Pidana adalah keseluruhan aturan ketentuan hukum mengenai perbuatan-perbuatan yang dapat dihukum dan aturan pidananya (Bambang Poernomo, 1993:9)
2. APELDOORN, menyatakan bahwa hukum Pidana dibedakan dan diberikan arti: Hukum Pidana Materiil yang menunjuk pada perbuatan pidana yang oleh sebab peraturan itu dapat dipidana, dimana perbuatan pidana itu mempunyai dua bagian, yaitu:
   a. Bagian objektif merupakan suatu perbuatan atau sikap yang bertentangan dengan hukum pidana positif, sehingga bersifat melawan hukum yang menyebabkan tuntutan hukum dengan ancaman pidana atas pelanggarannya.
   b. Bagian subjektif merupakan kesalahan yang menunjuk kepada pelaku untuk dipertanggung-jawabkan menurut hukum.
   c. Hukum pidana formal yang mengatur cara bagaimana hukum pidana materiil dapat ditegakkan.

Beberapa pendapat pakar hukum Indonesia mengenai Hukum Pidana, antara lain sebagai berikut:

1. MOELJATNO mengatakan bahwa Hukum Pidana adalah bagian daripada keseluruhan hukum yang berlaku di suatu negara yang mengadakan dasar-dasar dan aturan untuk:
   a. Menentukan perbuatan mana yang tidak boleh dilakukan, yang dilarang, yang disertai ancaman atau sanksi yang berupa pidana tertentu bagi barang siapa melanggar larangan tersebut.
   b. Menentukan kapan dan dalam hal-hal apa kepada mereka yang telah melanggar larangan-larangan itu dapat dikenakan atau dijatuhkan pidana sebagaimana yang telah diancamkan
   c. Menentukan dengan cara bagaimana pengenaan pidana itu dapat dilaksanakan apabila ada orang yang disangka telah melanggar larangan tersebut. (Bambang Poernomo, 1985: 19-22).
2. SATOCHID KARTANEGARA, bahwa Hukum Pidana dapat dipandang dari beberapa sudut, yaitu:
   a. Hukum Pidana dalam arti objektif, yaitu sejumlah peraturan yang mengandung

b. larangan-larangan atau keharusan-keharusan terhadap pelanggarannya diancam dengan hukuman.
c. b.Hukum Pidana dalam arti subjektif, yaitu sejumlah peraturan yang mengatur hak negara untuk menghukum seseorang yang melakukan perbuatan yang dilarang.

METODE PENELITIAN

Jenis penelitian (tipologi penelitian) atau metode penelitian yang dipergunakan dalam penelitian ini adalah dilihat dari segi sifatnya, penelitian ini adalah penelitian deskriptif, artinya penelitian yang menggambarkan objek tertentu dan menjelaskan hal-hal yang terkait dengan atau melukiskan secara sistematis fakta-fakta atau karakteristik populasi tertentu dalam bidang tertentu secara faktual dan cermat. Penelitian ini bersifat deskriptif karena penelitian ini semata-mata menggambarkan suatu objek untuk mengambil kesimpulan-kesimpulan yang berlaku secara umum.

Pendekatan penelitian (*approach)* yang digunakan dalam penelitian ini yaitu pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach),* pendekatan perbandingan (*comparative approach*)

Adapun jenis data yang digunakan dalam penelitian ini adalah data sekunder yang diperoleh dari bahan hukum primer dan sekunder. Sedangkan teknik pengumpulan data dilakukan secara studi kepustakaan (*library research*). Studi kepustakaan dilakukan untuk mencari dan memperoleh data sekunder adalah berupa studi dokumen. Alat pengumpulan data berupa studi dokumen tersebut dilakukan agar dapat mengetahui sebanyak mungkin pendapat atau konsep para ahli yang telah melakukan penelitian dan penulisan tentang *hacking s*ebagai salah satu kejahatan di dunia maya. Kemudian metode analisis data yang dipergunakan adalah metode analisis *kualitatif.* Penelitian kualitatif adalah penelitian yang bersifat menyeluruh dan merupakan satu kesatuan bulat (*holistic*), yaitu meneliti data yang diperoleh secara mendalam dari berbagai segi

PEMBAHASAN

Adapun hasil pembahasan yang penulis paparkan dalam penelitian ini adalah yang berkaitan dengan *hacking* sebagai salah satu kejahatan di dunia maya, peristiwa *hacking* yang pernah terjadi di dunia, peristiwa *hacking* yang pernah terjadi di Indonesia, *hacking* dalam persfektif hukum pidana.

Bentuk-Bentuk *Cyber Crime*

Adapun jenis-Jenis kejahatan *Cyber Crime* dapat berupa:

1. *Hacking* adalah kegiatan menerobos program komputer milik orang/pihak lain. *Hacker* adalah orang yang gemar mengotak-atik komputer, memiliki keahlian membuat dan membaca program tertentu, dan terobsesi mengamati keamanan (security)-nya. "*Hacker*" memiliki wajah ganda; ada yang budiman ada yang pencoleng. "*Hacker*" budiman memberi tahu kepada programer yang komputernya diterobos, akan adanya kelemahan-kelemahan pada program yang dibuat, sehingga bisa "bocor", agar segera diperbaiki. Sedangkan, *hacker* pencoleng, menerobos program orang lain untuk merusak dan mencuri datanya.
2. 2.*Cracking* adalah *hacking* untuk tujuan jahat. Sebutan untuk "*cracker*" adalah "*hacker"* bertopi hitam *(black hat hacker)*. Berbeda dengan "carder" yang hanya mengintip kartu kredit, "*cracker"* mengintip simpanan para nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntu-

ngan diri sendiri. Meski sama-sama menerobos keamanan komputer orang lain, "*hacker*" lebih fokus pada prosesnya. Sedangkan "*cracker*" lebih fokus untuk menikmati hasilnya.

3. *Cyber Sabotage* adalah kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.
4. 4.*Cyber Attack* adalah semua jenis tindakan yang sengaja dilakukan untuk mengganggu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersedian (*availability*) informasi. Tindakan ini bisa ditujukan untuk mengganggu secara fisik maupun dari alur logis sistem informasi.
5. *Carding* adalah berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data di internet. Sebutan pelakunya adalah "carder". Sebutan lain untuk kejahatan jenis ini adalah *cyberfraud* alias penipuan di dunia maya.
6. *Spyware* adalah program yang dapat merekam secara rahasia segala aktivitas *online user,* seperti merekam *cookies* atau *registry*. Data yang sudah terekam akan dikirim atau dijual kepada perusahaan atau perorangan yang akan mengirim iklan atau menyebarkan virus.

Hacking sebagai salah satu kejahatan di dunia maya

Hacking merupakan suatu seni dalam menembus sistem komputer untuk mengetahui seperti apa sistem tersebut dan bagaimana berfungsinya, sebagaimana dikatakan Revelation Loa-Ash: *"Hacking is the act of penetrating computer system to gain knowledge about the system and how it works. Hacking is illegal because we demand free access to* ***ALL*** *data, and we get it. This pisses people off and we are outcasted from society, and in order to stay out of prison, we must keep our status of being a hacker/phreaker a secret."*

Hacking adalah ilegal karena masuk dan membaca data seseorang dengan tanpa izin dengan cara sembunyi-sembunyi sama saja dengan *pissing people off* atau membodohi orang, sehingga para *hacker/phreaker* selalu menyembunyikan identitas mereka. Namun jika di dalami tidaklah demikian, karena di lingkungan para *hacker* ada budaya dan aturan-aturan tertentu, serta memiliki motif dan tujuan yang berbeda, disebutkan oleh pakar *hacker* Emmanuel Goldstein dari Amerika Serikat bahwa: *"One of the common misconceptions is that anyone considered a hacker is doing something illegal. It's a sad commentary on the state of our society when someone who is basically seeking knowledge and the truth is assumed to be up to something nefarious. Nothing could be further from the truth. Hackers, in their idealistic naiveté, reveal the facts that they discover, without regard for money, corporate secrets or government cover-ups."*

Walaupun illegal para *hacker* tidak seluruhnya jahat, *hacker* yang baik motifnya hanya untuk mencari tantangan dan kesenangan saja, membuktikan dirinya mampu menembus sistem, dikatakan Eric Steven Raymond: *"Being a hacker is lots of fun, but it's a kind of fun that takes lots of effort. The effort takes motivation. Successful athletes get their motivation from a kind of physical delight in making their bodies perform, in pushing themselves past their own physical limits. Similarly, to be a hacker you have to get a basic thrill from solving problems, sharpening your skills, and*

exercising your intelligence." (Menjadi *hacker* sangat menyenangkan dan akan memperoleh pengetahuan dasar-dasar memecahkan masalah, meningkatkan keterampilan serta mempertajam kepandaian.)

Hacker seperti itu disebut *real hacker* atau *hacker* sejati (baik). Ilustrasi dari kebaikan mereka adalah sebagai berikut: *"There is a community, a shared culture, of expert programmers and networking wizard that traces its history back through decades to the first time-sharing minicomputers and the earliest ARPAnet experiments. The members of this culture originated the term 'hacker'. Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work. If you are part of this culture, if you have contributed to it and other people in it know who you are and call you a hacker, you're a hacker."*

Sejak eksperimen ARPAnet, para *hacker* ikut membangun internet, membuat peranti lunak Unix dapat secanggih sekarang, mereka juga meluncurkan Usenet dan membuat World Wide Web (www) bekerja dengan baik. Memang dalam perkembangannya muncullah *cracker* yang merusak sistem, menyebarkan program-program *Trojan Horse* atau mengambil keuntungan finansial. Kemudian muncul *Preaker* dalam Net Mag dijelaskan: *"Phreaking is basically hacking with a telephone, using different "boxes" and "tricks" to manipulate the phone companies and their phones, you gain many things, two of which are: knowledge about telephones and how they work, and free local and long distance phone calls."* (*Phreaking* adalah *hacking* dengan telepon, menggunakan berbagai boks telepon yang berlainan dengan cara-cara tertentu, dengan motif untuk mengetahui bagaimana jaringan telepon tersebut bekerja dan mencuri pulsa agar bebas membayar dalam melakukan percakapan lokal atau percakapan jarak jauh [interlokal/ke luar negeri].)

Cara-cara *hacker* sama dengan *cracker* (hacker jahat) yang berbeda adalah motivasinya (*cracker* merusak dan mencuri). *Phreaker* motivasinya sama dengan *cracker* yang berbeda adalah cara dan sasarannya, *cracker* sasarannya jaringan komputer serta peranti lunaknya, sedangkan *phreaker* sasarannya jaringan telepon serta peranti lunak pencatat pulsa telepon.

Sebenarnya *hacker* (sejati) bisa dijadikan partner para penyidik Polri dalam upaya menyidik para *cracker* dan *phreaker* serta menyeretnya ke meja hijau. Karya *hacker* sejati yang diakui semua orang, antara lain:

a. Menulis sumber peranti lunak terbuka (*open source software*) yang tidak komersial sehingga siapa pun dapat memanfaatkan dan mengembangkannya, antara lain peranti lunak Demigods (manusia setengah dewa) di mana setiap orang dengan bebas menulis secara luas dan menggunakannya.
b. Membantu mengetes kelemahan-kelemahan peranti lunak terbuka.
c. Memublikasikan informasi-informasi yang berguna dalam BBS's dan FAQs (*frequently asked questions*) *lists*.
d. Membantu agar infrastruktur jaringan komputer tetap berjalan dengan baik.

Hacking yang terjadi di Dunia

Tiap hari sebuah pembobolan atau setidaknya pelanggaran kode etik dengan menerobos keamanan internet selalu terjadi di berbagai belahan dunia. Hal ini terjadi mulai dari sebuah website kecil,

hingga website yang dikelola perusahaan besar atau bahkan pemerintah. Enkripsi dengan kesulitan yang luar biasa pun belum tentu jadi penghalang yang kokoh bagi berbagai data penting yang ada di baliknya. Dengan makin mencuatnya banyak kasus peretasan yang terjadi di dunia dalam satu dekade terakhir, berbagai kasus terkait *hacker* makin membuat para penyimpan data di dunia maya takut. Bahkan beberapa kasus benar-benar mencolok di antara ribuan yang lainnya. Dalam satu dekade terakhir, terdapat penyerangan *hacker* mengerikan seperti Stuxnet yang mampu membuat error sebuah mesin sentrifugal nuklir, hingga kasus peretasan perusahaan film raksasa hingga film terbarunya tak jadi tayang.

Berikut beberapa kasus pembobolan *hacker* paling mengerikan di dunia:

1. Pembobolan Estonia
   Pembobolan besar-besaran terjadi di Estonia pada April 2007 silam. Peretasan yang terjadi di berbagai website Pemerintahan Estonia ini membuat beberapa website mati total. Bahkan, para *hacker* menghapus website dari sang Presiden, para Menteri, dan para anggota parlemen. Peretasan ini juga terjadi di sektor finansial dan juga situs-situs media di Estonia. Kejadian ini berlangsung dalam 21 hari, di mana Estonia harus menjalani hidup tanpa internet dalam jangka waktu tersebut. Saking masifnya, kejadian ini dijuluki *"Web War One,"* sebuah plesetan dari *World War One*. Hal ini terjadi diduga karena Pemerintahan Estonia memutuskan untuk menurunkan sebuah patung dari era Soviet dari ibukota negara di Eropa Utara tersebut, Tallinn. Estonia menuduh Rusia sebagai otak dibalik kejahatan teknologi ini. Meski ternyata akhirnya diketahui bahwa orang Rusia-lah yang 'memotong' koneksi Estonia dari dunia luar dengan memutus internetnya, ternyata sang *hacker* tidak disponsori oleh Pemerintah Rusia. Meski demikian, peretasan ini tetap jadi perhatian dunia di mana belum pernah terjadi peretasan sebuah negara yang merusak segala aspek digital dalam satu negara. Pemerintah Estonia yang sejak awal sudah membuat berbagai aksi untuk melawan hal ini, akhirnya mengalokasikan uang negara secara besar-besaran untuk urusan keamanan *cyber* di Estonia.
2. Penyerangan situs nuklir Iran oleh Amerika Serikat
   Di 2006 silam, Presiden Amerika Serikat saat itu, George W. Bush, sedang geram sekaligus gelisah terhadap upaya Iran dalam memperkaya diri dengan uranium. Negara di Asia Barat tersebut bahkan berencana untuk mengembangkan roket nuklir sendiri. Karena saat itu Bush sedang sibuk dalam berbagai hal seperti perang Iraq dan agresi militer Amerika Serikat di Timur Tengah yang juga melibatkan Israel, akhirnya Amerika Serikat memberi peringatan terhadap Iran dengan 'senjata' yang tentu lebih canggih dari nuklir, yakni *cyber*. Sebuah 'senjata *cyber*' yang mempunyai kode "*Olympic Games"* lalu diganti menjadi *"Stuxnet*" ini dirancang oleh para peneliti keamanan komputer untuk membobol pertahanan nuklir Iran. Kode tersebut akhirnya bisa masuk ke fasilitas nuklir Iran, bahkan bisa merusak sistem kontrol nuklirnya secara spesifik. Caranya adalah dengan mengatur kecepatan sentrifugal yang menjadi kunci dari pengembangan nuklir tersebut, ketika kecepatannya dipercepat atau diperlambat, lama-kelamaan sistem akan tak terkontrol dan rusak dengan

sendirinya. Hal ini terjadi dalam 13 hari setelah peretasan. Iran sendiri tak pernah mengakui hal ini, di mana kambing hitam kerusakan sistem nuklir tersebut ditujukan ke ilmuwan dan insinyur yang bekerja di proyek tersebut. Hal ini awalnya memang tak disadari oleh Iran karena saking canggihnya peretasan ini, setitik jejak pun sama sekali tak tertinggal.

3. Bangkitnya *Hacker* dari Iran
   Mungkin merupakan sebuah ironi yang tajam, di mana sebuah negara dilumpuhkan oleh *hacker* dan dari negara tersebut juga tumbuh sekelompok peretas yang mengerikan.Tak lama setelah sistem sentryfugal nuklir Iran dirusak, Iran membangun sebuah pasukan *cyber* yang didanai Pemerintah Iran secara gila-gilaan hingga mencapai angka 20 Juta Dollar. Beberapa sektor yang dikontrol *cyber* di Amerika Serikat seperti sektor finansial dan sistem kontrol bendungan, telah diserang oleh kelompok ini. Puncaknya adalah di tahun 2012 silam. Di bulan Agustus 2012, *hacker* Iran berhasil membobol perusahaan minyak Arab Saudi milik pemerintah Amerika Serikat, Saudi Aramco. Total 35.000 komputer mati total dalam peristiwa peretasan ini. Penyebabnya sederhana, sebuah email berisi tautan *phising* diklik oleh salah satu staf IT dari Saudi Aramco. Hal ini menyebabkan semua kontrak dari salah satu perusahaan minyak terbesar di dunia ini tak berlaku. Penyerangan yang dibocorkan dalam salah satu dokumen dari Edward Snowden ini, telah menunjukkan kemampuan Iran secara jelas dalam aksi kejahatan *cyber*. Saat ini, Iran mempunyai pasukan *cyber* terbesar nomor 4 di dunia, di belakang Rusia, China, dan Amerika Serikat.
4. Pembobolan SONY Entertainment yang diduga dilakukan Korea Utara
   Pada akhir 2014 silam, di mana SONY Pictures mengalami peretasan besar-besaran yang salah satu buntutnya adalah tak jadi tayangnya film komedi kontroversial tentang percobaan pembunuhan Presiden Korea Utara Kim Jong-Un, "*The Interview*."Dampaknya sebenarnya tak hanya batalnya pemutaran film, namun beberapa hal seperti bocornya email privat, bocornya angka keamanan sosial, bocornya film SONY yang belum dirilis, dan terhapus secara permanennya lebih dari separuh data perusahaan film tersebut. Bahkan, sang pemimpin dari perusahaan tersebut terpaksa turun dari jabatannya setelah sebuah email kontroversial berisi umpatan rasis terhadap Presiden obama dan komentar buruk tentang Angelina Jolie terkuak ke publik. Uniknya, pihak Pemerintah Amerika Serikat secara mengejutkan langsung menuduh Korea Utara sebagai otak di balik peristiwa ini. Hal ini menorehkan sejarah, di mana ini adalah pertama kalinya Amerika Serikat mengkambinghitamkan negara lain atas sebuah serangan *cyber*. Pihak Korea Utara sesegera mungkin membantahnya, dan akhirnya meninggalkan pertanyaan besar bagi warga dunia tentang siapa yang melakukan salah satu kejahatan terbesar via *cyber* ini.

***Hacking* yang terjadi di Indonesia**

1. Peretasan situs BPJS Kesehatan
   Pada bulan Mei 2021, website Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, yakni bpjs-kesehatan.go.id diduga telah diretas. Hal ini menyebabkan data 279 juta penduduk Indonesia bocor dan dijual di forum *online* Raid Forums oleh

akun bernama “Kotz”.Dataset berisi NIK, nomor ponsel, e-mail, alamat, hingga gaji tersebut dijual seharga 0,15 bitcoin, atau setara Rp84,4 juta. Sebagai antisipasi mencegah penyebaran data yang lebih luas, Kominfo kemudian mengajukan pemutusan akses terhadap tautan untuk mengunduh data pribadi tersebut dan memblokir Raid Forums.

2. Kebocoran data asuransi BRI Life
   Kasus *hacking* di Indonesia dengan insiden kebocoran data juga pernah dialami oleh perusahaan asuransi BRI Life. Pada Juli 2021, sekitar 2 juta data nasabah BRI Life diduga bocor dan dijual secara online seharga $7000 atau sekitar Rp101,6 juta. Hal ini pertama kali diungkap oleh akun Twitter @UnderTheBreach yang mengklaim bahwa *hacker* telah mengambil 250 GB data BRI Life, yang di dalamnya termasuk data 2 juta nasabah dalam format file PDF dan 463.000 dokumen lainnya. Data-data tersebut berisi informasi foto KTP, rekening, nomor wajib pajak, akte kelahiran, hingga rekam medis. Diduga, kebocoran data terjadi karena adanya celah keamanan di dalam sistem elektronik BRI Life, yang disalahgunakan oleh pihak tak bertanggungjawab.
3. Serangan *deface website* Sekretariat Kabinet RI
   Di waktu yang sama, website milik Sekretariat Kabinet RI yakni setkab.go.id terkena serangan *deface*. *Deface website* ini memungkinkan *hacker* mengubah tampilan situs target sasarannya. Diduga, peretasan ini dilakukan untuk keuntungan ekonomi yakni menjual *script backdoor* dari *website* korbann ya kepada pihak yang menginginkannya. Awalnya, situs Setkab.go.id diretas sehingga tak bisa diakses. Tampilan website kemudian berubah menjadi hitam dengan foto demonstran membawa bendera merah putih dan tulisan “Padang Blackhat ll Anon Illusion Team Pwned By Zyy Ft Luthfifake”. Menurut penyelidikan polisi, peretasan ini terjadi akibat kelemahan sistem keamanan dan kelengahan operator.
4. Serangan DDoS terhadap situs DPR RI
   Website resmi DPR RI, dpr.go.id pada 8 Oktober 2020 lalu sempat error dan tidak bisa diakses. Situs menampilkan halaman putih dengan pesan *“An error occurred while processing your request”*. Setelah ditelusuri, serangan tersebut dikategorikan sebagai DDoS, yaitu tindakan membanjiri lalu lintas pada suatu *server* atau sistem secara terus menerus, sehingga server tidak mampu mengatur *traffic* dan *down*. Ternyata, metode ini dimanfaatkan *hacker* untuk memasuki website dan melangsungkan *deface*.Ketika situs bisa kembali diakses, pengunjung akan melihat perubahan pada nama situs DPR. Aksi itu sempat ramai di Twitter, karena sejumlah akun diketahui sempat mengunggahnya perubahan itu di media sosial. Sebagai penanganan, DPR berkoordinasi dengan Telkom dan Mabes Polri untuk menghalau peretasan.
5. Kebocoran data e-HAC Kemenkes
   Pada Juli 2021, aplikasi *Electronic Health Alert* (e-HAC) buatan Kemenkes RI juga ikut menjadi korban kasus serangan siber akibat ulah para hacker. Aplikasi kartu kewaspadaan kesehatan yang menjadi syarat masyarakat bepergian ini mengakibatkan 1,3 juta data masyarakat Indonesia bocor. Selain bocornya data pengguna e-HAC, kasus ini mengakibatkan data tes Covid-19

penumpang, data rumah sakit, hingga data staf e-HAC juga ikut terungkap. Diduga, serangan ini terjadi akibat kurangnya protokol keamanan aplikasi yang memadai dan penggunaan database Elasticsearch yang dianggap kurang aman untuk menyimpan data.

6. Tiket.com dan Citilink diserang *hacker*

   Pada Oktober 2016, sekelompok *hacker* remaja berhasil meretas situs jual beli tiket online, Tiket.com di server Citilink. Tak tanggung-tanggung, kerugian yang dialami Tiket.com sebesar 4,1 miliar, sedangkan Citilink sejumlah 2 miliar. Kasus ini terungkap setelah Tiket.com melaporkan pembobolan situsnya ke Bareskrim Polri pada 11 November 2016. Menurut penyelidikan, aksi *hacker* sebenarnya bukanlah hal yang canggih. Namun sayangnya, situs-situs tersebut di waktu tersebut kurang memiliki tingkat keamanan yang cukup.

7. Data pengguna Tokopedia bocor ke *dark web*

   Korban kasus serangan *hacker* di Indonesia selanjutnya dialami oleh perusahaan *e-commerce* buatan anak bangsa, Tokopedia. Pada awal Mei 2020, Tokopedia mengalami kebocoran data terhadap 91 juta akun penggunanya dan 7 juta akun *merchant*. Data yang berisi nama lengkap, nama akun, email, toko online, tanggal lahir, nomor HP, tanggal mendaftar, serta beberapa data yang terenkripsi berbentuk hash ini diperjualbelikan di *dark web* seharga USD5.000 atau Rp70 juta. Tokopedia kemudian segera memeriksa kasus ini dan menyarankan penggunanya untuk rutin mengganti password akun.

8. Pembobolan database Polri

   Polri juga pernah ikut menjadi korban serangan *hacker*. Di November 2021, *hacker* dengan nama akun @son1x666 mengklaim telah meretas database milik Polri melalui akun Twitternya. Dalam cuitannya tersebut, ada 28.000 informasi log in dan data pribadi yang dicuri. Selain itu ada tiga link berisi sampel data yang diduga berasal dari database Polri berisi informasi nama, tempat tanggal lahir, nomor registrasi pokok, alamat, golongan darah, satuan kerja, suku, alamat email, pangkat, hingga pelanggaran anggota. Menanggapi hal ini, Polri telah memastikan data internal dan sistem keamanan Polri tetap aman. Menurut investigasi, peretasan ini dilakukan oleh *hacker* yang dikenal seringkali menyerang situs pemerintah di dunia untuk menunjukkan eksistensinya dan bentuk protes ketidakadilan pemerintah terhadap rakyat.

9. Peretasan channel YouTube BNPB

   Bukan hanya menyerang website, akun channel YouTube juga ikut menjadi sasaran ulah *hacker* tak bertanggung jawab. Salah satu korbannya, channel YouTube resmi milik Badan Nasional Penanggulangan Bencana (BNPB). Pada Desember 2021, channel YouTube dengan nama "BNPB Indonesia" berubah nama menjadi "Ethereum 2.0". Tak sampai di situ, ulah jahil *hacker* berlanjut dengan menggunakan akun YouTube tersebut untuk melakukan *live streaming* berjudul "Ethereum CEO: Ethereum Breakout! Ethereum News, ETH 2.0 RELEASE Date"

10. Situs Telkomsel diserang hacker

    Perusahaan operator seluler Telkomsel juga turut jadi korban kasus *hacker*. Pada April 2017, website resmi Telkomsel berubah tampilan dengan menampilkan protes terhadap

tarif internet yang mahal. Menurut penyelidikan, peretasan ini diduga terjadi akibat adanya celah keamanan pada web hosting yang dieksploitasi oleh kelompok peretas. Opsi lain, *username* dan *password* untuk mengakses *web hosting* jatuh ke tangan peretas. Menanggapi hal ini, pihak Telkomsel memastikan peretasan sama sekali tidak mengancam keamanan data penggunanya, karena data terletak di *server* berbeda yang dilapisi sistem keamanan berlapis. Layanan panggilan telepon dan SMS juga sama sekali tidak terganggu akibat kasus peretasan ini.

Hacking dalam Persfektif Hukum Pidana

Hacker secara umum adalah orang yang mengakses suatu sistem komputer dengan suatu cara yang tidak sah atau salah. Perbuatan ini biasanya dilakukan dengan diawali rasa keingintahuan, kekaguman dan terakhir adalah adanya suatu tantangan yang ditujukan terhadap suatu sistem komputer. (Edmon Makarim, 2003: 401).

Pada prakteknya *hacker* dapat dikategorikan ada yang baik dan buruk. Namun terlepas dari hal itu, keduanya tetap melakukan akses secara illegal atau dengan kata lain pelaku telah melakukan penyusupan terhadap sistem komputer (Edmon Makarim, 2003: 401).

Hacker dapat melakukan aksinya ada beberapa tahapan yang dilalui yaitu sebagai berikut:

1. Mencari sistem komputer yang hendak dimasuki;
2. Menyusup dan menyadap *password*;
3. Menjelajahi sistem komputer;
4. Membuat *backdoor* dan menghilangkan jejak. (Edmon Makarim, 2003: 402)

Dalam dunia nyata, kejahatan ini dapat dianalogikan dengan memasuki suatu wilayah tanpa izin. Dalam KUHP hal ini diatur dalam Pasal 167. Selanjutnya apakah kejahatan ini bisa dimasukkan dalam ketentuan pasal tersebut.

Pasal 167 KUHP menyatakan:

(1) Barang siapa dengan melawan hak orang lain dengan memaksa ke dalam rumah atau ruangan yang tertutup atau pekarangan, yang dipakai oleh orang lain, atau sedang ada di situ dengan tidak ada haknya, tidak dengan segera pergi dari tempat itu atas permintaan orang yang berhak, dihukum penjara selama-lamanya sembilan bulan atau denda sebanyak-banyaknya Rp 4.500.

(2) Barang siapa masuk dengan memecah atau memanjat, memakai kunci palsu, perintah palsu atau pakaian dinas palsu, atau barang siapa dengan tidak setahu yang berhak dan lain daripada lantaran keliru, masuk ke tempat yang tersebut tadi dan kedapatan di sana pada waktu malam, dianggap sebagai sudah masuk dengan memaksa. (R. Soesilo, 1994: 143).

Untuk mengkategorikan *hacking* ke dalam delik yang diatur Pasal 167, maka akan diuraikan unsur-unsurnya sebagai-mana disebut dalam Ayat (1):

- Barang siapa dengan melawan hak orang lain;
- Masuk dengan memaksa;
- Ke dalam rumah atau ruangan yang tertutup atau pekarangan, yang dipakai oleh orang lain;
- Atau sedang di situ dengan tidak ada haknya;
- Tidak segera pergi dari tempat itu;
- Atas permintaan orang yang berhak atau atas nama orang yang berhak.

Selanjutnya Pasal 167 ayat (2) unsur-unsurnya sebagai berikut:

- Barang siapa;
- Masuk;
- Dengan memecah atau memanjat, memakai kunci palsu, perintah palsu, atau pakaian dinas palsu;
- Atau barangsiapa;
- Dengan tidak setahu yang berhak dan lain daripada lantaran keliru;
- Masuk ke tempat yang tersebut tadi.

SIMPULAN

Kesimpulan pada penulisan ini adalah menjawab dua rumusan di atas yaitu: mengapa *hacking* dikategorikan ke dalam salah satu kejahatan di dunia maya? dan bagaimana persfektif Hukum Pidana Nasional melihat *Hacking* sebagai salah satu kejahatan di dunia maya?

Hacking dikategorikan sebagai salah satu kejahatan di dunia maya karena *hacker* merupakan orang yang menguasai pemrograman yang dapat melakukan *hacking* atau peretasan sistem keamanan pada komputer atau jaringan dengan tujuan tertentu. Seorang *hacker* umumnya memiliki pemahaman tentang komputer, pemrograman, jaringan, dan juga perangkat keras lebih lanjut. Dengan memahami apa sebenarnya *hacker* atau peretas tentu akan menjadi paham bahwa peretas atau kegiatan peretasan tidak selalu dihubungkan dengan kejahatan dunia maya. Di dalam dunia *Cyber*, peretas merupakan orang yang dapat melakukan peretasan perangkat misal seperti komputer, webcam, ponsel, sampai router. Tindakan peretasan yang menimbulkan kerugian suatu pihak merupakan kegiatan kriminal.

Sebuah kejahatan pastilah mengandung unsur Perbuatan Melawan Hukum (PMH). Di dalam Hukum Pidana Perbuatan Melawan Hukum (PMH) dicirikan: *pertama*, perbuatan melawan hukum pidana sering disebut *Wederrechttelijk*, *kedua*, dasar hukum pengaturannya terdapat pada Kitab Undang-Undang Hukum Pidana (KUHP), *ketiga*, sifat melawan hukum pidana bersifat publik artinya ada kepentingan umum yang dilanggar (disamping juga kepentingan individu), *keempat*, unsur-unsur perbuatan melawan hukum dalam hukum pidana adalah perbuatan yang melanggar undang-undang, perbuatan yang dilakukan di luar batas kewenangannya atau kekuasaannya dan perbuatan yang melanggar asas-asas umum yang berlaku di lapangan hukum. Dalam persfektif Hukum Pidana *hacking* di-analogikan dengan memasuki suatu wilayah tanpa izin. Dalam KUHP hal ini diatur dalam Pasal 167.

Pasal 167 KUHP menyatakan:

(1) Barang siapa dengan melawan hak orang lain dengan memaksa ke dalam rumah atau ruangan yang tertutup atau pekarangan, yang dipakai oleh orang lain, atau sedang ada di situ dengan tidak ada haknya, tidak dengan segera pergi dari tempat itu atas permintaan orang yang berhak, dihukum penjara selama-lamanya sembilan bulan atau denda sebanyak-banyaknya Rp 4.500.
(2) Barang siapa masuk dengan memecah atau memanjat, memakai kunci palsu, perintah palsu atau pakaian dinas palsu, atau barang siapa dengan tidak setahu yang berhak dan lain daripada lantaran keliru, masuk ke tempat yang tersebut tadi dan kedapatan di sana pada waktu malam, dianggap sebagai sudah masuk dengan memaksa.

DAFTAR PUSTAKA

Buku

Ibrahim, Jhonny. 2007. *Teori dan Metodologi Penelitian Hukum Normatif.* Cetakan ketiga, Bayu Media Publishing Malang-Jawa Timur.

Mamudji, Sri, et al. 2005. *Metode Penelitian dan Penulisan Hukum.* Cet 1. Badan Penerbit FH UI. Depok

Maskun. 2022. *Kejahatan Siber (Cyber Crime) Suatu Pengantar.* Cetakan Ketiga. Kencana, Jakarta.

Marzuki, Peter Muhammad Marzuki. 2013. *Penelitian Hukum.* ed Revisi. Cet 8. Kencana Prenada Media Grup. Jakarta.

Prasetyo, Teguh. *Hukum Pidana* Edisi Revisi. 2017. Rajawali Pers. Depok.

Sitompul, Josua, 2021. *Cyberspace, Cybercrimes, Cyberlaw Tinjuan Aspek Hukum Pidana.* PT Tatanusa. Jakarta

Wahid, Abdul. Labib, Mohammad. 2010. *Kejahatan Mayantara (Cyber Crime).* Cetakan Kedua. Refika Aditama. Bandung.

Yurizal, 2018. *Penegakan Hukum Tindak Pidana Cyber Crime.* Cetakan 1. Media Nusa Creative. Malang.

Peraturan Perundang-Undangan

Kitab Undang Undang Hukun Pidana (KUHP)

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE)

Artikel Jurnal

Gani, A.G. 2018, Cybercrime (Kejahatan Berbasis Komputer), *Jurnal Sistem Informasi Universitas Suryadarma*, Vol 5, No 1, DOI: https://doi.org/10.35968/jsi.v5i1.18

Awaludin, M., & Wahono, R. S. (2015). Penerapan Metode Distance Transform Pada Linear Discriminant Analysis Untuk Kemunculan Kulit Pada Deteksi Kulit. *Journal of Intelligent Systems*, *1*(1), 48–54.

Awaludin, M., & Yasin, V. (2020). APPLICATION OF ORIENTED FAST AND ROTATED BRIEF (ORB) AND BRUTEFORCE HAMMING IN LIBRARY OPENCV FOR CLASSIFICATION OF e-ISSN : 2598-8719 (Online). *Journal of Information System, Applied, Managemgent, Accounting, and Reserarch*, *4*(3), 51–59.

Subagyo, Agus. 2015. Sinergi Dalam Menghadapi Ancaman Cyber Warfare Synergy in Facing of Cyber Warfare Threat. *Jurnal Pertahanan.* Volume 5 Nomor 1. hal 89-102.

Sari, Indah, 2020. Perbuatan Melawan Hukum (PMH) Dalam Hukum Pidana Dan Hukum Perdata, J*urnal Ilmiah Hukum Dirgantara.* Vol 11 No1. September. 2020. Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma. Jakarta

Sumber Rujukan dari Website

Amelia Shinta, 2022, 10 Kasus Serangan Hacker yang pernah terjadi di Indonesia, https://www.dewaweb.com/blog/kasus-hacker-di-indonesia/. Diakses tanggal 1 Juni 2023

4 Kasus pembobolan hacker paling mengerikan di dunia ! Diakses tanggal 1 Juni 2023 https://www.merdeka.com/teknologi/4-kasus-pembobolan-hacker-paling-mengerikan-di-dunia.html?page=5. Diakses tanggal 1 Juni 2023

Hacking Adalah: Pengertian, Jenis Dan Macam -Macam Hacking https://course-net.com/blog/hacking-adalah/. Diakses tanggal 1 Juni 2023

Pengertian Hacking (Peretasan), Sejarah, Tujuan, Jenis, Contohnya! https://rifqimulyawan.com/blog/pengertian-hacking/amp/. Diakses tanggal 1 Juni 2023