KAJIAN ETIOLOGI KRIMINAL TINDAK PIDANA *CRACKING* SISTEM OPERASI WINDOWS DI PROVINSI DAERAH ISTIMEWA YOGYAKARTA

Christiara Febriliani, Ismunarno, Diana Lukitasari
E-mail: cfebriliani@gmail.com; ismunarno@yahoo.com; lukitasari.diana@gmail.com

Abstrak

Penelitian ini bertujuan untuk mengetahui faktor penyebab dan modus operandi tindak pidana *cracking* sistem operasi Windows di Provinsi Daerah Istimewa Yogyakarta. Penelitian ini merupakan penelitian empiris yang bersifat deskriptif. Pendekatan penelitian menggunakan pendekatan kualitatif. Jenis data yang digunakan adalah data primer dan data sekunder. Teknik pengumpulan bahan hukum yang digunakan adalah melalui wawancara, kuesioner, dan studi pustaka. Analisis hukum menggunakan metode kualitatif. Tindak pidana *cracking* merupakan tindak pidana khusus karena diatur di luar KUHP. Tindak pidana *cracking* sistem operasi Windows telah merugikan pihak pemerintah dan perusahaan Microsoft. Pengaturan mengenai tindak pidana *cracking* secara khusus telah diatur dalam Pasal 30 Ayat (3) juncto Pasal 46 Ayat (3) Undang-Undang Nomor 11 Tahun 2008 sebagaimana diperbaharui dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Tindak pidana tersebut masih terjadi dan penegakan hukumnya belum optimal karena faktor penyebab dan modus operandi yang belum diteliti secara khusus. Berdasarkan hasil penelitian, faktor penyebab terjadinya tindak pidana *cracking* sistem operasi Windows ini adalah karena faktor ekonomi, sosial dan budaya, masyarakat dan hukum. Tindak pidana *cracking* ini memiliki modus operandi yang berbeda dari tindak pidana pada umumnya karena menggunakan sarana teknologi yang semakin canggih. Modus operandi yang digunakan terdapat 2 (dua) macam yaitu *cracking* secara langsung dan tidak langsung.

Kata kunci: *Cracking,* Sistem Operasi Windows, Modus Operandi

Abstract

This study aims to determine the causes and modus operandi of the crime of cracking the Windows operating system in the province of Yogyakarta Special Region. This study is a descriptive empirical research. The research approach uses a qualitative approach. The data used are primary data and secondary data. Collection techniques used were legal materials through interviews, questionnaires, and literature. Legal analysis using qualitative methods. Cracking criminal act is a criminal offense specifically for regulated outside the Criminal Code. The criminal act of cracking the Windows operating system has been detrimental to the government and Microsoft.Arrangements regarding the crime of cracking specifically been regulated in Article 30 Paragraph (3) in conjunction with Article 46 Paragraph (3) of Law No. 11 of 2008 as amended by Act No. 19 of 2016 on Information and Electronic Transactions. The offense is still going on and the law enforcement is not optimal because the causes and modus operandi that has not been specifically studied. Based on the results of the study the underlying causes of the crime of cracking the Windows operating system this is due to economic, social and cultural, and legal communities. This cracking criminal offense has a different modus operandi of criminal acts in general because it uses increasingly sophisticated means of technology. The modus operandi used there are two (2) types of cracking directly and indirectly.

***Keywords*:** *Cracking, Windows Operating System*, Modus Operandi

A. Pendahuluan

Perkembangan teknologi informasi yang begitu pesat telah menyebabkan dunia menjadi tanpa batas dan menyebabkan terjadinya perubahan sosial sehingga dapat dikatakan teknologi informasi menjadi pedang bermata dua. Teknologi informasi disebut sebagai pedang bermata dua

karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus dapat menjadi sarana efektif perbuatan melawan hukum (Budi Suhariyanto, 2012:2). Perbuatan melawan hukum menggunakan sarana teknologi informasi lebih dikenal dengan *cybercrime. Cybercrime* dalam pengertian sempit adalah kejahatan terhadap sistem komputer, sedangkan *cybercrime* dalam pengertian luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer (Widodo, 2009:24).

Indonesia telah membuat aturan khusus mengenai tindak pidana teknologi informasi atau *cybercrime* ini. *Cybercrime* diatur dalam Undang-Undang Nomor 11 Tahun 2008 (selanjutnya disebut Undang-Undang ITE) sebagaimana telah diperbaharui oleh Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Undang-Undang ITE memuat beberapa bentuk *cybercrime* salah satunya adalah mengenai *cracking. Cracking* merupakan suatu kegiatan merusak sistem yang bertujuan untuk kepentingan pribadi dengan cara-cara yang tidak sah (Anthoni, 2018:265). Pada Pasal 30 Ayat (3) Undang-Undang ITE menyebutkan cara-cara *cracking* antara lain dengan melanggar, menerobos, melampaui atau menjebol sistem pengamanan. Sistem pengamanan yang telah dirusak oleh pelaku *cracking* kemudian dapat dijadikan salah satu sarana untuk mendapatkan keuntungan, misalnya sistem operasi Windows pada komputer. Sistem operasi Windows yang memiliki lisensi berbayar dapat diperoleh secara utuh tanpa harus membayar yaitu dengan cara melakukan *cracking*. Sistem Windows yang telah berhasil dirusak ini kemudian diperbanyak dalam bentuk palsu (bajakan) dan dijual untuk mendapatkan keuntungan.

Tindak pidana *cracking* sistem operasi Windows ini menjadi sebuah dilema tersendiri bagi penegakan hukumnya. Pada satu sisi, *cracking* bertentangan dengan hukum negara dan di sisi lain dengan adanya *cracking* dapat mempermudah penyebarluasan data informasi elektronik karena masyarakat yang sebagian besar adalah pengguna sistem operasi Windows. Penguasaan dan pemahaman penyidik terhadap tindak pidana teknologi informasi ini masih sangat minim, pengetahuan ilmu tentang teknologi informasi dan belum memahami teknik atau modus operandi para *cracker* dan profil-profilnya serta metode penyerangannya (Rudi Hernawan, 2013:48). Pada kasus *cracking* ini modus operandi yang digunakan para *cracker* ini berbeda dari modus operandi kejahatan konvensional lainnya. Pada cabang ilmu kriminologi, modus operandi diartikan sebagai teknik atau cara cara beroperasi yang dilakukan oleh penjahat (R. Soesilo, 1985:98). Kriminologi juga bertujuan untuk menciptakan perkembangan pengetahuan lain berkenaan dengan proses penyusunan undang-undang kejahatan dan pencegahan kejahatan. Selain itu, kriminologi dalam penegakan hukum pidana merupakan bagian integral dari kebijakan untuk mencapai kesejahteraan, maka wajar jika dikatakan bahwa usaha penanggulangan kejahatan merupakan penegakan hukum pidana (Sudarto,1986:111).

Berdasarkan uraian di atas, penulis tertarik untuk mendalaminya secara khusus dan lebih lanjut dalam bentuk tulisan atau karya ilmiah dengan pokok permasalahan yaitu faktor penyebab dan modus operandi tindak pidana *cracking* sistem operasi Windows di Provinsi Daerah Istimewa Yogyakarta.

B. Metode Penelitian

Dalam penelitian ini, penulis mendeskripsikan secara objektif mengenai faktor penyebab dan modus operandi tindak pidana *cracking* sistem operasi Windows di provinsi Daerah Istimewa Yogyakarta. Sifat penelitian yang penulis susun yaitu secara deskriptif dimaksudkan untuk memberikan data yang teliti tentang keadaan manusia atau gejala-gejala lainnya, termasuk untuk mempertegas hipotesa-hipotesa agar dapat membantu dalam memperkuat teori-teori lama atau di dalam kerangka menyusun teori-teori baru (Soerjono Soekanto, 2010: 10). Pendekatan yang digunakan adalah pendekatan kualitatif. Sumber data yang digunakan dalam penelitian hukum ini sumber data primer dan sumber data sekunder. Sumber data primer yaitu para pelaku tindak pidana *cracking* sistem operasi Windows. Sumber data sekunder yaitu KUHP, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 19

Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

C. Hasil dan Pembahasan

1. Faktor Penyebab Tindak Pidana *Cracking* Sistem Operasi Windows di Yogyakarta

Kemajuan teknologi informasi pada masa kini ditandai dengan meningkatnya penggunaan teknologi dalam setiap aspek kehidupan manusia. Teknologi seperti internet, komputer dan perangkat lainnya banyak memberikan kemudahan bagi manusia untuk dapat melakukan aktivitas yang bermanfaat namun di sisi lain juga dapat memberikan kemudahan akses bagi pihak tertentu untuk melakukan suatu tindak pidana, salah satunya adalah *cracking*. Berdasarkan pendekatan etiologi kriminal, maka perlu dilihat faktor-faktor yang menyebabkan terjadinya *cracking* sistem operasi Windows khususnya di Daerah Istimewa Yogyakarta. Faktor-faktor penyebab tersebut antara lain adalah:

a. Faktor Ekonomi

Rendahnya tingkat kesadaran masyarakat di Indonesia masih menjadikan ekonomi sebagai faktor utama terhadap tingginya tingkat tindak pidana *cracking* sistem operasi Windows. Tingginya angka pengangguran dan harga sistem operasi Windows yang mahal mendorong sebagian masyarakat untuk melakukan tindak pidana ini.

Para pelaku tindak pidana *cracking* sistem operasi Windows ini memiliki 2 (dua) tujuan ekonomi. Pertama untuk mengehemat pengeluaran ekonomi dimana sistem operasi Windows yang telah diaktivasi secara ilegal (*crack*) hanya digunakan untuk diri sendiri dan tidak untuk diperjualbelikan. Hal ini karena tidak perlu mengeluarkan uang sama sekali untuk melakukan tindak pidana *cracking* sistem operasi Windows. Pelaku tindak pidana *cracking* sistem operasi Windows dengan tujuan ini sebagian besar merupakan mahasiswa.

Tujuan ekonomi yang kedua adalah untuk mendapatkan pemasukan dari tindak pidana *cracking* sistem operasi Windows ini. Masyarakat memiliki daya tarik yang tinggi terhadap Windows dengan lisensi yang tidak resmi karena harga yang cenderung lebih murah daripada Windows dengan lisensi resmi. Tingginya permintaan pasar membuat beberapa pelaku tindak pidana *cracking* sistem operasi Windows menyediakan layanan berbayar (*service*) untuk komputer sehingga masyarakat yang ingin menggunakan Windows dapat membayar dengan harga yang terjangkau dibandingkan dengan membeli pada toko resminya.

b. Faktor Sosial Budaya

Faktor sosial budaya dapat dilihat dari beberapa aspek, salah satunya yaitu kemajuan teknologi informasi. Perkembangan ilmu pengetahuan dan teknologi yang semakin maju telah memengaruhi berbagai motif melakukan tindak pidana di bidang teknologi. Sebagian besar masyarakat umum telah terbiasa dengan menggunakan sistem operasi Windows. Hal ini menjadi salah satu alasan masyarakat lebih memilih melakukan tindak pidana *cracking* sistem operasi Windows karena dorongan kebutuhan meskipun pada dasarnya terdapat sistem operasi lain yang bersifat *open source* atau dapat diakses dan diunduh secara bebas tanpa melakukan pembayaran apapun. Salah satu sistem operasi yang termasuk dalam *open source* adalah Linux. Linux tidak banyak diminati oleh masyarakat karena kurang memiliki daya tarik dan tidak mudah untuk digunakan.

Aspek lainnya adalah adanya sumber daya manusia (SDM). Teknologi informasi dengan operator yang mengawali mempunyai hubungan yang erat dan keduanya tidak dapat dipisahkan. Sumber daya manusia dan teknologi informasi mempunyai peranan penting yaitu sebagai pengendali dari sebuah alat. Pelaku tindak pidana *cracking* sistem

operasi Windows mempelajari dan meneliti mengenai tindak pidana ini. Hal lain yang dapat memengaruhi adalah bermunculan komunitas baru dalam kehidupan sosial. Dengan adanya teknologi sebagai sarana untuk mencapai tujuan, diantaranya media internet sebagai sarana untuk berkomunikasi, secara sosiologis terbentuklah sebuah komunitas baru salah satunya adalah komunitas *cracker* yang keberadaannya sangat tersembunyi dan dirahasiakan. Pada komunitas tersebut memudahkan antara satu pelaku dengan pelaku lainnya untuk mendapatkan informasi yang bermanfaat bagi kegiatannya melakukan *cracking.*

c. Faktor Masyarakat

Tindak pidana *cracking* sistem operasi Windows ini, masyarakat masih sangat rendah dalam kepatuhan terhadap hukum. Kesadaran masyarakat mengenai aturan ini masih sangat rendah karena berdasarkan penelitian yang dilakukan oleh penulis, sebagian besar pelaku tindak pidana *cracking* sistem operasi Windows mengetahui adanya peraturan perundang-undangan yang mengatur tentang tindak pidana *cracking* ini akan tetapi pelaku tetap melakukan tindak pidana tersebut.

d. Faktor Hukum

Praktik penyelenggaraan hukum di lapangan ada kalanya terjadi pertentangan antara tindak pidana yang terjadi dengan penegakan hukumnya. Setiap aparat dan aparatur penegak hukum memiliki tugas dan peran terkait dengan kegiatan pelaporan atau pengaduan, penyelidikan, penyidikan, penuntutan, pembukaan, penjatuhan vonis dan pemberian sanksi serta upaya pemasyarakatan kembali (resosialisasi) terpidana (Mulyanto, 2000:14).

Pada ketentuan Pasal 30 ayat (3) Undang-Undang Nomor 11 Tahun 2008 sebagaimana diperbaharui dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik menyebutkan: "*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*". Pasal ini diatur sebagai delik biasa sehingga siapa saja dapat melaporkan tindak pidana *cracking* sistem operasi Windows ini. Jika dilihat pada penerapan di lapangan, masyarakat belum mau melaporkan pelanggaran ini kepada pihak penegak hukum. Penegakan hukum tindak pidana *cracking* sistem operasi Windows ini juga tidak optimal karena belum pernah ada kasus yang dilaporkan mengenai tindak pidana *cracking* sistem operasi Windows di Polda Daerah Istimewa Yogyakarta. Hal ini membuat efek jera pada pelaku tindak pidana *cracking* sistem operasi Windows kurang. Pelaku tindak pidana *cracking* sistem operasi Windows juga mengetahui bahwa belum pernah ada pelaku yang tersentuh oleh sanksi pidana sehingga tujuan pemidanaannya tidak tercapai.

2. Modus Operandi Tindak Pidana *Cracking* Sistem Operasi Windows di Yogyakarta

Modus yang dilakukan oleh para *cracker* sistem operasi Windows dalam Pasal 30 ayat (3) Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diperbaharui oleh Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik biasanya disebut *Illegal access* yaitu suatu tindak pidana yang dilakukan dengan memasuki atau menyusup atau merusak ke dalam suatu sistem komputer secara ilegal atau tanpa izin dan sepengetahuan dari pemilik atau penyedia layanan suatu sistem. Langkah-langkah yang dilakukan oleh *cracker* sistem operasi Windows kurang lebih sama, sedangkan yang berbeda adalah metode dan dampak yang ditimbulkan. Adapun modus operandi *cracker* sistem operasi Windows dibedakan menjadi 2 (dua) yaitu sebagai berikut:

a. Tindak Pidana *Cracking* Sistem Operasi Windows secara Langsung

Tindak pidana *cracking* sistem operasi Windows dapat dilakukan secara langsung tanpa menggunakan program lain. Metode ini memiliki tingkat kesulitan yang tinggi karena tidak semua orang dapat melakukan *cracking* dengan metode ini, dibutuhkan *cracker* dengan tingkat pengetahuan dan kemampuan terhadap teknologi yang tinggi. *Cracking* dengan metode ini memiliki beberapa tahapan umum yang hanya dapat dilakukan oleh seorang pelaku *cracker* yang handal. Tahapan-tahapan melakukan *cracking* tersebut antara lain adalah:

1) *Footprinting* dan/atau Pencarian Data;

   Kegiatan yang dilakukan pada tahap ini adalah menentukan ruang lingkup serangan kemudian melakukan interogasi pada jaringan dan mengintai jaringan tersebut.

2) *Scanning* atau Pemilihan Sasaran;

   Pada tahapan ini sangat rawan karena dapat memunculkan jaringan yang tidak tenang sehingga mudah dikenali oleh sistem. Seorang *cracker* dapat menggunakan alat khusus untuk melindungi diri dari kegiatan *scanning* dengan memasang *firewall* atau dengan menggunakan aplikasi Snort.

3) *Enumeration* atau Pencarian Data Mengenai Sasaran;

   Pada tahapan ini, *cracker* mencari data mengenai sasaran. Pada sistem Windows, terdapat *port 139* (NetBIOS *session service)* yang terbuka untuk berbagi sumber antar pemakai dalam jaringan. NetBIOS tersebut dapat dilihat oleh semua orang.

4) *Gaining Access* atau Akses Ilegal;

   Pada tahapan ini berupa kegiatan untuk mencoba mendapatkan suatu akses pada sistem sebagai pengguna biasa. Apabila *resource share* telah diproteksi dengan kata sandi, maka kata sandi ini dapat ditebak. Proses menebak dapat dilakukan secara otomatis melalui *dictionary attack* (mencobakan kata-kata dari kamus sebagai suatu *password*) atau *brute-force attack* (mencobakan kombinasi semua karakter sebagai *password*).

5) *Escalating Privilege* atau Menaikkan Posisi;

   Pada tahap ini diasumsikan bahwa seorang *cracker* sudah mendapatkan izin akses pada sistem sebagai pengguna biasa. *Cracker* yang sudah mendapat izin akan berusaha menaikkan posisi menjadi admin (pada sistem Windows). Posisi *cracker* yang sudah naik menjadi admin ini memberikan keuntungan dengan dapat mengakses secara bebas dan mengatur sistem tersebut.

6) *Pilfering* atau Proses Pencurian;

   Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke *trusted system*. Mencakup evaluasi *trust* dan pencarian *cleartext password* di *registry, config file*, dan *user data*.

7) *Covering Tracks* atau Menutup Jejak;

   Pada tahapan ini merupakan suatu tahapan yang penting karena harus membersihkan jaringan dan menutup jejak menggunakan program tertentu.

8) *Denial of Service* atau Melumpuhkan Sistem;

   Tahapan ini bukan merupakan tahapan terakhir melainkan suatu tahapan yang dilakukan apabila *cracker* tidak berhasil memasuki sistem yang kuat pertahanannya maka hal yang dapat dilakukan adalah melumpuhkan sistem dengan melakukan penyerangan secara bertubi-tubi.

b. Tindak Pidana *Cracking* Sistem Operasi Windows Secara Tidak Langsung

1) Menggunakan Program Windows

Pada sistem operasi Windows terdapat beberapa program yang dapat dimanfaatkan dengan baik salah satunya adalah *command prompt* atau CMD. Program *command prompt* adalah suatu perintah yang sudah disediakan oleh Windows untuk menjalankan file dengan cara menuliskan perintahnya atau secara sederhana dapat diartikan sebagai sistem operasi berbasis baris perintah.

Tindak pidana *cracking* sistem operasi Windows menggunakan *command prompt* ini memiliki tingkat kesulitan sedang karena seorang *cracker* harus menemukan kode atau kunci seri (*serial key*) sendiri agar dapat melakukan aktivasi pada Windows. Seorang *cracker* akan mencoba satu persatu kunci seri yang terdapat di internet secara bebas kemudian disesuaikan dengan permintaan versi Windows yang akan diaktivasi secara ilegal. Apabila berhasil maka ketika diperiksa melalui *system info* pada *control panel* akan muncul tulisan berupa "*Windows activated*" sedangkan *cracking* yang gagal akan memunculkan kotak dialog bertuliskan "*code error*" atau "*key is blocked*". Hal yang dapat dilakukan oleh pelaku *cracking* sistem operasi Windows apabila *crack* tidak berhasil adalah menghapus kembali baris perintah yang telah dimasukkan supaya *command prompt* dapat menerima perintah yang lainnya.

2) Menggunakan Program Tambahan (Pihak Ketiga)

Tindak pidana *cracking* sistem operasi Windows pada masa kini dipermudah dengan munculnya beberapa program yang secara instan dapat melakukan *cracking*. Program-program ini berasal dari seorang *cracker* yang handal yang melakukan tindak pidana *cracking* dengan metode langsung atau tanpa perantara alat. *Cracker* tersebut kemudian menuangkan hasil pemikiran dan uji cobanya melalui suatu program yang saat ini tersebar luas secara bebas di internet. Program-program tersebut antara lain KMS, Loader, RemoveWat, Windows Activator, dan lain sebagainya.

Sebagian besar program tersebut sudah secara langsung bertindak sebagai *patch* (kunci yang menghubungkan *cracker* dengan sistem sehingga tidak perlu memunculkan kode untuk dimasukkan) atau bertindak sebagai *keygen* (kunci yang memunculkan kode atau nomor seri supaya *cracker* dapat memasuki sistem dengan cara memasukkan nomor seri tersebut pada waktu sistem membutuhkan. Hal yang perlu diperhatikan adalah koneksi internet dan antivirus pada saat proses *cracking*. Koneksi internet akan menghubungkan *cracker* atau pengguna Windows dengan sistem pada Microsoft sehingga akan terdeteksi bahwa adanya penyusup atau akses ilegal pada sistem tersebut. Antivirus berperan untuk memberantas virus yang masuk dalam perangkat oleh karena program-program tersebut didapat dari sumber yang bebas maka kemungkinan besar program tersebut membawa virus atau virus sudah menempel pada program tersebut sehingga antivirus akan mendeteksi program tersebut sebagai suatu virus atau *malware*.

D. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dijabarkan penulis, maka dapat ditarik suatu kesimpulan bahwa:

1. Faktor penyebab terjadinya tindak pidana *cracking* sistem operasi Windows di Daerah Istimewa Yogyakarta adalah sebagai berikut:
   a. Faktor ekonomi;

      Tujuan ekonomi melakukan tindak pidana *cracking* sistem operasi Windows ada 2 (dua) yaitu:

1) Kepentingan pribadi yaitu Windows hanya digunakan oleh pelaku dan tidak dijual bebas.
2) Kepentingan penjualan. Pelaku tindak pidana *cracking* sistem operasi Windows menjual jasa melakukan *cracking* sistem operasi Windows untuk mendapatkan keuntungan materiil.

b. Faktor sosial dan budaya;

Pada faktor sosial dan budaya terdapat 3 (tiga) aspek yang memengaruhi. Aspek tersebut antara lain adalah:

1) Kemajuan teknologi informasi
2) Adanya sumber daya manusia yang mendukung
3) Munculnya komunitas baru pada bidang teknologi informasi

c. Faktor masyarakat;

Kesadaran masyarakat terhadap tindak pidana *cracking* sistem operasi Windows ini masih sangat rendah karena meskipun masyarakat mengetahui bahwa tindak pidana *cracking* sistem operasi Windows ini telah diatur dalam undang-undang tetapi tetap dilakukan. Kesadaran yang rendah membawa pada tingkat kepatuhan yang juga rendah.

d. Faktor hukum.

Tindak pidana *cracking* sistem operasi Windows ini telah diatur dalam Pasal 30 ayat (3) Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diperbaharui dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Penegakan hukum yang lemah membuat pelaku tidak berhenti melakukan tindak pidana *cracking* sistem operasi Windows ini karena merasa aman dari jeratan hukum.

2. Modus operandi tindak pidana *cracking* sistem operasi Windows di Daerah Istimewa Yogyakarta adalah sebagai berikut:

a. *Cracking* secara langsung;

Metode ini terdiri dari beberapa tahapan yang hanya dapat dilakukan oleh seorang *cracker* yang ahli dalam bidang teknologi. Tahapan tersebut antara lain adalah:

1) *Footprinting* dan/atau Pencarian Data;
2) *Scanning* atau Pemilihan Sasaran;
3) *Enumeration* atau Pencarian Data Mengenai Sasaran;
4) *Gaining Access* atau Akses Ilegal;
5) *Escalating Privilege* atau Menaikkan Posisi;
6) *Pilfering* atau Proses Pencurian;
7) *Covering Tracks* atau Menutup Jejak;
8) *Denial of Service* atau Melumpuhkan Sistem;

b. *Cracking* secara tidak langsung.

Metode ini menerapkan tindak pidana *cracking* sistem operasi Windows melalui suatu program bantuan sehingga dapat dilakukan dengan mudah. Program tersebut terbagi ke dalam dua jenis, yaitu:

1) Program Windows
2) Program Tambahan

E. Saran

Berdasarkan hasil penelitian dan pembahasan yang telah dijabarkan penulis, maka peneliti memberikan saran sebagaimana berikut:

1. Pemerintah melakukan sosialisasi kepada masyarakat dengan lebih mengenalkan eksistensi Undang-Undang Nomor 11 Tahun 2008 sebagaimana diperbaharui oleh Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dalam rangka mengantisipasi meningkatnya tindak pidana *cracking* sistem operasi Windows;
2. Pemerintah seharusnya menciptakan undang-undang lebih khusus (pembaharuan hukum) mengenai tindak pidana ini karena peraturan perundang-undangannya terlihat belum jelas sehingga penegakannya pun belum optimal;
3. Aparat penegak hukum membentuk tim untuk berpatroli dalam menangani kasus tindak pidana yang sudah dilatih secara khusus untuk mempelajari modus-modus operandi tindak pidana.

F. Daftar Pustaka

Antoni. 2017. "Kejahatan Dunia Maya (*Cyber Crime*) Dalam Simak Online". *Jurnal Nurani.* Volume 17 Nomor 2.

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

Mulyatno. 2000. *Asas-asas Hukum Pidana.* Jakarta: Rineka Cipta

R. Soesilo. 1985. *Kriminologi (Pengetahuan Tentang Sebab-Sebab Kejahatan).* Bogor: Politeia

Rudi Hermawan. 2013. "Kesiapan Aparatur Pemerintah Dalam Menghadapi *Cyber Crime* di Indonesia". *Jurnal Faktor Exacta*. Volume 6 Nomor 1.

Soerjono Soekanto. 2010. *Pengantar Penelitian Hukum*. Jakarta: UI Press.

Sudarto. 1990. *Hukum Pidana Jilid IA-IB.* Semarang: Fakultas Hukum UNDIP.

Widodo. 2009. *Sistem Pemidanaan dalam Cyber Crime*. Yogyakarta: Aswaja Pressindo.