UNSUR PIDANA *HACKING* DALAM UNDANG-UNDANG NOMOR 11 TAHUN 2008 MENURUT HUKUM ISLAM

(Analisis Putusan Pengadilan Negeri Jember Nomor 253/pid B/2013/PN JR)

SKRIPSI

Diajukan Oleh:

HAUZAN AKMAL
NIM. 140104014
Mahasiswa Fakultas Syari'ah dan Hukum
Prodi Hukum Pidana Islam

FAKULTAS SYARI'AH DAN HUKUM
UNIVERSITAS ISLAM NEGERI AR-RANIRY
DARUSSALAM-BANDA ACEH
2024 M/1445 H

UNSUR PIDANA *HACKING* DALAM UNDANG-UNDANG NOMOR 11 TAHUN 2008 MENURUT HUKUM ISLAM
(Analisis putusan pengadilan Negeri Jember Nomor 253/pid B/2013/PN JR)

SKRIPSI

Diajukan Kepada Fakultas Syariah dan Hukum
Universitas Islam Negeri (UIN) Ar-Raniry Banda Aceh
Sebagai Salah Satu Beban Studi Program Sarjana (S-1)
dalam Ilmu Hukum Pidana Islam

Oleh

HAUZAN AKMAL
NIM. 140104014
Mahasiswa Fakultas Syari'ah dan Hukum
Prodi Hukum Pidana Islam

Disetujui Untuk Dimunaqasyahkan Oleh:

Pembimbing I,	Pembimbing II,
Dr.Abdul Jalil Salam, S.Ag.,MA	Muslem,S.Ag.,M.H.
NIP. 197011091997031001	NIND 2011057701

UNSUR PIDANA *HACKING* DALAM UNDANG-UNDANG NOMOR 11 TAHUN 2008 MENURUT HUKUM ISLAM
(Analisis Putusan Pengadilan Negeri Jember Nomor: 253/Pid.B/2013/PN JR)

SKRIPSI

Telah Diuji oleh Panitia Ujian Munaqasyah Skripsi
Fakultas Syariah dan Hukum UIN Ar-Raniry
dan Dinyatakan Lulus Serta Diterima
Sebagai Salah Satu Beban Studi
Program Sarjana (S-1)
dalamIlmu Hukum
Pidana Islam

Pada Hari/Tanggal: Kamis, 28 Januari, 2021 M
15 Jumadil Akhir 1442 H

Di Darussalam, Banda Aceh
Panitia Ujian Munaqasyah Skripsi

Ketua	Sekretaris
Dr. Abdul Jalil Salam, M.Ag	Muslem, S.Ag., M.H
NIP 197011091997031001	NIDN 2011057701
Penguji I	**Penguji II**
Saifuddin, S.Ag., M.Ag	Muhammad Iqbal, MM
NIP 197102022001121002	NIP 197005122014111001

Mengetahui,
Dekan Fakultas Syariah dan Hukum
UIN Ar-Raniry Banda Aceh

Prof. Muhammad Siddiq, M.H, Ph.D
NIP. 197703032008011015

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA ACEH
FAKULTAS SYARI'AH DAN HUKUM
Jl. Syeikh Abdul Rauf Kopelma Darussalam Banda Aceh
Telp./Fax. 0651-7557442 Email: fash@ar-raniry.ac.id

LEMBARAN PERNYATAAN KEASLIAN KARYA ILMIAH

Yang bertanda tangan dibawah ini:

Nama : Hauzan Akmal
NIM : 140104014
Fakultas/Jurusan : Syariah dan Hukum/ Hukum Pidana Islam

Dengan ini menyatakan bahwa dalam penulisan skripsi ini,saya:

1. ***Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggungjawabkan.***
2. ***Tidak melakukan plagiasi terhadap naskah karya orang lain.***
3. ***Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya.***
4. ***Tidak melakukan manipulasi dan pemalsuan data.***
5. ***Mengerjakan sendiri dan mampu bertanggung jawab atas karya ini.***

Bila dikemudian hari ada tuntutan dari pihak lain atas karya saya melalui pembuktian yang dapat dipertanggung jawabkan dan teryata ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap untuk dicabut gelar akademik saya atau diberikan sanksi lain berdasarkan aturan yang berlaku di Fakultas Syari'ah dan Hukum UIN Ar-Raniry.

Demikian pernyataan ini saya buat dengan sesungguhnya,

Banda Aceh, 11 Desember 2020
Yang menyatakan,

Hauzan Akmal
NIM. 140104014

ABSTRAK

Nama	: Hauzan Akmal
NIM	: 140104014
Fakultas/Jurusan	: Syariah dan Hukum/ Hukum Pidana Islam
Judul	: UNSUR PIDANA HACKING DALAM UNDANG-UNDANG NOMOR 11 TAHUN 2008 MENURUT HUKUM ISLAM (Analisis Putusan Pengadilan Negeri Jember Nomor 253/pid B/2013/PN JR)
Tebal Skripsi	: 66
Pembimbing I	: Dr. Abdul Jalil Salam, S. Ag., MA
Pembimbing II	: Muslem, S. Ag., M.H.
Kata Kunci	: Hacking, Hukum Islam, Unsur Pidana.

Perkembangan globalisasi menyebabkan perkembangan teknologi dan informasi. Kemajuan dalam bidang teknologi informasi menyebabkan perubahan besar-besaran dalam peradaban manusia, perkembangan tersebut tidak dapat dipisahkan dari komputer dan internet. Perkembangan teknologi komunikasi dan informasi ini tidak selamanya membawa dampak positif untuk kehidupan manusia. Jika perkembangan ini dilakukan dengan sebagaimana mestinya, sudah tentu akan membawa manfaat yang sangat besar, namun jika tidak malah sebaliknya. Dalam hal ini seperti *Hacking* yang pada dasarnya adalah seni dalam menembus sistem komputer untuk mengetahui seperti apa sistem tersebut dan bagaimana fungsinya. Dalam penelitian ini, penulis mencoba mengetahui tinjauan tindak pidana *hacking* dalam Undang-Undang Nomor 11 tahun 2008 dan menganalisis putusan Pengadilan Negeri Jember Nomor 253/pid B/2013/PN JR melihat bagaimana tinjauan hukum Islam terhadap *Hacking*. Kemudian keduanya dianalisis dengan metodelogi deskriptif analisis dan metode penelitian kualitatif. Hasil analisis bahwa Putusan Pengadilan Negeri Jember menjatuhkan hukuman berdasarkan perbuatan yang telah meretas server dan membuat akun secara illegal dan secara sah terbukti melakukan tindak pidana dan tanpa hak melawan hukum mengakses komputer dan sistem elektronik milik orang lain sehingga hakim menjatuhkan pidana kepada terdakwa MJL007 selama 6 bulan penjara dan denda sebesar Rp. 250 000,- (dua ratus lima puluh ribu subsidair 15 hari kurungan. Sedangkan dalam hukum Islam lebih fleksibel dalam melihat aktivitas *Hacking* yaitu, dengan tidak mengikat para *hacker* dalam melakukan *hacking* atas dasar untuk mencapai kemaslahatan yang lebih besar (saddu az-zari'ah).

KATA PENGANTAR

بِسْـــــــــــــمِ اللهِ الرَّحْمَنِ الرَّحِيْمِ

Dengan mengucapkan puji beserta syukur penulis panjatkan kehadirat Allah SWT, atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini Dalam rangka menyelesaikan studi pada Fakultas Syari'ah dan Hukum Universitas Islam Negeri Ar-Raniry, penulis berkewajiban untuk melengkapi dan memenuhi salah satu persyaratan akademisi untuk menyelesaikan Studi pada Program Sarjana (S-1) Fakultas Syari'ah dan Hukum UIN Ar-Raniry Banda Aceh, untuk itu penulis memilih judul yang berjudul **"UNSUR PIDANA *HACKING* DALAM UNDANG-UNDANG NOMOR 11 TAHUN 2008 MENURUT HUKUM ISLAM (Analisis Putusan Pengadilan Negeri Jembar Nomor 253/pid B/2013/PN JR)".** Selanjutnya shalawat dan salam penulis sanjungkan kepada baginda kita Nabi besar Muhammad SAW. Beserta keluarnya dan sahabat beliau yang telah menunjukkan umat manusia kejalan yang lurus. Skripsi ini disusun untuk melengkapi dan memenuhi salah satu syarat untuk memperoleh gelar sarjana pada Fakultas Syari'ah dan Hukum UIN Ar-Raniry Banda Aceh.

Penyusunan skripsi ini berhasil diselesaikan berkat bantuan berbagai pihak. Dalam kesempatan ini penulis mengucapkan terima kasih sebesar-besarnya kepada bapak Dr. Abdul Jalil Salam, S. Ag., MA sebagai pembimbing I dan bapak Muslem S.Ag., MH sebagai pembimbing II. Dimana pada saat-saat kesibukannya sebagai dosen di Fakultas Syari'ah dan Hukum masih menyempatkan diri untuk memberikan bimbingan dan pengarahan, sehingga skripsi ini diselesaikan meski bukan seperti target semula.

Terima Kasih penulis ucapkan kepada Penasehat Akademik Bapak Dr. Hasanuddin Yusuf Adan, MCL., M.A yang telah membimbing penulis dari sejak kuliah hingga skripsi ini selesai. Ucapan terima kasih kemudian kepada Bapak Muhammad Siddiq, M.H., PhD selaku Dekan Fakultas Syari'ah dan

Hukum, serta seluruh staff akademika Fakultas Syariah Dan Hukum. Selanjutnya kepada Dr. Faisal, S. TH., MA selaku Ketua Prodi Hukum Pidana Islam. Staff Prodi Hukum Pidana Islam dan juga seluruh staf akademik Fakultas Syari'ah dan Hukum beserta jajaran dosen yang telah membimbing penulis selama masa pendidikan di Fakultas Syari'ah dan Hukum UIN Ar-Raniry.

Penulis berharap penyusunan skripsi ini dapat bermanfaat bagi penulis sendiri dan juga pihak-pihak yang ingin membacanya. Penulis menyadari bahwa skripsi ini masih banyak kekurangan, untuk itu dengan kerendahan hati penulis menerima kritikan atau saran yang bersifat konstruktif dari semua pihak demi kesempurnaan dan untuk pengetahuan penulis di masa mendatang.

Akhirnya kepada Allah SWT, penulis memohon doa semoga amal bantuan yang telah diberikan oleh semua pihak mendapat pahala dari-Nya. Tiada kata yang paling indah untuk mengungkapkan semua ini, hanya satu kata Alhamdulillahirabbil'alamin.

Banda Aceh, 17 Februari 2024

Penulis,

Hauzan Akmal
NIM. 140104014

TRANSLITERASI

Keputusan Bersama Menteri Agama dan Menteri Pendidikan dan Kebudayaan

Nomor: 158 Tahun 1987 – Nomor: 0543 b/u/1987

1. Konsonan

No	Arab	Latin	Ket	No	Arab	Latin	Ket
1	ا	Tidak dilambangkan		16	ط	ṭ	t dengan titik di bawahnya
2	ب	b		17	ظ	ẓ	z dengan titik di bawahnya
3	ت	t		18	ع	‘	
4	ث	ṡ	s dengan titik di atasnya	19	غ	G	
5	ج	j		20	ف	F	
6	ح	ḥ	h dengan titik di bawahnya	21	ق	Q	
7	خ	kh		22	ك	K	
8	د	d		23	ل	L	
9	ذ	ż	z dengan titik di atasnya	24	م	M	
10	ر	r		25	ن	N	
11	ز	z		26	و	W	
12	س	s		27	ه	h	
13	ش	sy		28	ء	’	
14	ص	ṣ	s dengan titik di bawahnya	29	ي	y	
15	ض	ḍ	d dengan titik di bawahnya				

2. Vokal

Vokal bahasa Arab, seperti vokal bahasa Indonesia, terdiri dari vokal tunggal atau monoftong dan vokal rangkap atau diftong.

a. Vokal Tunggal

Vokal tunggal bahasa Arab yang lambangnya berupa tanda atau harkat, transliterasinya sebagai berikut:

Tanda	Nama	Huruf Latin
◌َ	*Fatḥah*	A
◌ِ	*Kasrah*	I
◌ُ	*Dhammah*	U

b. Vokal Rangkap

Vokal rangkap bahasa Arab yang lambangnya berupa gabungan antara harkat dan huruf, transliterasinya gabungan huruf, yaitu:

Tanda dan Huruf	Nama	Gabungan Huruf
◌َي	*Fatḥah* dan ya	Ai
◌َو	*Fatḥah* dan wau	Au

Contoh:

كيف : *kaifa* هول : *haula*

3. Maddah

Maddah atau vokal panjang yang lambangnya berupa harkat dan huruf, transliterasinya berupa huruf dan tanda, yaitu:

Harkat dan Huruf	Nama	Huruf dan Tanda
◌َا/ي	*Fatḥah* dan alif atau ya	*Ā*

ـِي	*Kasrah* dan ya	Ī
ـُي	*Dammah* dan waw	Ū

Contoh:

قال : *qāla*

رمى : *ramā*

قيل : *qīla*

يقول : *yaqūlu*

4. Ta *Marbutah* (ة)

Transliterasi untuk ta marbutah ada dua:

a. Ta *marbutah* (ة) hidup

Ta marbutah (ة) yang hidup atau mendapat harkat *fatḥah, kasrah* dan *dammah*, transliterasinya adalah t.

b. Ta *marbutah* (ة) mati

Ta marbutah (ة) yang mati atau mendapat harkat sukun, transliterasinya adalah h.

c. Kalau pada suatu kata yang akhir katanya ta *marbutah* (ة) diikuti oleh kata yang menggunakan kata sandang al, serta bacaan kedua kata itu terpisah maka ta *marbutah* (ة) itu ditransliterasikan dengan h.

Contoh:

روضةالاطفال : *rauḍah al-aṭfāl/ rauḍatul aṭfāl*

المدينةالمنورة : *al-Madīnah al-Munawwarah/ al-Madīnatul Munawwarah*

طلحة : *Ṭalḥah*

Catatan:

Modifikasi

1. Nama orang berkebangsaan Indonesia ditulis seperti biasa tanpa transliterasi, seperti M. Syuhudi Ismail. Sedangkan nama-nama lainnya ditulis sesuai kaidah penerjemahan. Contoh: Hamad Ibn Sulaiman.
2. Nama negara dan kota ditulis menurut ejaan bahasa Indonesia, seperti Mesir, bukan Misr; Beirut, bukan Bayrut; dan sebagainya.
3. Kata-kata yang sudah dipakai (serapan) dalam kamus bahasa Indonesia tidak ditransliterasikan. Contoh: Tasauf, bukan Tasawuf.

DAFTAR LAMPIRAN

DAFTAR ISI

BAB SATU
PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan globalisasi menyebabkan perkembangan teknologi dan informasi. Kemajuan dalam bidang teknologi informasi yang menyebabkan perubahan besar-besaran dalam peradaban manusia, perkembangan tersebut tidak dapat dipisahkan dari komputer dan internet. Komputer dan internet sebagai penemuan yang begitu mengangumkan merupakan awal dari pencapaian apa yang telah manusia rasakan saat ini.[1] Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global. Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat.[2] yang mana budaya tersebut yang membuat setiap orang berhak untuk mendapatkan pengetahuan seluas-luasnya. Hal tersebut sangat dimungkinkan sebab cara bergaul di dalam *Cyberspace* tidak mengenal lagi batasan-batasan negara, suku, bangsa dan kelompok. Kejadian yang terjadi di suatu negara dapat dengan mudah diketahui oleh negara lainya yang berjarak ratusan ribu kilometer hanya beberapa menit setelah kejadian.

Cyberspace merupakan sebagai sebuah dunia komunikasi yang berbasis komputer. *Cyberspace* juga menjadi sebagai sebuah kebiasan baru dalam kehidupan manusia yang dalam bahasa sehari-hari dikenal dengan

[1] Budi Agus Riswansi, *Hukum dan Internet di Indonesia*, (Yogyakarta: UII Press,2003), hlm. 1.

[2] Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, (Bandung: PT. Refika Aditama, 2004), hlm. 1.

sebutan internet.[3] Internet dapat dikatakan sebagai dunia virtual yang tidak ada batasannya. Internet memiliki jaringan-jaringan yang dapat menghubungkan satu pengguna komputer dengan pengguna komputer yang lain dari seluruh penjuru dunia. Jarak bukanlah masalah bagi internet

Perkembangan teknologi komunikasi dan informasi ini tidak selamanya membawa dampak positif untuk kehidupan manusia. Jika perkembangan ini dilakukan dengan sebagaimana mestinya, sudah tentu akan membawa manfaat yang sangat besar. Akan tetapi jika dimanfaatkan dengan niat untuk melakukan suatu kejahatan maka akan menimbulkan dampak yang negatif. Sebab komputer dan internet sebagai ciptaan manusia memiliki karakteristik yang mudah dieksploitasi oleh siapa saja yang memiliki keahlian di bidang tersebut.

Dalam pembahasan komputer dan internet tidak akan mungkin terlepas dari pembahasan masalah keamanan dari kedua teknologi tersebut. Kecanggihan komputer dan internet dapat memunculkan masalah baru, yaitu kejahatan. Komputer dan internet akan menjadi sarana kejahatan yang canggih bagi pelaku kejahatan dalam melancarkan aksinya. Tindak kejahatan menggunakan media komputer dan internet dikenal dengan istilah *cybercrime.*

Cybercrime merupakan kejahatan yang meliputi beberapa jenis kejahatan yang tidak asing lagi seperti kejahatan pencurian, pelanggaran HAKI, Pembajakan, fitnah secara online, Pornografi dan lain-lain. Tetapi memiliki perbedaan tersebut terletak pada media yang digunakan untuk melakukan kejahatan yaitu komputer dan internet. *Cybercrime* merupakan

[3] Maskun, *Kejahatan Siber Cyber Crime Suatu Pengantar*,(Jakarta: Kencana Prenada Media Group, 2013), hlm. 46.

salah satu sisi gelap dari kemajuan teknologi komunikasi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini.[4]

Komputer dan internet juga memunculkan beberapa tindak kejahatan baru seperti menyusup ke suatu sistem komputer tanpa izin. Suatu tindakan dimana seseorang mengakses ke komputer milik orang lain melalui sistem program tertentu, dalam hal ini pembahasan menyangkut salah satu aktivitas dalam dunia *Cyberspace* yaitu *Hacking* yang merupakan suatu seni dalam menembus sistem komputer untuk mengetahui seperti apa sistem tersebut dan bagaimana berfungsinya,[5] *Hacking* itu sendiri terbagi menjadi dua *white hats hacker* adalah tindakan hacking yang dilakukan atas izin dan atas sepengetahuan pemilik, dan *black hats hacker* tindakan hacking yang dilakukan tanpa izin dan tanpa sepengetahuan pemilik dan memiliki tujuan untuk kepentingan diri sendiri.

Namun Penulis lebih memfokuskan pada pembahasan *black hats hacker* yang melakukan akses terhadap sistem komputer tanpa seizin atau dengan melawan hukum sehingga dapat menembus sistem pengamanan komputer yang dapat mengancam berbagai kepentingan.[6] sebagai sebuah bentuk kegiatan telah ada dan berkembang bersama perkembangan teknologi komputer dan internet.

Kemajuan teknologi komputer dan internet saat ini tidak akan terlepas dari *hacking.* Sebab awal mulanya *hacking* merupakan suatu bentuk kegiatan seorang *hacker* untuk meningkatkan performa, menguji sistem, atau mencari *bug* suatu program komputer dan internet. Oleh karena itu, *hacking*

---

[4] Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: PT. Raja Grafindo Persada, 2007), hlm. 1-2.

[5] Maskun, *kejahatan Siber Cyber Crime Suatu Pengantar*, (Jakarta: Kencana Prenada Media Group, 2013), hlm. 64.

[6] Niniek Suparni, *Cyberspace Problematika & Antisipasi Pengaturannya*, (Jakarta: Sinar Grafika, 2009), hlm. 6.

diperlukan untuk, mengubah-ubah, membongkar pasang sistem, *software* atau *hadware* komputer yang telah dimiliki.

Tentunya untuk *hacker* yang bersifat positif (*white hats hacker*) akan banyak memberikan manfaat dan kemudahan yang didapat dari kemajuan teknologi komputer dan internet, dan tidak dapat dipungkiri bahwasanya dengan perkembangan teknologi ini juga dapat menciptakan kejahatan yang semulanya bersifat konvensional berkembang menjadi sebuah kejahatan modern dengan tingkat kerugian yang lebih besar dengan dampak yang luas.

Pemerintah Indonesia juga sudah mengesahkan Undang-undang ITE Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang diharapkan dapat menghadapai kegiatan *hacking* yang marak terjadi di Indonesia serta dapat menjawab berbagai persoalan yang timbul dari kasus yang menyangkut teknologi informasi, termasuk *hacking,* perihal tersebut dibuktikan dengan pembaruan Undang-Undang ITE Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Membuktikan bahwa pemerintah Indonesia sangat berupaya untuk menjerat para *hacker*, meskipun dalam Undang-Undang Nomor 11 Tahun 2008 tidak secara eksplisit menyebutkan *hacking* di dalamnya. Tujuan lain dari Undang-Undang Nomor 11 Tahun 2008 agar dapat menutupi kelemahan dari KUHP, KUHAP dan Undang-Undang terkait yang dipandang sudah tidak mampu untuk menjawab berbagai permasalahan yang timbul akibat penerapan teknologi informasi di masyarakat.

Dalam Undang-Undang Nomor 11 Tahun 2008 telah dijelaskan mengenai tidak pidana *Hacking* dalam Pasal 30 ayat 1 sampai 3.

(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.

Sedangkan mengenai hukuman bagi pelakunya diatur dalam Pasal 46 ayat 1 sampai 3.

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Dalam Islam yang menjadi agama hukum sudah pasti memiliki andil untuk merespon fenomena yang sedang terjadi di masyarakat. Perubahan situasi dan kondisi di masyarakat, termasuk akibat buruk yang ditimbulkan dari perkembangan teknologi informasi, salah satunya adalah tindak pidana *hacking*.

Dalam Hukum Islam sendiri belum terdapat aturan yang pasti dan jelas mengenai tindak pidana *Hacking* karena pada jaman dahulu belum adanya komputer dan internet yang membuat tidak munculnya persoalan mengenai kejahatan yang dilakukan melalui internet, tetapi berdasarkan pengertian dari *Hacking* maka dapat ditemukan perbuatan-perbuatan yang sudah ada pada zaman dulu seperti *Ghasab* (tindakan mempergunakan hak

milik orang lain tanpa seizin yang berhak)[7] yang mengarah pada perbuatan *Hacking* tetapi yang membedakannya adalah tempat melakukan perbuatan tersebut jika dalam dunia nyata *Ghasab* itu dilakukan ditempat yang nyata dan dapat di lihat secara nyata, sedangkan *Ghasab* dalam pengertian *Hacking* dilakukan di dalan dunia maya yaitu di dalam sistem jaringan-jaringan yang berupa kode-kode yang hanya dapat dipahami oleh mesin dan orang yang profesional dibidang itu.

Dalam putusan perkara Peradilan Negeri Jember Nomor : 253/Pid B/2013/PN JR menyatakan terdakwa yang bernama Wildan Yani Ansari Alias Yayan Alias MJL 007, terbukti melakukan tindak pidana *Hacking* terhadap server *my. Techscape.co.id* dengan menggunakan komputer billing warnet surya com milik CV. Surya Infotama, dengan menggunakan alat berupa *scrit* yang berbasis bahasa pemograman PHP, dan berhasil membuat account secara ilegal pada webshosting *www.jatirejanetwork.com* dan juga pelaku Wildan Yani alias MJL007 berhasil membuat akun domain *presidensby.info* diserver pihak perusahaan webhosting *Jatirejahost.com* dan berhasil menempatkan file HTML "Jember *Hacker* Team" di server *Jatirejahost.com*, sehingga bagi pengguna internet yang ingin mengakses konten diwebsite *www.presidensby.info* yang sebenarnya malah mengakses tampilan file HTML "Jember *Hacker* Team".

Berdasarkan uraian di atas dalam hal ini penulis tertarik untuk melakukan suatu penelitian ilmiah dengan judul ***"Unsur Pidana Hacking dalam Undang-Undang Nomor 11 Tahun 2008 Menurut Hukum Islam (Analisis putusan pengadilan Negeri Jember Nomor 253/pid B/2013/PN JR)"***

[7] *Esiklopedi Hukum Islam* ,(Jakarta: PT. Ichtiar Baru van Hoeven, 2006), hlm. 400-401.

B. Rumusan Masalah

Berdasarkan latar belakang yang dikemukakan diatas, penulis membatasi perumusan masalah sebagai berikut:

1. Bagaimana tinjauan tindak pidana *hacking* dalam Undang-Undang Nomor. 11 tahun 2008 menurut Hukum Islam?
2. Bagaimana Kajian Unsur Pidana *Hacking* dalam Putusan Pengadilan Negeri Jember Nomor. 253/Pid B/2013/PN JR Ditinjau Menurut Hukum Islam?

C. Tujuan Penelitian

Adapun Tujuan dalam penulisan ini adalah:

1. Untuk mengetahui tinjauan tindak pidana *hacking* dalam Undang-Undang Nomor. 11 tahun 2008 menurut perspektif Hukum Islam.
2. Untuk mengetahui Unsur Pidana *Hacking* Dalam Putusan Pengadilan Negeri Jember Nomor. 253/Pid B/2013/PN JR Ditinjau Menurut Hukum Islam.

D. Penjelasan Istilah

Untuk menghindari kesalahpahaman dalam menafsirkan istilah-istilah yang terdapat dalam judul skripsi ini, maka penulis menjelaskan istilah-istilah sebagai berikut ini:

1. *Hacking*

   Adalah suatu seni dalam menembus sistem komputer untuk mengetahui seperti apa sistem tersebut dan bagaimana berfungsinya, Hacking itu sendiri terbagi menjadi dua white hats hacker adalah tindakan hacking yang dilakukan atas izin dan atas sepengetahuan pemilik,[8] dan black hats hacker tindakan hacking yang dilakukan tanpa izin dan tanpa sepengetahuan pemilik dan memiliki tujuan

[8] Maskun, *kejahatan Siber Cyber Crime Suatu Pengantar*, (Jakarta: Kencana Prenada Media Group, 2013), hlm. 64.

untuk kepentingan diri sendiri. Seperti : pencurian, penyusupan, pencurian data merubah tampilan situs, pembajakan software, pencurian uang.

2. Hukum Islam

Secara kebahasaan, di dalam buku *Ensiklopedi Islam*, *al-hukm* berarti menetapkan sesuatu atas sesuatu atau tidak menetapkannya.[9] Sementara menurut Ushul Fiqh, definisi hukum adalah *khitab* Allah yang mengatur amal perbuatan *mukallaf* baik berupa *iqtida* (perintah, larangan, anjuran untuk melakukan atau anjuran untuk meninggalkan), *takhyir* (memilih untuk dikerjakan atau memilih untuk ditinggalkan) atau *wadh'I* (ketentuan yang menetapkan sesuatu sebagai sebab, syarat, atau penghalang).[10]

Di dalam buku *Metodologi Studi Islam* tergambar bahwa Islam dari segi kebahasaan berasal dari bahasa Arab, yaitu dari kata *salima* yang berarti selamat sentosa. Dari asal kata tersebut dibentuk kata *aslama* yang artinya memelihara dalam keadaan selamat sentosa dan berarti pula menyerahkan diri, tunduk, patuh dan taat. Kata *aslama* itulah yang selanjutnya menjadi kata Islam yang mengandung segala arti yang terkandung dalam arti pokoknya. Oleh sebab itu, orang yang berserah diri, patuh dan taat disebut sebagai orang muslim.[11]

Hukum Islam adalah seperangkat norma atau peraturan yang bersumber dari Allah SWT dan Nabi Muhammad SAW untuk mengatur tingkah laku manusia ditengah-tengah masyarakatnya. Atau dapat juga diartikan sebagai hukum yang bersumber dari ajaran

---

[9] Perpustakaan Nasional RI: Katalog Dalam Terbitan (KDT), *Ensiklopedi Islam*, (Jakarta: Ichtiar Baru Van Hoeve, 2005), hlm. 46.

[10] Satria Effendi, *Ushul Fiqh*, (Jakarta: Rajawali Pers, 2013), hlm. 62.

[11] Abuddin Nata, *Metodologi Studi Islam*, (Jakarta: Rajawali Pers, 2013), hlm. 62.

Islam. Sementara itu menurut Hasbi Ash-Shidqie, hukum Islam adalah koleksi dan upaya para fuqaha dalam menerapkan syari'at Islam sesuai dengan kebutuhan masyarakat. Sedangkan Muhammad Khudri Beik menyebutkan bahwa, hukum Islam adalah *khitab* Allah yang berhubungan dengan semua perbuatan orang-orang yang dibebebaskan hukum, baik yang berupa kebolehan atau ketetapan yang mesti dikerjakan.[12]

E. Kajian Kepustakaan

Berdasarkan penelusuran yang dilakukan tidak ditemukan tulisan yang sama dengan skripsi yang dikaji, tetapi dalam skripsi yang lain penulis menemukan judul *"Tinjauan Hukum Internasioanal Terhadap Kasus Hacking Sony Pictures Entertainment"* yang ditulis oleh Haryo Andi Setiaji tahun 2016 mahasiswa Universitas Hasanuddin. Dalam skripsinya dibahas tentang masalah Penerapan yurisdiksi dalam kasus hacking Sony Pictures Entertainment ada dua, yaitu prinsip teritorial objektif dan prinsip teritorial. Oleh karena itu negara yang merasa dirugikan atau negara tempat terjadinya kejahatan dapat memberlakukan yurisdiksinya. Dalam kasus ini, Amerika Serikat mengeluarkan sanksi kepada Korea Utara sebagai bentuk pembalasan serangan siber tersebut.

Selanjutnya skripsi yang ditulis oleh Fana Akbarkan, oleh mahasiswa Universitas Airlangga tahun 2007, dengan judul *"Tindak Pidana Cracking dan Hacking"*. Di dalam skripsinya memaparkan perbedaan mendasar antara *Cracking* dan *Hacking*. Tidak membahas kejahatan *hacking* menurut Undang-Undang ITE karena belum di undangkan pada saat itu.

Selain dari itu ada juga skripsi yang ditulis oleh Samira Agustina, mahasiswa Universitas Islam Negeri Ar-raniry Banda Aceh tahun 2014

[12] Hasbi Ash-Shiddieqi, *Filsafat Hukum Islam,* (Jakarta: Bulan Bintang, 1979), hlm. 24.

dengan judul *"Tindak Pidana Cyberporn dalam Undang-Undang Nomor. 11 Tahun 2008 ditinjau Menurut Hukum Islam".* Skripsi ini secara khusus membahas tentang kejahatan mayantara dalam kategori *Cyberporn* yang arah penelitianya berbeda dengan penulisan skripsi ini walaupun memiliki kesamaan dalam mengkaji undang-undang yang sama.

Kemudian buku yang ditulis oleh Khairul Anam yang berjudul "*Hacking VS Hukum Positif dan Islam*". Buku ini membahas secara umum tentang *Hacking* dan dalam buku ini juga membahas tentang *White Hat Hacker* dan *Black Hat Hacker.*

Kemudian skripsi yang ditulis oleh mahasiswa UIN Surabaya yang berjudul "*Studi Hukum Pidana Islam Terhadap Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia Dalam Putusan Pengadilan Negeri Jember Nomor.253/Pid.B/2013/PN.JR".* dalam skripsi ini lebih fokus pada sanksi yang diberikan oleh hakim kepada pelaku, sedangkan yang penulis kaji akan lebih fokus pada unsur *Hacking* yang terdapat dalam putusan Nomor.253/Pid.B/2013/PN.JR.

Berbeda dengan lima tulisan di atas, penelitian ini lebih fokus pada Unsur Pidana *Hacking* dalam Undang-Undang Nomor 11 Tahun 2008 menurut Hukum Islam (Kajian Putusan Pengadilan Negeri Jember Nomor 253/Pid B/2013/PN JR).

F. Metode Penelitian

Pada prinsipnya dalam setiap penulisan karya ilmiah selalu diperlukan data-data yang lengkap, objektif, mempunyai metode dan cara tertentu sesuai dengan permasalahannya yang diteliti. Penelitian secara ilmiah berarti suatu metode yang bertujuan untuk mempelajari satu atau beberapa gejala dengan menganalisa dan pemeriksaan yang mendalam

terhadap fakta tersebut untuk kemudian mengusahakan suatu pemecahan atas masalah-masalah yang ditimbulkan oleh fakta tersebut.[13]

1. Jenis Penelitian

Metode penelitian yang digunakan dalam penyusunan skripsi ini adalah deskriptif analisis, yaitu suatu metode untuk menganalisa dan memecahkan masalah berdasarkan gambaran yang dilihat dan didengar dari hasil penelitian baik dilapangan atau teori berupa data-data dan buku-buku yang berkaitan dengan topik pembahasan.[14] Selain itu, penulis juga menggunakan metode penelitian kualitatif yaitu penelitian yang mengacu pada norma hukum yang terdapat dalam peraturan perundang-undangan dan putusan pengadilan. Kajian data yang digunakan disini adalah Kajian terhadap putusan Pengadilan Negeri Jember No. 253/Pid. B/2013/PN JR. mengenai Unsur Pidana *Hacking* dalam Undang-Undang Nomor 11 Tahun 2008 menurut Hukum Islam.

2. Teknik Pengumpulan Data

Dalam mengumpulkan data yang berhubungan dengan objek kajian, yang berupa data primer dan sekunder, peneliti menggunakan sumber data *field research* (penelitian lapangan) dan *library reaserch* (penelitian kepustakaan), yaitu:

a. *Field research* (penelitian lapangan) adalah data primer dan merupakan suatu penelitian lapangan yang dilakukan terhadap objek pembahasan yang akan diteliti dan digunakan dalam penulisan skripsi ini. Di sini penulis mengadakan penelitian terhadap putusan Pengadilan Negeri Jember No 253/Pid B/2013/PN JR.

---

[13] Soerjono Soekanto, *Pengantar Penelitian Hukum*, (Jakarta: Universitas Indonesia 2006), hlm. 121.

[14] Muhammad Nazir, *Metode Penelitian*, (Jakarta: Gahalia Indonesia, 2004), hlm. 63.

b. *Library reasearch* (penelitian kepustakaan), yaitu pengumpulan data sekunder dan merupakan penelitian dengan menggunakan buku bacaan sebagai landasan untuk mengambil data yang ada dengan kaitannya dengan penulisan skripsi ini. Dalam hal ini penulis mengkaji buku-buku, artikel, majalah dan situs wabsite yang berkaitan dengan Unsur Pidana *Hacking* dalam Undang-Undang Nomor 11 Tahun 2008 menurut Hukum Islam, di antaranya buku Niniek Suparni yang berjudul *"Cyberspace Problematika dan Antisipasi Pengaturannya"*, Ahmad Wardi Muslich dengan bukunya yang berjudul *"Pengantar dan Asas Hukum Pidana Islam Fiqih Jinayah"*, serta beberapa buku lain yang mempunyai relevansi dengan materi pembahasan skripsi dalam hasil penelitian yang berkaitan dengan pembahasan isi.

G. Sistematika Pembahasan

Untuk memudahkan para pembaca dalam mengikuti pembahasan skripsi ini, maka dipergunakan sistematika pembahasannya dalam empat bab, sebagaimanatersebut dibawah ini:

Bab satu pendahuluan yang terdiri dari latar belakang masalah, rumusan masalah, tujuan penelitian, penjelasan istilah, kajian kepustakaan, metode penelitian dan sistematika pembahasan.

Bab dua *hacking* dalam dalam Undang-undang Nomor.11 Tahun 2008 yang berisi tentang Pengertian *hacking*, Ruang Lingkup Kerja *hacking*, macam-macam tipe *hacker*, unsur-unsur Pidana Kejahatan *Hacking* dan *Hacking* dalam Undang-Undang Nomor 11 Tahun 2008 dan KUHP Indonesia.

Bab tiga Kajian Putusan Pengadilan Negeri Jember Nomor 253/Pid B/2013/PN JR yang berisi tentang *Hacking* dalam Hukum Islam, Kronologi Putusan Pengadilan Negeri Jember Nomor 253/Pid B/2013/PN JR,dan

Kajian Unsur Pidana *Hacking* dalam Putusan Pengadilan Negeri Jember Nomor 253/Pid B/2013/PN JR menurut Hukum Islam.

Bab empat merupakan bab penutup dari keseluruhan pembahasan skripsi ini yang berisi kesimpulan dan saran dari penulis yang dianggap perlu.

DAFTAR PUSTAKA

Riswandi, Budi Agus. 2003. *Hukum dan Internet di Indonesia.* Yogyakarta: UII Press.

M. Ramli, Ahmad. 2004. *Cyber Law dan HAKI dalam Sistem Hukum Indonesia.* Bandung: PT. Refika Aditama.

Maskun. 2013. *Kejahatan Siber Cyber Crime Suatu Pengatar*. Jakarta: Kencana Prenada Media Group.

Arief, Barda Nawawi. 2007. *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia.* Jakarta: PT. Raja Grafindo Persada.

Suparni, Niniek. 2009. *Cyberspace Problematika & Antisipasi Pengaturannya.* Jakarta: Sinar Grafika.

Efendi, Satria. 2013. *Ushul Fiqh.* Jakarta: Rajawali Pers.

Nata, Abuadin. 2013. *Metodologi Studi Islam.* Jakarta: Rajawali Pers.

Nazir, Muhammad. 2004. *Metode Penelitian*. Jakarta: Ghalia Indonesia

Ash-Shidqie, Hasbi. 1979. *Filsafat Hukum Islam.* Jakarta: Bulan Bintang.

Soekanto, Soerjono. 2006. *Pengantar Penelitian Hukum.*Jakarta: Universitas Indonesia.

Sunggono, Bambang. 2007. *Pengantar Metodologi Penelitian Hukum.* Jakarta: PT. Raja Grapindo Persada.

Surakhmad, Winarno. 1978. *Dasar dan Teknik Research.*Bandung: Tarsito.

BAB DUA
HACKING DALAM UNDANG-UNDANG NOMOR 11 TAHUN 2008

A. Pengertian *Hacking*

Sebelum melangkah lebih jauh dalam memahami aturan-auran tentang *Hacking* makan lebih baiknya difahami dulu arti dari *hacking* itu secara menyeluruh agar tidak salah dalam membedakan mana yang dikatakan *Hacking* dan mana yang dikatakan kejahatan lain yang juga dapat dilakukan dengan menggunakan komputer dan jaringan sebagai wadah kejahatan tersebut.

Dalam perkembangannya *Hacking* sudah berkembang pesat di luar negeri dan begitu pula di Indonesia. Tentunya kejahatan ini sangat berbeda dengan kejahatan pada umumnya seperti perampokan. Contohnya perampokan bank di kota New York yang tidak ada pengaruh dan hubunganya dengan perampokan bank di Jakarta. Akan tetapi, *Hacking* yang terjadi dan dilakukan di New York dapat mempengaruhi dan berakibat di Indonesia, sebab para *hacker* di New York dapat secara langsung menyerang *wabsite* yang ada di Indonesia. Oleh karena itu perlu kiranya untuk mengetahui pekembangan *Hacking* di luar Indonesia, dan dapat memahami pengertian dari *Hacking*, *Cracking* (kraking), dan *Phreaking* (preking).

Hacking merupakan suatu seni dalam menembus sistem komputer untuk mengetahui seperti apa sistem tersebut dan bagaimana berfungsinya[15], 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 gate 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 didalami tidak lah demikian,

[15]Maskun, *Kejahatan Siber Cyber Crime Suatu Pengantar*, (Jakarta: Kencana Prenada Media Group, 2013), hlm. 64.

karena di lingkungan para *hacker* ada budaya dan aturan-aturan tertentu, serta memiliki motif dan tujuan yang berbeda-beda.

Walaupun illegal para hacker tidak seluruhnya jahat, *hacker* yang baik motifnya hanya untuk mencari tantangan dan kesenangan saja, membuktikan dirinya mampu menembus sistem, seperti dikatakan oleh 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 dengan *real hacker* atau *hacker* sejati (baik). Dalam perkembanganya juga muncul *cracker* yang merusak sistem, dan menyebarkan program-program Trojan Horse atau yang mengambil keuntungan finansial. Kemudian muncul juga *preaker* yang melakukan kejahatanya melalui telepon, *preaker* adalah *Hacking* dengan telepon. Menggunakan berbagai boks telepon yang berlainan dan 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 (luar negeri).[16]

Pada umumnya cara kerja *Hacker* sama dengan *cracker* yang berbeda adalah motivasi untuk melakukannya. *Phreaker* motivasinya sama dengan *cracker* (mencuri dan merusak) yang berbeda adalah cara dan sasaranya, *cracker* sasaranya jaringan komputer serta piranti lunaknya, sedangkan *phreaker* sasaranya jaringan telepon serta piranti lunak pencatat pulsa telepon.

[16]*Ibid.,* hlm.67

Dari defenisi diatas harus diperjelas kembali dari cara dan akibat yang ditimbulkan. Sebab cara dan akibat yang ditimbulkannya inilah yang akan membedakan mana *Hacking* yang baik dan *Hacking* yang melanggar hukum. Pada umumnya media sering salah kaprah dalam membedakan *hacking* baik dan *hacking* jahat (*cracker).*[17] Karena media sering menuduh pelaku kejahatan yang menggunakan komputer dan internet dengan sebutan *Hacker*. Padahal dari sekian banyaknya kejahatan komputer semuanya memiliki karakteristik yang berbeda dan otomatis pelakunya memiliki panggilan yang berbeda pula. Seperti dalam kejahatan konvensional pada umumnya, pelaku atau terdakwa bisa disebut pembunuh, pencuri, dan lain sebagainya sesuai tindakan yang bersangkutan. Begitu pula dalam kejahatan yang terjadi di dunia mayantara, pelaku kejahatan tersebut disebut sebagai *crackir, phreaking* dan lain sebagainya sesuai dengan kejahatanya.

B. Ruang Lingkup Kerja *Hacking*

Dalam penjelasan untuk cara yang digunakan dalam *Hacking* sangat berkaitan dengan kelompok atau tipe-tipe *Hacking.* Cara inilah yang akan membedakan siapa *hacker* yang baik dan hacker yang jahat. Dalam dunia *hacking* terdapat istilah *ethic* dan *unethic* hal inilah yang membedakan mana *hacking* yang mendapat legitimasi hukum dan mana yang dapat melanggar hukum. Perlu diketahui bahwa perbedaan antara *ethical hacking* dan *unethical hacking* sangat tipis sekali. Sama seperti orang yang terkadang rancu menyebutkan mana *hacker* baik dan *hacker* jahat (*cracker).*

Kegiatan *hacking* memiliki banyak cara, tergantung objek sasaran yang akan dihac*k*. Menurut Stuard McClure, Joel Scambary dan George Kurz sebagaimana dikutip S'to bahwa metode *hacking* dapat ditempuh dalam beberapa langkah,[18] yaitu:

---

[17] *http://www.kompas.com/read/xml/2008/06/13/2004422/merangkul*. diakses 10 oktober 2018.

[18] S'to, *Seni internet Hacking* (Jakarta: Jasakom 2006), hlm. 29.

1. *Footprinting* : Pencarian data calon korban melalui media.
2. *Scanning* : Proses analisa sistem atau software yang akan di*hack.*
3. *Enumeration* : Proses percobaan koneksi ke sistem dan mesin target.
4. *Gaining Access*: jika berhasil pada langkah ketiga di atas maka langkah selanjutnya mengambil alih target.
5. *Escalating Privilege*: jika mesin target sudah dapat diambil alih, berikutnya meningkatnya hak penyerang di mesin target.
6. *Covering Track*: Proses ini dibutuhkan untuk menghapus segala aktivitas penyerang agar tidak bisa terdeteksi.
7. *Creating Back doors*: menciptakan jalan pintas rahasia agar bisa masuk secara lebih mudah ke mesin target, sehingga sewaktu-waktu dapat dimanfaatkan kembali.
8. *Denial of Service*:[19] Proses ini menjadi pilihan dengan menyerang target menggunakan data sehingga target menjadi gagal berfungsi.

Secara teknis cara *hacking* di atas kurang lebih sama dengan yang dipaparkan oleh Tom Thomas sebagai berikut:[20]

1. *Reconaissance* dan *footprinting*
2. *Scanning*
3. *Enumerasi*
4. Mendapatkan akses
5. Membuat *backdoor* dan menyembunyikan jejak.

Proses di atas bukan proses yang harus dilakukan oleh *hacker.* Cara yang digunakan bisa berubah sesuai dengan kondisi dan situasi. Secara teknik metode *hacking* di atas tidak jauh beda penerapannya antara *ethical hacker* dengan

[19]Dony Ariyus, *Kamus Hacker* (Yogyakarta: Andi, 2005), hlm. 106.
[20]Tom Thomas, *Network Security First-Step*,terj.(Yogyakarta: Andi, 2005), hlm.14.

unethical hacker, dan yang membedakan keduanya adalah proses secara keseluruhan yang tidak masuk kategori teknis sebagaimana berikut:[21]

1. Perencanaan serangan
2. Akses ke target
3. Test dan eksekusi serangan
4. Pengumpulan informasi
5. Analisis
6. Diagnosis
7. Laporan akhir

Inilah metode *ethical hacking* yang dilakukan oleh *white hats hacker* sekaligus membedakannya dengan *black hats hacker*, jadi apa yang dilakukan oleh *white hats hacker* selain untuk meningkatkan kemampuan sistem komputer, juga merupakan upaya bertahan atau bagaimana menemukan kelemahan sistem dan program serta memperbaiki kelemahan yang ada agar tidak mudah ditembus oleh serangan hacker yang jahat, sehingga cara berpikir dan metode*hacking* yang mereka gunakan tidak jauh berbeda seperti *hacker* yang jahat. Jika disimpulkan secara umum *ethical hacking* adalah kegiatan yang tunduk pada beberapa aturan :

1. Meng-*hack* sistem bukan untuk merusak
2. Menjaga dengan melindungi data-data penting (privasi), yang diperoleh selama proses *hacking*.
3. Proses *hacking* dilakukan secara terbuka, tidak ada agenda rahasia.

Dalam proses melakukan *hacking* baik bagi *white hats*(*hacker* baik) maupu *black hats*(*hacker* jahat) menggunakan berbagai macam tool atau

[21] Khairul Anam, *Hacking VS Hukum Positif & Hukum Islam* (Yogyakarta: Sunan Kalijaga Press, 2010), hlm. 36.

peralatan mulai dari perencanaan hingga eksekusi. Berikut adalah beberapa contoh alat yang mereka gunakan.[22]

1. *Port Scanner*:[23] berfungsi untuk men-*scanport* komputer target dan mencari port terbuka yang sekiranya dapat digunakan sebagai jalan untuk menyerang. Jika ditemukan port yang terbuka di computer target, akan memudahkan penyerang memasukkan program berbahaya.
2. *Malware*: merupakan suatu perangkat lunak dalam beberapa jenis dengan fungsi yang begitu banyak, *malware* merupakan tool favorit bagi para *hacke.* dengan fungsi yang bermacam-macam seperti mengendalikan komputer dari jarak ribuan kilometer, menyadap aktivitas komputer korban. Contohnya seperti *trojan horses* merupakan tool favorit *hacker* untuk menjebol dan mengendalikan sistem target. Selain *trojan* masih ada alat lain (*malware)* yang sering digunakan oleh *hacker,* misalnya: *Virus, Worms, Rootkits, Spyware, Logic Bombs*, dan aplikasi (software) pengaman seringkali juga digunakan untuk alat *hacking.*
3. Dalam mencari mangsanya *hacker* menggunakan suatu media atau alat yang bervariasi. Bisa berupa software yang familiar atau sering digunakan *user* komputer, contoh, Microsoft Office, Adobe Photoshop dan lain sebagainya. *Tool* yang mereka gunakan berfungsi untuk menyebarkan paket yang sudah berisi *Trojan.*[24]

---

[22] Rahmat Putra, *The Secret of Hacker Mengungkap Cara Kerja Hacker dan melindungi Diri dari Serangan Mereka,* (Jakarta selatan: Mediakita,2007), hlm. 85.

[23]Firrar Utdirartatmo, *Awas Ada Hacker!* (Yogyakarta: Gava Media,2004),hlm.11.

[24]*http://tekno.kompas.com/read/xml/2008/03/24/22062449,* diakses pada 29 oktober 2018.

Cara ataupun metode *hacking* di atas lebih ditujukan untuk membobol sistem komputer yang berupa server, website dan lain-lain. Sedangkan untuk membobol sistem proteksi *software, craker* biasanya akan men-*decompile* untuk mempelajari terlebih dahulu bahasa pemograman dan algoritma software yang akan di *crack.* Sambil mempelajari *craker* akan mencari titik lemah sistem proteksi dari *software* bersangkutan. Bila telah menemukan *hole* dari susunan bahasa program yang digunakan, pada tahap selanjutnya *craker* akan membiarkan software tetap seperti apa adanya (tanpa merubah apapun), memodifikasi atau menulis ulang bahasa pemogramannya. Proses ini akan menghasilkan *patch, crack* dan *keygen* yang digunakan membajak untuk mem-*bypass* proteksi *software* sehingga *user* mampu mengoperasikan perangkat lunak tampa membayar *license.*

C. Macam-macam Tipe *Hacker*

Hacker pada umumnya bisa berbentuk individual bebas dan berbentuk komunitas. Dalam komunitas tersebut ada yang diorganisir secara baik dan ada pula yang tidak memiliki ikatan apapun, dengan kata lain mereka menyatu dalam asas saling tolong menolong dengan menyebarkan pengetahuan mereka di komunitas tersebut.

Media yang digunakan oleh para *hacker* untuk berkomunikasi dan berkonsolidasi bermacam-macam. Bisa dalam bentuk bertemu langsung atau menggunakan internet melalui jejaring sosial (*chat room, mailing list, internet massager*) untuk mereka yang memiliki kendala dalam jarang ratusan ribu kilometer.

Macam-macam komunitas *hacker* terbagi menjadi beberapa golongan biasa disebut *hacker activism* atau *hactivism* ini diklasifikasikan melalui niat dari para *hacker*, cara melakukan *hacking* dan tujuan yang hendak dicapai oleh pelakunya. Mereka yang berkecimpung dalam dunia *hactivism* bisa disebut *hactivist.* Bagi mereka yang memiliki tujuan mulia yaitu menggunakan

kemampuan *hacking* mereka untuk tujuan meningkatkan kemampuan komputer, sistem, software dan lain-lain, biasa disebut *white hats hacker* (*hacker* topi putih). *White hats hacker* bisa juga dijuluki *Ethical hacker, Samurai hacker, Elite hacker.*

Sedangkan mereka yang melakukan *hacking* dengan misi tertentu dan berakibat merusak biasa disebut dengan *black hats hacker*. Sifat utama dari tipe *hacker* ini bisa berupa sabotase, rakus, balas dendam, teror dan lain-lain.[25] Pada golongan ini kelompok-kelompok turunannya menyebarkan banyak musibah dalam dunia teknologi. berikut beberapa varian dari kelompok ini:[26]

1. *Recreational hacker*: *Hacker* tipe ini bisa juga disebut "*Hacker* anak muda." *Hacker* jenis ini biasanya mereka yang sekedar mencoba berkecimpung dalam dunia *hacking*. Mereka lakukan seperti mencoba menembus proteksi suatu sistem dengan pengetahuan yang kurang memadai.
2. *Political Hacker*: *Hacking* tipe ini akan melakukan serangan kepada lawan politik dengan meng-*hack* situs atau menyerang sistem lawan. Kasus ini pernah terjadi antara *hacker* Indonesia dan Malaysia pada saat perseteruan tentang pulau Ambalat. *Hacker* asal kedua negara saling menyerang dengan men-*deface* situs penting dari negara lawan.[27]
3. *Craker*: jika awalnya motivasi *hacker* hanya pada tataran mencari kelemahan suatu sistem komputer dan memperbaikinya maka kini motivasi mereka sudah berbeda. Pada *hacker* jenis ini memiliki ciri-

[25] Khairul Anam, *Hacking VS Hukum Positif & Hukum Islam* (Yogyakarta: Sunan Kalijaga Press,2010),hlm.30.

[26] Sutarwan, *Cyber Crime Modus Operandi dan Penanggulangannya* (Jogjakarta:Laks Bang Pressindo, 2007), hlm. 56.

[27] *https://www.google.com/amp/s/m.liputan6.com/amp/97375/perang-ihackeri indonesia malaysia dinilai-merugikan-situs?espv=1*diakses pada 10 November 2018.

ciri khusus yaitu *hacking* yang dilakukan bertujuan untuk pengrusakan, mendapat keuntungan secara finansial, dan sabotase. Mereka tidak seperti "*kiddie hacker"* tetapi kemampuan yang mereka punya digunakan untuk mendapatkan keuntungan finansial atau untuk membuat mereka terkenal.[28]

4. *Internal Hacker*: merupakan orang yang bekerja pada perusahaan yang dirinya bermasalah dengan perusahaan tersebut dan melakukan *hacking* terhadap sistem perusahaan tersebut karena pelaku sudah paham betul dengan cara kerja sistem di perusahaan tempat dirinya bekerja. Apalagi jika sistem tersebut adalah hasil pekerjaan dirinya.

Dari *hacking* yang dilakukan oleh *black hats hacker* menimbulkan beberapa akibat yang melanggar hukum dan dapat dikatakan sebagai kejahatan, seperti: *deface* (merubah tampilan situs), pembajakan software, pencurian data, pencurian uang, dan lain sebagainya.

D. Unsur-unsur Pidana Kejahatan *Hacking*

Ada tiga bentuk pidana ITE dalam Pasal 30 jo 46 UU ITE sebagaimana dalam Ayat (1), (2) dan (3). Jika Pasal 30 dirumuskan dalam satu naskah dengan Pasal 46, maka rumusan selengkapnya sebagai berikut:

1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun, dipidana penjara paling lama 6 (enam) tahun dan/atau dengan paling banyak Rp 600.000.000, 00 (enam ratus juta rupiah).

2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun

[28] Rahmat Putra, *The Secret of Hacker Mengungkap Cara Kerja Hacker dan melindungi Diri dari Serangan Mereka*,(Jakarta Selatan: Mediakita,2007),hlm.83.

dengan tujuan untuk memperoleh informasi eletronik dan/atau Dokumen Elektronik, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000, 00 (tujuh ratus jura rupiah).

3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan, dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000, 00 (delapan ratus juta rupiah).

1. Tindak Pidana ITE dalam Pasal 30 Ayat (1)

Dalam Pasal 30 ayat (1) terdapat unsur-unsur sebagai berikut ini.

a. Kesalahan: *dengan sengaja;*

b. Melawan hukum: *tanpa hak atau melawan hukum;*

c. Objek: *komputer dan/atau sistem elektronik milik orang lain.*

Dalam hubungannya dengan unsur-unsur lainnya, arti sengaja di sini adalah kehendak untuk mewujudkan tindak pidana tersebut, dan menyadari mengenai unsur-unsurnya. Kesadaran tentang apa yang (hendak) diperbuatnya sebagai dilarang atau menjadi celaan. Keadaan bahwa sistem elektronik yang (akan) diaksesnya adalah milik orang lain.

Mencantumkan frasa "melawan hukum" dalam unsur "tanpa hak atau melawan hukum" terdapat dua keganjilan/kelemahan. Pertama, dirasa sangat berlebihan. Kedua dirumuskan dengan cara yang tidak sempurna.

Dirasa berlebihan, karena frasa "tanpa hak" sesungguhnya sudah cukup. Frasa "melawan hukum" menggambarkan sifat celaan secara umum. Sementara sifat itu dapat digambarkan dengan istilah-istilah yang lebih khusus, misalnya “tanpa hak”, “tanpa izin” atau “menyalahgunakan kewenangan” dan sebagainya, bergantung dari apa sebab apa sifat celaan itu bergantung atau melekat.

Mencantumkan frasa “milik orang lain” saja dalam rumusan tidak cukup. Seharusnya ditambahkan frasa “tanpa izin”. Alasannya karena letak sifat melawan hukumnya perbuatan mengakses, sesungguhnya bukan sekedar terletak pada system elektronik milik orang lain, melainkan justru melekat pada “tidak ada izin” dari pemilik. Seharusnya setelah frasa “milik orang lain” ditambahkan frasa “tanpa izin dari yang berhak”.

Kesalahan ini mengandung akibat hukum yang cukup serius. Semua orang yang melakukan perbuatan mengakses system elektronik milik orang lain akan dicakup oleh rumusan tindak pidana Pasal 30 Ayat (1) Undang-undang ITE. Karena itu dapat dijadikan tersangka dan diajukan ke sidang pengadilan. Meskipun pada akhirnya pengadilan akan melepaskan dari tuntutan hukum (*onslag van alle rechtsvervolging*), apabila terbukti ada izin dari pemilik. Keadaan tanpa izin bukan merupakan unsur tindak pidana, melainkan dasar peniadaan pidana. Terdapatnya “izin dari pemilik”, berfungsi sebagai alasan pembenar yang meniadakan pidana di luar Undang-undang. Merupakan alasan meniadakan sifat melawan hukumnya perbuatan. Hukum pidana Indonesia menganut azas berlakunya sifat melawan hukum materiil dalam fungsinya yang negatif.[29]

[29] Adami Chazawi, *Pelajaran Hukum Pidana 2,* (Jakarta: PT.RajaGrafindo Persada,2005), hlm. 67.

kesalahan pembentuk Undang-undang ITE ini, berdampak pada pekerjaan pembuktian. Agar dapat menuntut penjatuhan pidana pada terdakwa dalam *requisitor,* jaksa tidak cukup membuktikan unsur "milik orang lain" dari system elektronik yang diakses terdakwa. Melainkan juga harus membuktikan kedaan "tanpa izin" si pemilik. Padahal tanpa izin ini bukan merupakan unsur tindak pidana. Melainkan alasan peniadaan pidana di luar Undang-undang, yang sesungguhnya bukan masuk lapangan dan tugas pekerjaan jaksa, melainkan terdakwa atau penasehat hukumnya.

Sifat melawan hukum perbuatan yang sesungguhnya terletak pada tidak ada izin dari si pemilik sistem elektronik yang diakses pembuat. Merupakan sifat melawan hukum objektif. Dalam hubungannya dengan unsur "sengaja", maka bukan miliknya dan tanpa izin si pemilik tersebut, harus disadarinya. Kesadaran terhadap terlarangnya disebabkan bukan miliknya, dan tanpa izin pemiliknya itulah yang disebut melawan hukum subjektif.

Jadi sesungguhnya sifat melawan hukum di sini bercorak dua. Melawan hukum objektif, karena terletak pada keadaan sistem komputer tersebut bukan miliknya dan perbuatan mengakses komputer tersebut tanpa izin pemilik. Sementara melawan hukum subjektif karena keadaan tercelanya perbuatan itu disadari oleh si pembuat. Dua macam bentuk melawan hukum tersebut harus dibuktikan oleh jaksa. Melawan hukum subjektif, harus dibuktikan karena unsur melawan hukum diletakkan sesudah kata sengaja dalam rumusan tindak pidana.

Mengakses adalah isitilah yang sangat popular digunakan dalam bidang ITE. Kata dasar dari mengakses adalah akses, Undang-undang

ITE memberi tafsir otentik tentang akses adalah kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau jaringan.[30]

Sebagai suatu kegiatan, maka akan terdapat banyak cara yang dapat digunakan dalam mengakses. Cara-cara ini tidak dibatasi secara limitative oleh Undang-undang, dengan cara apapun juga, asalkan cara itu dapat berinteraksinya sistem elektronik milik orang lain tersebut.

2. Tindak Pidana dalam Pasal 30 Ayat (2)

Rumusan Pasal 30 Ayat (2) terdiri dari unsur-unsur berikut ini.

a. Kesalahan: *dengan sengaja;*

b. Melawan hukum: *tanpa hak atau melawan hukum;*

c. Perbuatan: *mengakses dengan cara apapun;*

d. Objek: *computer dan/atau sistem elektronik;*

e. *Dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.*

Kalimat yang dicetak miring adalah unsur formal yang membentuk tindak pidana Pasal 30 Ayat (2).

Sesuai dengan petunjuk MvT (Memorie van Toelichting). dalam tindak pidana ini, sengaja adalah kehendak untuk mengakses komputer dan/atau sistem elektronik dengan cara tertentu dengan tujuan untuk memperoleh informasi elektronik. Si pembuat menyadari bahwa perbuatan mengakses dengan cara tertentu untuk memperoleh Informasi Elektronik. Disadari perbuatan itu dapat mencapai tujuan tersebut. Pembuat menyadari bahwa perbuatan tersebut dilarang atau tercela.[31]

Dalam Pasal 30 Ayat (1) yang sebelumnya sudah dibicarakan, bahwa sifat melawan hukum perbuatan mengakses sistem elektronik milik orang lain, letak sifat melawan hukumnya, ialah pada tanpa izin

---

[30] Undang-undang ITE Pasal 1 angka 15.

[31] Adami Chazawi, Ardi Ferdian, *Tindak Pidana Informasi & Transaksi Elektronik Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik* ,hlm. 142.

dari si pemilik. Berbeda dengan letak sifat melawan hukumnya perbuatan dalam rumusan ayat kedua ini. Tidak dengan mudah dicari dimana letak sifat melawan hukumnya perbuatan, sehingga si pembuat patut dibebani pertanggungjawaban pidana dan dipidana.

Rumusan Pasal 30 ayat (2) ini tidak begitu tegas, dan dapat menimbulkan multi tafsir, terutama mengenai sifat melawan hukumnya perbuatan. Mengenai apa yang menyebabkan –larangan mengakses sistem elektronik untuk memperoleh Informasi Elektronik.

Kiranya secara terselubung terdapat kerahasiaan dari informasi elektronik yang menjadi objek tindak pidana pada ayat (2) ini. Hanya orang-orang tertentu dan dengan cara (sistem elektronik) tertentu saja yang boleh untuk memperoleh Informasi Elektronik tersebut. Oleh karena itulah tidak dibenarkan untuk mengakses Informasi Elektronik orang lain. Kiranya tidak logis Undang-undang melarang setiap orang untuk mengakses sistem elektronik untuk memperoleh suatu Informasi Elektronik. Kecuali informasi elektronik tersebut termasuk rahasia, atau Informasi Elektronik tersebut mempunyai nilai ekonomis, yang bisa diperoleh dengan membayar sejumlah uang.

Bisa juga timbul penafsiran, bahwa sifat terlarangnya harus dicari di luar rumusan. Khususnya dapat dicari pada kasus peristiwa yang terjadi. Maksudnya bersifat kasuistis, tidak sama-bergantung dari kasusnya masing-masing. Kiranya inilah alasan pembentuk Undang-undang ITE memberikan contoh-contoh dalam penjelasan ayat kedua tersebut.

Contoh pertama. Melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapapun yang tidak berhak untuk menerimanya. Dalam contoh

tersebut, sifat melawan hukum terdapat atau disebabkan-oleh karena si penerima tidak berhak menerima Informasi Elektronik yang dikirimkan si pembuat.

Contoh kedua. Sengaja menghalang-halangi agar informasi dimaksud tidak dapat atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah. Dalam contoh kedua, sifat melawan hukum justru terletak pada "lingkungan pemerintah atau pemerintah daerah". Logika hukumnya, ialah Informasi Elektronik tersebut memuat segala sesuatu informasi untuk kepentingan umum. Setiap orang tidak diperbolehkan menghalang-halangi atau menggagalkan diterimanya suatu Informasi Elektronik untuk kepentingan umum yang sengaja dikirim ke pemerintah atau pemerintah daerah.

Selain itu bisa juga ditafsirkan, bahwa sifat terlarangnya perbuatan mengakses komputer dan/atau sistem elektronik untuk memperoleh informasi elektronik, karena sistem elektronik tersebut milik orang lain dan tidak ada izin dari yang bersangkutan.

3. Tindak Pidana ITE Pasal 30 Ayat (3)

Norma tindak pidana Pasal 30 ayat (3) terdiri dari unsur-unsur berikut ini.

a. Kesalahan: *dengan sengaja;*
b. Melawan hukum: *tanpa hak atau melawan hukum;*
c. Perbuatan: *mengakses;*
d. Objek: *computer dan atau sistem elektronik;*
e. Caranya: *dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan;*

Kalimat yang dicetak miring merupakan unsur formal yang membentuk norma tindak pidana Pasal 30 ayat (3).

Dalam hubungan unsur sengaja dengan unsur yang diletakkan sesudah kata sengaja, maka sengaja disini harus diartikan kehendak untuk mengakses yang diketahuinya komputer dan/atau sistem elektronik dengan melanggar, melampaui, menerobos atau menjebol sistem pengaman. Si pembuat menyadari perbuatan semacam itu bersifat melawan hukum.

Perbuatan mengakses asal kata akses, yang oleh Pasal 1 angka 15 diberikan arti otentik adalah kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan.

Letak sifat melawan hukumnya perbuatan mengakses kiranya terdapat ada caranya mengakses dengan melanggar, menerobos, melampaui atau menjebol sistem pengaman. Penjelasan ayat (3) menjelaskan tentang arti sistem pengaman, adalah sistem yang membatasi akses komputer atau melarang akses ke dalam komputer dengan berdasarkan kategorisasi atau klarifikasi pengguna beserta tingkatan kewenangan yang ditentukan.

Misalnya sistem pengaman yang dibuat pemilik suatu website, ialah untuk dapat memasuki website tersebut harus menggunakan kombinasi username dan password. Apabila seorang cracker melanggar, menerobos, atau menjebol sistem pengaman tersebut maka terjadilah tindak pidana menurut Pasal 30 Ayat (3) Undang-Undang ITE.

E. *Hacking* dalam Undang-Undang Nomor 11 Tahun 2008 dan KUHP Indonesia

Indonesia merupakan negara hukum yang memiliki dasar hukum dalam menerapkan sebuah aturan, begitu juga dengan tindak pidana *Hacking* yang akan dibahas, dasar hukum yang dapat digunakan untuk menjerat pelaku tindak

pidana *Hacking* adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebelum lahirnya undang-undang Informasi dan Transaksi Elektronik kejahatan *hacking* sudah lebih dulu muncul yang membuat para penyidik cenderung melakukan analogi dalam menjerat pelaku kejahatan *Hacking* dengan dasar hukum KUHP,KUHAP dan ada beberapa undang-undang yang terkait.

Untuk lebih jelasnya penulis akan menjelaskan dasar hukum kejahatan *Hacking* yang terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sebagai undang-undang yang khusus, Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur beberapa pasal mengenai kejahatan *Hacking* (tentang kegiatan *Hacking*, pembuktian, ketentuan pidana, yurisdiksi).

1. Undang-undang Informasi dan Transaksi Elektronik
   a. Dalam Pasal 30 ayat (1) sampai (3) dengan jelas menyatakan bahwa perbuatan mengakses komputer atau sistem elektronik (melalui website, jaringan, internet dan lain-lain) milik orang lain dan dengan tujuan apapun dilarang. Pada pasal ini kegiatan *hacking* dilarang dikarenakan kegiatan yang dilakukan tidak memiliki izin dari pemilik komputer ataupun sistem elektronik tersebut. Kegiatan *hacking* yang dapat dikenai pasal ini adalah menyusup, menjebol sistem. Ketentuan pidana yang diataur pada Pasal 30 ayat (1) sampai (3) ini tertulis dalam Pasal 46 ayat (1) sampai (3).
   b. Dalam Pasal 31 ayat (1) sampai (3) melarang tindakan memata-matai:
      (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukanintersepsi atau penyadapan atas informasi Elektronik dan/atau Dokumen Elektronik dalam suatu komputer dan/atau Sistem elektronik tertentu milik orang lain.
      (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam

suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditrasmisikan.

(3) Ketentuan sebagaimana dimaksud pada ayat (1) dan (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian,kejaksaan, atau institusi lainnya yang kewenagannya ditetapkan berdasarkan undang-undang.

Dalam pasal ini penyadapan hanya diberi kewenangan bagi aparat penegak hukum. Penjelasan pasal ini mengartikan bahwa perusahaan atau lembaga tidak dibenarkan melakukan penyadapan (memata-matai) terhadap komputer atau sistem elektronik karyawannya walaupun memiliki niat yang baik (untuk memonitor kinerja karyawan). Tindak pidana yang dapat dikenai pasal ini adalah kejahatan *hacking* berupa memata-matai. Ketentuan pidana yang dapat dikenakan pada pelaku pelanggaran Pasal 31 ayat (1) dan (2) diatur dalam Pasal 47 yang bunyinya:

" Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah)"

c. Dalam Pasal 32 ayat (1) sampai (3) mengatur masalah penggunaan dokumen elektronik dan memiliki keterkaitan dengan peraturan hak Cipta.

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi

Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal ini dapat menjerat pelaku pembajakan *software,* menyebarkan *password* orang lain dan *cracker* yang membuat atau menyediakan *patch, keygen* atau *crack* tanpa hak dari pengembangnya. Pelaku atau orang yang melanggar pasal ini dikenakan pidana sebagaimana diatur dalam Pasal 48 ayat (1),(2) dan (3).

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).
(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).
(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Peratutan Hak cipta dan Hak pribadi dalan Undang-undang ITE diatur dalam Pasal 25 yang bunyinya:

“Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual berdasarkan ketentuan Peraturan Perundang-undangan”.

Dan juga di atur dalam Pasal 26 ayat (1) dan (2) yang bunyinya

(1) Kecuali ditentukan lain oleh Peraturan Perundangundangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.

(2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Pasal 25 dan 26 tersebut menyatakan bahwa informasi atau dokumen elektronik (bisa berupa *software*, situs internet, data pribadi dan lain sebagainya) dilindungi berdasarkan ketentun peraturan perundang-undangan.

d. Dalam Pasal 33 mengatur permasalahan tentang gangguan suatu sistem elektronik yang disebabkan oleh pihak-pihak tertentu.

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya."

Jadi dalam pasal ini dapat dikenakan untuk pelaku tindak pidana *hacking* dari sudut akibat yang timbul dari ulah pelakunya seperti *defacmen* yang membuat ganguan pada suatu sistem elektronik yang disebabkan oleh pelaku. Bagi pelaku yang melanggar pasal ini ketentuan pidananya diatur dalam Pasal 49.

"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah)."

Dalam Pasal 34 ayat (1) kurang lebih memiliki fungsi yang sama dengan Pasal 32 tapi dengan penjelasan yang lebih eksplisit.

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33; b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi

perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

Dengan penambahan, orang yang menciptakan atau menyediakanalat-alat *hacking* (seperti virus trojan), seperti yang diatur dalam ayat (1) huruf a dapat dikenai pidana. Dalam ayat 1 huruf b memuat larangan pendistribusian *password*, kode akses, atau kode-kode lainnya kepada orang yang tidak berhak. Ketentuan pidana bagi pelanggar pasal ini diatur dalam Pasal 50 yang bunyinya.

"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah)".

e. Kegiatan *hacking* yang melanggar yurisdiksi Negara, seperti *hacker* yang luar negeri yang menyerang target dalam yurisdiksi negara Indonesia atau *hacker* dalam negeri yang menyerang terget di luar negeri atau yurisdiksi negara lain dapat dikenakan Pasal 37.

"Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia."

Dengan ancaman pidana seperti disebutkan dalam Pasal 52 ayat (3).

"Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/ atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masingmasing Pasal ditambah dua pertiga."

f. Dalam aturan dasar pembuktian Undang-undang ITE dapat ditemukan dalam Pasal 5 sampai Pasal 6.

Pasal 5:

(1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
(2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.
(3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam UndangUndang ini.
(4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk: a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan b. surat beserta dokumennya yang menurut UndangUndang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Pasal 6:

"Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan".

Dalam pasal-pasal tersebut secara eksplisit menegaskan bahwa informasi atau dokumen elektronik dapat digunakan sebagai alat bukti hukum yang sah. Jadi suatu dokumen atau informasi elektronik dapat menjadi bukti jika dapat diakses, ditampilkan secara visual, dapat dicetak meskipun bukti tersebut harus dalam bentuk tertulis asli.

g. Alat bukti elektronik bisa juga berupa tanda tangan elektronik yang diatur dalam Pasal 11.

(1) Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:
   a. data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan;
   b. data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan;

c. segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
d. segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;
e. terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatangannya; dan
f. terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

(2) Ketentuan lebih lanjut tentang Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal ini mengatur bahwa tanda tangan elektronik memiliki ketentuan hukum dan akibat hukum yang sah. Dalam penjelasan Pasal 11 ayat (1) menyatakan bahwa tanda tangan elektronik bisa berupa kode tententu (*password*).

2. KUHP dan Undang-undang terkait.

Sebelum lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik para penyidik cenderung melakukan analogi dalam menjerat para pelaku tindak kejahatan Informasi dan Transaksi Elektronik dengan menggunakan KUHP dan Undang-Undang yang terkait berikut penjelasannya:

a. Dalam Pasal 406 KUHP

(1) Barang siapa dengan sengaja dan melawan hukum menghancurkan, merusakan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian milik orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

(2) Dijatuhkan pidana yang sama terhadap orang yang dengan sengaja dan melawan hukum membunuh, merusakkan, membikin tak dapat digunakan atau menghilangkan hewan, yang seluruhnya atau sebagian milik orang lain.

Pelaku (*hacker)* yang menggunakan metode *hacking* dapat dikenakan pasal tersebut. Tindakan *hacking* yang dapat dikenai pasal ini adalah hacking yang memiliki dampak bagi korbannya seperti *deface* (merubah halaman asli dari situs yang di masukinya), yang membuat website atau sistem korban tidak dapat berfungsi sebagaimana mestinya.

Dapat dipahami dari pasal di atas, bagi para pelaku hacking yang hanya sekedar menyusup, mengintai, melihat-lihat, menggunakan komputer korban tanpa menimbulkan kerusakan tidak akan termasuk dalam pasal ini.

b. Pasal 22 Undang-Undang Nomor 36 Tahun 1999 tentang telekomunikasi.

"Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi : a. akses ke jaringan telekomunikasi; dan atau, b. akses ke jasa telekomunikasi ; dan atau, c. akses ke jaringan telekomunikasi khusus."

Pasal ini lebih tegas meyebutkan bahwa kegiatan *hacking* dapat menimbulkan akibat hukum. Pasal ini mengatur bahwa setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi: *pertama*, akses ke jaringan telekominukasi, *kedua*, akses ke jasa telekomunikasi. *Ketiga*, akses ke jaringan telekomunikasi khusus.

Bagi pelaku yang melakukan *hacking* ke suatu sistem komputer tidak sesuai prosedur dengan Pasal 22 ini, akan dikenakan Pasal 50 yang berbunyi:

"Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000.- (enam ratus juta rupiah)".

c. Dalam Undang-Undang Nomor19 Tahun 2002 tentang Hak Cipta. Program komputer adalah sekumpulan intruksi yang diwujudkan dalam

bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut.

Dengan alat-alat yang dibuat oleh para *hacker* atau *cracker*, pengguna dari *software* tidak harus membayar biaya *license* kepada pembuat atau pengembang yang sah dari *software* bersangkutan. Sehingga pengguna suatu aplikasi komputer tersebut dapat menggunakan *software* dengan harga yang murah atau bahkan gratis.

Untuk pelaku *craker* (pembajakan) *software* dapat dikenakan Pasal 72 ayat (3) yang berbunyi:

"Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program komputer dipidana penjara paling lama 5 (lima) tahun penjara dan/atau denda paling banyak Rp. 5000.000.000.- (lima ratus juta rupiah).

d. Alat bukti dalam kasus *hacking*, di dalam Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan diatur tentang pengakuan mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang disimpan di dalamnya). Seperti CD-ROM, yang diatur dalam Pasal 12 yang dapat dijadikan alat bukti sah.

Dalam menyelesaikan perkara menyangkut *hacking* ada beberapa mekanisme yang perlu dijabarkan yaitu, *pertama*, Undang-undang umum atau beberapa Undang-undang khusus lainnya yang digunakan sebelum disahkannya Undang-undang ITE tidak dapat digunakan sebagai alat untuk menjerat pelaku

kejahatan yang menggunakan metode *hacking* dengan catatan Undang-undang bersangkutan bertentangan dengan Undang-undang ITE.

Kedua, jika Undang-undang yang digunakan untuk menjerat pelaku kejahatan yang menggunakan metode *hacking* sebelum disahkannya Undang-undang ITE tidak bertentangan dengan Undang-undang ITE maka Undang-undang yang baru menyingkirkan yang lebih lama atau dengan kata lain Undang-undang ITE harus digunakan untuk menyelesaikan permasalahan. Kedua penjelasan tersebut telah tertulis dalam Pasal 53 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

"Pada saat berlakunya Undang-Undang ini, semua Peraturan Perundang-undangan dan kelembagaan yang berhubungan dengan pemanfaatan Teknologi Informasi yang tidak bertentangan dengan Undang-Undang ini dinyatakan tetap berlaku."

Sehingga dapat ditarik kesimpulan bahwa Undang-undang ITE tetap menjadi acuan utama dalam menyelesaikan perkata yang menyangkut informasi dan transaksi elektronik. Beberapa Undang-undang yang digunakan sebelum adanya Undang-undang ITE tetap dapat digunakan selama Undang-undang ITE tidak mengatur permasalahan yang timbul dalam perkara penerapan informasi dan transaksi elektronik.

Dengan demikian akan lebih membatasi gerak para pelaku kejahatan informasi dan transaksi elektronik untuk mencari kelemahan dari Undang-Undang yang menjerat pelaku tindak pidanan informasi dan transaksi elektronik.

Dan juga untuk menciptakan rasa aman dan melindungi para pengguna *Cyberspace* dari pelaku *Hacking* yang dapat meretas informasi dan data pribadi.

BAB TIGA
KAJIAN PUTUSAN PENGADILAN NEGERI JEMBER NOMOR 253/Pid B/2013/PN JR

A. *Hacking* dalam Hukum Islam

Hukum Islam sebagai hukum yang memiliki aspek teologis dan bersifat provan tentunya memiliki fleksibilitas dalam menghadapi realitas sosial yang ada. Beberapa tahun terakhir, Islam menunjukkan keterhubungannya dengan dunia teknologi informasi, namun yang nampak dipermukaan, teknologi informasi (komputer dan internet) lebih cenderung digunakan motif kejahatan oleh orang yang mengaku dirinya sebagai muslim.

Islam sebagai agama samawi telah mengatur masalah hak-hak (agama, hidup, ilmu/akal, keturunan dan harta) yang harus dilindungi untuk setiap insan. Kegiatan *hacking* dikategorikan sebagai objek hukum (*mahkum fih*) yang memiliki konsekuensi hukum. Sebelum lebih jauh mengeluarkan pendapat atau dalil mengenai *hacking*. Tentunya perlu di klarifikasikan terlebih dahulu cara/proses dan akibat dari *hacking*.

Secara garis besar *hacking* dapat dibagi dua pengertian yaitu : pertama, *hacking* merupakan cara atau proses memperbaiki, mencari kelemahan, mengakses komputer atau suatu sistem komputer/ elektronik (internet, intranet, bluetooth dan lain sebagainya). Kedua, *hacking* bisa berupa proses akses kesuatu program atau proses menggunakan aplikasi komputer (*software*). Dari kedua pemahaman tersebut dapat disimpulakn bahwa proses *hacking* yang tidak melalui cara atau prosedur yang sah (seperti yang diterapkan oleh *white hats hacker* sebagaimana telah dijelaskan pada bab dua) atau merugikan pihak lain tentunya akan menimbulkan persoalan baru yang dapat mengganggu hak orang lain seperti:

1. Penyusupan/pelanggaran privasi:[32] menjebol sistem sehinnga pelaku mampu melihat atau metai-matai isi komputer target (*e-spionage*) menggunakan komputer korban untuk menyerang target dll.
2. Pencurian: pencurian file, *password*, nomor kartu kredit dan lain-lain yang merupakan info/data digital.
3. Pengrusakan: yang menyebabkan komputer korban tidak berjalan sebagaimana mestinya.
4. Pelanggaran perjanjian: setiap program komputer (software,sistem operasi) dipastikan memiliki EULA (*end user license agreement*). Dari EULA tersebut akan diketahui apakah software bersifat *freeware, shareware,trial* dan lain-lain. *Black had hacker* dengan tindakan membuat *patch, keygen* atau *crack* dan menyebarkan melalui situs-situs seperti wares-site bisa disebut melanggar perjanjian penggunakan yang diatur oleh pengembang atau pemilik software bersangkutan.
5. Pelanggaran amanat *internal hacker* atau *insider hacker* masuk dalam kategori ini. Apa yang dilakukan oleh *insider hacker*kurang lebih sama dengan *hacker* lainnya, tapi memiliki perbedaan yaitu *internal hacker* telah melanggar amanat yanng telah dilimpahkan perusahaan atau lembaga dia pernah bekerja, yaitu melindungi perusahaan.

Dalam mengambil *adillah* atau dalil-dalil untuk dijadikan dasar hukum dalam penelitian ini, penulis menggunakan pendekatan kontekstual dalil-dalil (Al-Qur'an, hadis, pendapat ulama) yang ada, dengan artian pendekatan konstektual, penyusup mencoba untuk men-*qiyas*kan[33] kajadian yang terjadi dalam dalil dengan fenomena yang terjadi dalam

[32]Khairul Anam, *Hacking VS Hukum Positif & Hukum Islam* (Yogyakarta: Sunan Kalijaga Press,2010), hlm.35.

[33]Nasrun Haroen, *Ushul FiqihI* (Ciputat: Logos Publishing House,1996), hlm.62.

permasalahan *hacking*. Sebab, jika dalil-dalil yang ada tidak diqiaskan atau diterjemahkan secara tekstual maka yang terjadi objek (kejadian, tindakan) dalam dalil bersangkutan akan berbeda secara lahiriyah dengan pembahasan dan objek kajian penelitian ini.

Kegiatan *hacking* dengan segala proses dan akibatnya dapat dikategorikan dalam kategori berat dan sedang. Hal tersebut didasarkan pada pengkategorian *jarimah* dalam *fiqih jinayah*. Dalam pembahasan ini penyusun tidak akan membahas aspek hukuman yang ditimpakan dari perbuatan dan akibat yang ditimbulkan kejahatan menggunakan *hacking*, tapi penyusun lebih mengedepankan mengeluarkan dalil-dalil yang dapat dijadikan acuan/dasar hukum saat menghadapi permasalahan *hacking*. Berikut ini penjabarannya:

1. Untuk kasus pertama, misal penyusupan (masuk secara diam-diam atau secara sembunyi-sembunyi tanpa sepengetahuan dan seizin dari pemilik barang). Segala perbuatan di atas yang melibatkan objek dan subjek yang jelas telah memiliki hukum dasarnya dalam nash sebagaimana al-Qur'an telah melarang sebagaimana termaktub berikut :

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَدۡخُلُواْ بُيُوتًا غَيۡرَ بُيُوتِكُمۡ حَتَّىٰ تَسۡتَأۡنِسُواْ وَتُسَلِّمُواْ عَلَىٰٓ أَهۡلِهَاۚ ذَٰلِكُمۡ خَيۡرٞ لَّكُمۡ لَعَلَّكُمۡ تَذَكَّرُونَ ٢٧

Hai orang-orang yang beriman, janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat.(An-nur:27).

Perbuatan yang dilarang oleh ayat di atas masuk dalam kategori *jarimah ta'zir* yang berkaitan dengan pelanggaran

kemaslahatan individu, seperti mengganggu hak milik orang lain.[34] Selain ayat di atas, al-Qur'an juga melarang perbuatan memasuki tempat orang lain apalagi memata-matai (spionase) isi dari tempat yang dimasuki.

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱجۡتَنِبُواْ كَثِيرٗا مِّنَ ٱلظَّنِّ إِنَّ بَعۡضَ ٱلظَّنِّ إِثۡمٞۖ وَلَا تَجَسَّسُواْ وَلَا يَغۡتَب بَّعۡضُكُم بَعۡضًاۚ أَيُحِبُّ أَحَدُكُمۡ أَن يَأۡكُلَ لَحۡمَ أَخِيهِ مَيۡتٗا فَكَرِهۡتُمُوهُۚ وَٱتَّقُواْ ٱللَّهَۚ إِنَّ ٱللَّهَ تَوَّابٞ رَّحِيمٞ ١٢

Hai orang-orang yang beriman, jauhilah kebanyakanpurba-sangka (kecurigaan), karena sebagiandaripurba-sangka itu dosa. Dan janganlah mencari-cari keburukan orang dan janganlah menggunjingkan satu sama lain. Adakah seorang diantara kamu yang suka memakan daging saudaranya yang sudahmati? Maka tentulah kamu merasa jijik kepadanya. Dan bertakwalah kepada Allah. Sesungguhnya Allah MahaPenerima taubat lagi Maha Penyayang. (Al-hujurat:12)

Dalam kasus menyusup, menjebol sistem komputer dan e-spionage sehingga pelaku mampu masuk, melihat, dan menjadikan sistem komputer korban untuk melakukan perbuatan yang tidak dikehendaki yang hak belum memiliki dasar hukum dalam hukum islam, namun jika melihat larang yang ada dan cara yang dilakukan oleh pelaku sama dengan yang dijabarkan oleh beberapa dalil di atas. Oleh karenanya kegiatan tersebut termasuk dilarang menurut hukum Islam.

[34] H.A Jazuli, *Fiqih Jinayah Upaya Menanggulangi Kejahatan dalam Islam*,(Jakarta:PT. Raja Grafindo,1997), hlm. 128.

Sebab komputer dan sistem yang melingkupi adalah properti yang tidak boleh sembarang orang melanggar hak pemiliknya. Menyusup, sekedar melihat-lihat dan memata-matai isi komputer korban, secara kontekstual dikandung dan diatur oleh dalil-dalil tersebut (bersifat sama). Isi komputer yang berupa data atau apapun itu tentunya ada yang berbentuk file/data privasi (bisa berupa: bank, lembaga pemerintahan, atau bahkan individu) yang pemiliknya tidak ingin orang lain atau orang yang tidak berhak mengetahuinya.

Hacker yang mampu menyusup dan menjebol komputer korbannya, biasanya disertai niat tertentu, di antaranya menggunakannya untuk menyerang target utama. Dari penjabaran di atas dapat ditarik sebuah kaidah *fiqhiyyah* sebagai dasar hukum untuk menyusup, yaitu tidak dibolehkan bagi seseorang bertindak atas milik otang tanpa seizinnya.[35]

لايخوز لاحدانيتصرففيملكالغيربلااذنة

Tidak dibenarkan seseorang mendistribusikan milik orang lain tanpa adanya pemberian otoritas dari pemiliknya.

2. Pencurian (s*ariqah*) dalam Islam termasuk dalam kejahatan kategori berat, *jarimah hudud*. *Sariqah* memiliki arti mengambil harta (*mal*) orang lain dengan sembunyi-sembunyi atau diam-diam[36]. Dalam penelitian ini yang dimaksud mal (harta) di atas bukan hanya uang (nuqud), jadi harta di sini bisa dimaknai berupa hak milik, properti atau barang, barang bisa berupa data, data bisa berupa data keras (kertas, surat-surat penting dalam

[35] Asjmuni A. Rahman, *Qaidah-Qaidah fiqih* (Jakarta: Bulan Bintang, 1976), hlm. 140.
[36] M. Nurul Irfan, Masyrofah, *Fiqih Jinayah*,(Jakarta: Amzah, 2015), hlm. 99-100.

bentuk cetakan) atau data lunak (file) seperti data dalam komputer.

Hacker yang meng-hack sistem komputer atau elektronik tentunya memiliki tujuan dari tujuan yang paling mulia hingga paling buruk. Salah satu dampak buruk yang ditimbulkan oleh para *black at hacker* adalah berupa pencurian data (*password*, file/data penting dan lain sebagainya).

Kasus pencurian dalam permasalahan ini cara dan objek (komputer, internet, dan data) pada beberapa hal berbeda, tentunya belum ada dalam hukum Islam yang mengatur hal ini. Namun dalam hukum islam ada dalil yang menyinggung tentang pencurian seperti dalam Al-Quran sebagai berikut.

وَٱلسَّارِقُ وَٱلسَّارِقَةُ فَٱقْطَعُوٓاْ أَيْدِيَهُمَا جَزَآءًۢ بِمَا كَسَبَا نَكَٰلًا مِّنَ ٱللَّهِ ۗ وَٱللَّهُ عَزِيزٌ حَكِيمٌ ﴿٣٨﴾

Laki-laki yang mencuri dan perempuan yang mencuri, potonglah tangan keduanya (sebagai) pembalasan bagi apa yang mereka kerjakan dan sebagai siksaan dari Allah. dan Allah Maha Perkasa lagi Maha Bijaksana.(Al-maidah:38)

Namun demikian, dilihat dari segala aspek, proses pencurian yang menggunakan perangkat teknologi komunikasi informasi ini tetap dikategorikan perbuatan terlarang, dengan alasan pencurian ini menjadi dilarang karena memiliki sifat yang sama dengan proses atau sifat barang yang menjadi syarat dari dalil di atas.

3. Dari dulu hingga sekarang manusia suka berbuat kerusakan dalam segala bidang seperti berperang yang menimbulkan kehancuran dalam bentuk fisik dan non-fisik, merusak

lingkungan dan lain sebagainya yang terus berlanjut hingga kini, yang tentunya kerusakan itu sendiri memberikan kerugian yang tidak sedikit dari sisi materil dan immateril. Tingkah laku manusia yang cenderung merusak ini telah memiliki dasar hukum pelanggarannya dan diancam sebagaimana allah berfirman:

هُوَ ٱلَّذِى خَلَقَ لَكُم مَّا فِى ٱلۡأَرۡضِ جَمِيعًا ثُمَّ ٱسۡتَوَىٰٓ إِلَى ٱلسَّمَآءِ فَسَوَّىٰهُنَّ سَبۡعَ سَمَٰوَٰتٍۚ وَهُوَ بِكُلِّ شَىۡءٍ عَلِيمٌ ﴿٢٩﴾ وَإِذۡ قَالَ رَبُّكَ لِلۡمَلَٰٓئِكَةِ إِنِّى جَاعِلٌ فِى ٱلۡأَرۡضِ خَلِيفَةً‌ۖ قَالُوٓاْ أَتَجۡعَلُ فِيهَا مَن يُفۡسِدُ فِيهَا وَيَسۡفِكُ ٱلدِّمَآءَ وَنَحۡنُ نُسَبِّحُ بِحَمۡدِكَ وَنُقَدِّسُ لَكَ‌ۖ قَالَ إِنِّىٓ أَعۡلَمُ مَا لَا تَعۡلَمُونَ ﴿٣٠﴾

Dia-lah Allah, yang menjadikan segala yang ada di bumi untuk kamudan Dia berkehendak (menciptakan) langit, lalu dijadikan-Nya tujuh langit. Dan Dia Maha mengetahui segala sesuatu. Ingatlah ketika Tuhanmu berfirman kepada Para Malaikat: "Sesungguhnya aku hendak menjadikan seorang khalifah di muka bumi." mereka berkata: "Mengapa Engkau hendak menjadikan (khalifah) di bumi itu orang yang akan membuat kerusakan padanya dan menumpahkan darah, Padahal Kami Senantiasa bertasbih dengan memuji Engkau dan mensucikan Engkau?" Tuhan berfirman: "Sesungguhnya aku mengetahui apa yang tidak kamu ketahui."(al-baqarah:29-30)

إِنَّمَا جَزَٰٓؤُاْ ٱلَّذِينَ يُحَارِبُونَ ٱللَّهَ وَرَسُولَهُۥ وَيَسۡعَوۡنَ فِى ٱلۡأَرۡضِ فَسَادًا أَن يُقَتَّلُوٓاْ أَوۡ يُصَلَّبُوٓاْ أَوۡ تُقَطَّعَ أَيۡدِيهِمۡ وَأَرۡجُلُهُم مِّنۡ خِلَٰفٍ

أَوۡ يُنفَوۡاْ مِنَ ٱلۡأَرۡضِۚ ذَٰلِكَ لَهُمۡ خِزۡيٞ فِي ٱلدُّنۡيَاۖ وَلَهُمۡ فِي ٱلۡأٓخِرَةِ عَذَابٌ عَظِيمٌ ٣٣

Sesungguhnya pembalasan terhadap orang-orang yang memerangi Allah dan Rasul-Nya dan membuat kerusakan di muka bumi, hanyalah mereka dibunuh atau disalib, atau dipotong tangan dan kaki mereka dengan bertimbal balik, atau dibuang dari negeri (tempat kediamannya). Yang demikian itu (sebagai) suatu penghinaan untuk mereka didunia, dan di akhirat mereka peroleh siksaan yang besar,(Al-maidah:33)

Munculnya teknologi informasi tidak luput juga dari upaya pengrusakan yang berakibat fatar bagi kemaslahatan hidup orang-orang banyak. Dasar hukum Islam atas *Hacking* yang merusak belum didapatkan disebabkan dalil yang ada tidak secara eksplisit menyebut perbuatan merusak pada sistem elektronik dan komputer. Padahal akibat yang ditimbulkan kurang lebih sama dengan jenis pengrusakan sebagaimana terkandung dalam nash di atas. Oleh sebab itu, hukum dasar untuk perbuatan merusak dengan metode *Hacking* dapat dikenakan hukuman yang sama dengan dalil di atas. Sebab, kerugian yang ditimbulkan oleh aktivitas (defacemen, accesfload, dan Dos) ini tidak bisa dibilang kecil. Dapat kita bayangkan, seandainya situs milik bank diserang oleh *black hat hacker* dengan ketiga metode di atas, berapa ribu nasabah yang akan dirugikan dan berapa kerugian yang akan dialami oleh bank bersangkutan.

Dari penjelasan sebelumnya, bisa ditarik sebuah kaidaf *fiqhiyyah*, yaitu, walaupun kegiatan *hacking* memiliki maslahat tapi lebih dianjurkan tidak menerapkannya (meniggalkannya) jika

mengakibatkan kerusakan (ini sesuai dengan prinsip *ethical hacking* bahwa *hacking* bukan untuk merusak) seperti disebutkan kaidah berikut:[37]

درئ المفاسد مقدم على خلب المصالح

Menolak mafsadah (kerusakan) didahulukan daripada mengambil kemaslahatan.

4. Pembahasan seputar perjanjian (‘aqd) dalam hukum Islam memiliki bidangnya sendiri, yaitu fiqih mu’amalah. Perjanjian secara etimologi adalah mu’ahada ittifa’ (‘aqd). Definisinya adalah perjanjian atau persetujuan adalah suatu perbuatan di mana seorang atau lebih mengikatkan dirinya terhadap seseorang lain atau lebih.[38] Artinya suatu perjanjian akan terjadi jika yang ditawari janji menerima dari sipenawar. Namun pada dasarnya hukum pokok suatu perjanjian adalah kerelaan atas akad yang dijalani oleh kedua belah pihak.[39]

Menurut hukum barat, lahirnya perjanjian melalui 4 teori, teori pertama (uiting theorie, theorie de la declaration), menyatakan bahwa perjanjian jarak jauh yang mana si pembuat janji membuat perjanjian secara tertulis dan bila pihak kedua menyatakan akseptadinya terhadap isi perjanjian tersebut, maka perjanjian terjadi antara keduanya.[40] Teori perjanjian ini sering digunakan dalam transaksi cepat dan praktis, contohnya dalam pendistribusian software yang mana perjanjian disertakan dalam

[37] Asjmuni A.Rahman, *Qaidah-Qaidah Fiqih*(Jakarta: Bulan Bintang, 1976), hlm.29.

[38] Chairuman Pasaribu, Suhrawadi k. Lubis, *Hukum Perjanjian dalam Islam*, cet. 3, (Jakarta: Sinar Grafika, 2004), hlm. 1.

[39] Asjmuni A.Rahman, *Qaidah-Qaidah Fiqih*(Jakarta: Bulan Bintang, 1976), hlm. 44.

[40] Syamsul Anwar, *Hukum Perjanjian Syari’ah*: Studi *tentang Teori Akad dalam Fiqih Muamalat*, (Jakarta: Raja Grafindo Persada, 2007), hlm.155.

proses instalasi dan dipastikan user yang akan mengistall aplikasi bersangkutan membacanya.

Al-Quran mengatur hukum perjanjian seperti termaktub dalam ayat-ayat berikut.

وَإِن نَّكَثُوٓاْ أَيۡمَٰنَهُم مِّنۢ بَعۡدِ عَهۡدِهِمۡ وَطَعَنُواْ فِي دِينِكُمۡ فَقَٰتِلُوٓاْ أَئِمَّةَ ٱلۡكُفۡرِ إِنَّهُمۡ لَآ أَيۡمَٰنَ لَهُمۡ لَعَلَّهُمۡ يَنتَهُونَ ١٢ أَلَا تُقَٰتِلُونَ قَوۡمٗا نَّكَثُوٓاْ أَيۡمَٰنَهُمۡ وَهَمُّواْ بِإِخۡرَاجِ ٱلرَّسُولِ وَهُم بَدَءُوكُمۡ أَوَّلَ مَرَّةٍۚ أَتَخۡشَوۡنَهُمۡۚ فَٱللَّهُ أَحَقُّ أَن تَخۡشَوۡهُ إِن كُنتُم مُّؤۡمِنِينَ ١٣

Jika mereka merusak sumpah (janji)nya sesudah mereka berjanji, dan mereka mencerca agamamu, Maka perangilah pemimpin-pemimpin orang-orang kafir itu, karena Sesungguhnya mereka itu adalah orang-orang (yang tidak dapat dipegang) janjinya, agar supaya mereka berhenti. Mengapakah kamu tidak memerangi orang-orang yang merusak sumpah (janjinya), Padahal mereka telah keras kemauannya untuk mengusir Rasul dan merekalah yang pertama mulai memerangi kamu?. Mengapakah kamu takut kepada mereka Padahal Allah-lah yang berhak untuk kamutakuti, jika kamu benar-benar orang yang beriman.(At-taubah:12-13)

Kasus *craker*, dalam modus operandinya menggunakan bermacam aplikasi tertentu untuk menjebol sistem pengamanan suatu *software* agar dapat dimanfaatkan secara bebas, tanpa membayar biaya *license*. Padahal, setiap pengembang *software* telat mengikat penggunakanya dalam sebuah bentuk perjanjian pemakaian *software* yang mereka rilis. Dalam perjanjian tersebut biasanya ditentukan bahwa *software* tersebut bersifat gratis, *shareware* (dapat mencoba beberapa hari dengan atau tanpa

pembatasan dalam fitur, setelah itu dikenakan biaya pemakaian), atau *public domain software*.

Permasalahannya, banyak dari *cracker* dengan penguasaan bahasa pemograman yang mumpuni mampu menjebol pengamanan dari suatu *software*, lebih miris lagi mereka membuat *patch, keygen* dan *crack* dan menjualnya untuk keuntungan sendiri. Perbuatan tersebut, mempunyai unsur kesengajaan pengabaian perjanjian dari pengembang *software* yang mereka *crack*. Selain itu *user* lain yang menggunakan jasa mereka (*cracker*) secara langsung juga mengabaikan perjanjian penggunaan *software* tersebut.

Oleh karenanya *cracker* dengan karyanya berupa *crack*, *patch, keygen*, merupakan suatu bentuk upaya merusak perjanjian. Begitu pula dengan pengguna, pengelola, penyedia barang bajakan masuk dalam kategori perusakan perjanjian. Sifat aktivitas *cracker* ini sama dengan apa yang dilarang oeh dalil-dalil di atas, yang menyebabkan segala aktivitas dari hulu ke hilir atas ulah *cracker* termasuk perbuatan yang dilarang oleh syara'.

5. Orang yang bekerja dalam suatu lembaga, tentunya akan mendapatkan sebuah amanat tertentu, amanat tersebut ada yang bersifat rahasia atau tidak. Selama bekerja dan setelah berhenti, amanat tetap menjadi tanggung jawab bersangkutan untuk tidak menyebarkan pada orang lain atau mengunakan pengetahuan yang didapat selama bekerja digunakan untuk menghancurkan lembaga di mana ia bekerja.

Dalam alquran juga menyinggung orang-orang yang suka melanggar amanat yang diembannya seperti termaktub dalam ayat berikut:

يَـٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَـٰنَـٰتِكُمۡ وَأَنتُمۡ تَعۡلَمُونَ ٢٧

Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui. (Al-anfal: 27)

Dalam kasus *insider hacker* ada upaya kesengajaan untuk mengkhianati amanat. Ada berbagai cara yang bisa ditempuh *insider hacker*, dan pastinya pengetahuan mereka akan rahasia-rahasia lembaga/institusi di mana mereka bekerja merupakan senjata utama operasi mereka. Jika pada kenyataannya *insider hacker* melakukan hal yang dapat merugikan tempat di mana ia bekerja, maka dapat diambil kesimpulan bahwa bersangkutan telah melakukan pelanggaran amanat lembaga atau institusi tempat iya (atau pernah) bekerja. Sehingga apa yang dilakukan oleh mereka telah memenuhi syarat pelanggaran dari dalil-dalil.

B. Kronologi Putusan Pengadilan Negeri Jember Nomor 253/Pid B/2013/PN JR

Dalam putusan pengadilan negeri Jember nomor 253/Pid B/2013/PN JR yang menjadi terdakwa adalah saudara Wildan Yani Ashari Alias Yayan Alias MJL 007, tanggal lahir 18 Juni 1992 berkebangsaan Indonesia, tempat tinggal Dusun Krajan Rt.001 Rw.007, Desa Balung Lor, Kecamatan Balung, Kabupaten Jember, terdakwa di tahan pada hari dan tanggal 26 Januari 2013 sampai dengan tanggal 14 Februari 2013 terdakwa ditahan karena melakukan perbuatan tanpa hak, tidak sah atau memanipulasi akses ke jasa telekomunikasi.

Terdakwa melakukannya dengan cara meretas server my.Techscape.co.id dan membuat akun secara ilegal pada webhosting www.jatirejanetwork.com dengan menggunakan komputer billing Warnet Surya Com milik CV. Surya Infotama, sedangkan posisi terdakwa sebagai operator billing warnet tersebut, terdakwa menggunakan software atau tools berupa scrit khusus yang berbasiskan bahasa pemrogaman PHP dan terdakwa menggunakan nickname MJL007 terhadap website www.jatirejanetwork.com dengan menggunakan ip 210.247.249.58. tak berhenti di situ, terdakwa sadara Wildan Yani Ashari juga melakukan peretasan terhadap website www.presidensby.info dengan cara mencari DNS server dari domain presidensby.info melalui login ke akun techscape dengan password : "tsc800puri" tanpa seijin CV. Techscape dan juga untuk mengakses website www.jatirejanetwork.com agar dapat mengganti DNS presidensby.info.

Laman www.jatirejanetwork.com yang dikelola Eman Sulaiman bergerak di bidang jasa pelayanan domain hosting. Wildan Yani Ashari alias Yayan mencari celah keamanan di laman itu. Kemudian melakukan SQL Injection atau Injeksi SQL, teknologi yang biasa digunakan para peretas atau hacker agar bisa mendapatkan akses ke basis data di dalam sistem.

Wildan Yani Ashari lantas menanamkan backdoor berupa tools (software) berbasiskan bahasa pemrograman PHP yang bernama wso.php (web sell by orb). Dalam dunia teknologi informasi dan komunikasi, dengan mekanisme backdoor yag ditanamkannya, hacker bisa melakukan compromise, yakni melakukan bypass atau menerobos sistem keamanan komputer yang diserang tanpa diketahui oleh pemiliknya.

Wildan pun mengutak-atik lamanwww.techscape.co.id yang memiliki ip 202.155.61.121 dan menemukan celah keamanan. Wildan berhasil meretas

server yang dikelola CV.Techscape itu dan memasuki aplikasi WebHost Manager Complete Solution (WHMCS) pada direktori my.techscape.co.id

Pada November 2012 Wildan mulai mengakses laman www.jatirejanetwork.com yang telah awal diretasnya. Menjalankan aplikasi backdoor yang telah lebih dulu dia tanam sebelumnya, wildan menggunakan perintah Command linux: cat/home/tech/www/my/configuration/.php, hingga akhirnya berhasil mendapatkan username dan kata kunci dari basis data WHMCS yang dikelola CV.Techschape.

Setelah itu Wildan menjalankan program WHMKiller dari laman www.jatirejanetwork.com untuk mendapat username dan kata kunci dari setiap domain dengan username:root,dan password: b4p4kg4nt3ngTIGA dengan port number: 2086.

Dengan username dan kata kunci tersebut, Wildan lantas menanamkan pula backdoor di server www.techscape.co.id, pada pukul 04.58.31 WIB pada 16 November 2012, agar beackdoor tersebut tidak diketahui admin Wildan merubah nama tools menjadi domain.php dan ditempatkan pada subdirectori my.techscape.co.id/id/feeds/, sehingga Wildan bisa leluasa mengakses server www.techscape.com melalui URL: my.techscape.co.id/feeds/domain.php

Kemudian pada 8 Januari 2013 Wildan mengakses laman www.enom.com, sebuah laman yang merupakan domain registrar www.techscape.co.id, hingga berhasil melakukan login ke akun techscape di domain registrar eNom.Inc yang bermarkas di Amerika Serikat. Dari situlah Wildan mendapatkan informasi tentang Domain Name Server (DNS) lama www.presidensby.info.

Setidaknya ada empat informasi penting berupa data Administrative Domain/Nameserver yang dia dapatkan dari laman pribadi Presiden SBY itu, yakni :

Sahi7879.earth.orderbox-dns.com,

Sahi7879.mars.orderbox-dns.com,

Sahi7879.venus.orderbox-dns.com,

Sahi7879.mercuri.orderbox-dns.com.

Wildan lantas mengubah keempat data tersebut menjadi id1.jatirejanetwork.com dan id2.jatirejanetwork.com. selanjutnya pada 22.45 WIB, Wildan menggunakan akun tersebut (lewat WHMjatirejanetwork) sehingga dapat membuat akun domain www.presidensby.info dan menempatkan sebuah file HTML Jember Hacker Team pada server www.jaterjahost.com.

Dan akibat perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada jam 22.45 wib melakukan pembuatan akun domain presidensby.info diserver pihak perusahaan webhosting jatirejahost.com dan menempatkan sebuah file HTML "Jember Hacker Team" di server jatirejahost.com, sehingga ketika para pengguna internet ingin mengakses website presidensby.info yang sebenarnya, akan tetapi konten yang terakses pada pengguna internet adalah tampilan file HTML "Jember Hacker Team" yang pada awalnya tampilan pada website presidensby.info adalah gambar Presiden SBY dan juga Istana, bendera merah putih dan garuda tetapi malah berubah tampilannya menjadi warna hitam dan bertuliskan "Jember Hacker Team".

Perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dijatuhi hukuman oleh hakim sebagai berikut:

1. Menyatakan bahwa terdakwa Wildan Yani Ashari alias Yayan Alias MJL007 telah terbukti secara sah meyakinkan bersalah melakukan tindak pidana dengan sengaja dan tanpa hak melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun;
2. Menjatuhkan pidana terhadap terdakwa oleh karena itu dengan pidana penjara selama 6 (enam) bulan dan denda sebesar Rp. 250 000,- (dua ratus lima puluh ribu subsidair 15 hari kurungan;
3. Menetapkan bahwa masa penahanan yang telah dijalani oleh terdakwa dikurangkan seluruhnya dan pidana yang dijatuhkan
4. Memerintahkan agar terdakwa tetap berada dalam tahanan;
5. Menetapkan barang bukti berupa; 1 (satu) Unit CPU merk Simbada warna abu-abu kapasitas 1 TB 1 (satu) unit CPU merk Power Case warna merah hitam kapasitas 80 GB dikembalikan kepada yang berhak yaitu Warnet CV.Surya Infotama. 1 (satu) KTP atas nama Wildan Yani Ashari dikembalikan kepada terdakwa. 1 (satu) keping Compact disc (CD) berisi file domain PHP pada server techscape, 1 (satu) keping media cakram DVD berisi file akses*IP address* 180.247.245.185 pada *server* Alvin development.com dirampas untuk dimusnahkan;
6. Membebankan biaya perkara kepada terdakwa sebesar Rp. 5.000,- (lima ribu rupiah);

C. KAJIAN UNSUR PIDANA HACKING DALAM PUTUSAN PENGADILAN NEGERI JEMBER DITINJAU MENURUT HUKUM ISLAM

Salah satu yang perlu digarisbawahi dari aktivitas dalam *hacking* yaitu kompleks. [41] karena dari sekian kejahatan dunia maya atau *cybercrime* hampir

[41]http://*cetak*.kompas.com/read/xml/2008/04/17/02300074, diakses pada tanggal 01 Maret 2020.

tidak luput dari metode *hacking*. Beberapa Undang-undang terkait yang digunakan sebelum diberlakukannya Undang-undang tentang Informasi dan Transaksi Elektronik saat ini tetap digunakan sebagai pelengkap untuk menanggulangi kejahatan dunia maya yang menggunakan metode *hacking*. Karena bagaimanapun Undang-undang tentang Informasi dan Transaksi Elektronik yang masih memiliki beberapa celah yang tetap perlu diperbaiki.

Salah satu aktivitas *hacking* yang sering diperdebatkan adalah penyusupan untuk tujuan tertentu dalam suatu sistem teknologi informasi. Perlu digarisbawahi aspek terpenting dalam pembahasan *hacking* di sini adalah penyusupan yang berupa percobaan menjebol, menerobos melampaui sistem proteksi dari suatu sistem atau *software*. Sebab dengan berhasilnya seseorang menyusup dan menjebol proteksi sistem atau *software* maka akan terbuka lebar peluang untuk melakukan kejahatan seperti pencurian data penting, password, nomor kartu kredit atau sengan lain yang berupa *deface* dan lain sebagainya.

Undang-undang tentang Informasi dan Transaksi Elektronik mengatur hal tersebut dalam Pasal 30 ayat 1 sampai 3, yang dengan tegas melarang penyusupan (mengakses sistem atau software orang lain) dalam bentuk apapun kecuali dengan izin dari sang pemilik. Dalam pasal tersebut terdapat kata "melawan hukum" yang mengandung berbagai pertanyaan dan sering diperdebatkan.

Sebagai contoh permasalahan, untuk mencari kelemahan sistem (*bug* atau *hole*), *programmer* atau *admin* suatu jaringan komputer skala kecil akan menerapkan metode *hacking* dengan mencoba menyusup untuk menguji keamanan sistem yang dimilikinya. Dan juga tanpa permintaan penyusupan dari pihak institusi hukum seperti tertera dalam Pasal 31 yang menyatakan aktivitas *hacking* membolehkan intersepsi atau penyadapan dilakukan atas permintaan institusi hukum (kejaksaan atau kepolisisan). Jadi segala bentuk aktivitas

hacking hanya diperbolehkan jika atas permintaan melalui institusi yang ditetapkan Undang-undang. Bila yang dimaksud dengan "melawan hukum" seperti penjelasan di atas. Maka Pasal 30 dapat dimaknai *hacking* merupakan aktivitas yang hanya boleh dilakukan oleh pihak-pihak tertentu saja.

Dalam hukum Islam lebih tegas lagi dalam menyikapi fenomena *hacking* ini. Dua aspek mendasar dari kegiatan *hacking* yang perlu digarisbawahi adalah :

1) *hacking* merupakan kegiatan yang positif tapi berubah negatif ketika pelaku tidak memiliki hak untuk mengakses komputer tujuan. Ditinjau dari aspek ini maka hukum yang dapat dikenakan atau dijadikan pedoman adalah fiqih jinayah. Tindakan penyusupan secara mutlak dilarang kecuali ada izin dari yang berhak. Dapat disimpulkan bahwa *hacking* tanpa izin walaupun hanya sekedar melihat isi dari properti yang dituju tetap dilarang. Jadi aspek niat di pelaku tidak dapat dijadikan alasan pembenaran dalam menerapkan penyusupan tanpa izin, karena niat merupakan suatu yang abstrak dan hanya bisa diketahui bila dijabarkan secara lisan. Walaupun terdapat dalil yang berbunyi :

   انماالاعمالبالنياتوانمالامرىءمانواى

   Segala sesuatu tergantung pada niatnya, dan apa yang didapatkan ialah apa yang telah diniatkan.

   Tetapi dilihat dari maqasid al-shari'ah dan maslahah mursalah-nya, izin dalam penerapan hacking adalah cara terbaik dan teraman bagi kedua belah pihak yang berkepentingan. Sebab izin merupakan upaya keridhaan atau semacam perjanjian yang mengikatkan antara kedua belah pihak dari akibat yang akan ditimbulkan dari proses yang diperjanjikan dalam masalah ini *hacking.*

Dari penjabaran di atas, hukum Islam telah meletakkan dasar preventif (pencegahan) dengan mewajibkan setiap orang yang akan memasuki properti (dalam kasus ini bisa berupa komputer yang terhubung secara sistematis melalui jaringan internet secara global) milik orang lain dengan izin. Hal ini sebagai pencegahan akan timbulnya pelanggaran turunan dari penyusupan seperti pencurian data, file, password, dan pengrusakan seperti *deface*. Dasar hukum upaya tindakan preventif dapat ditemukan dalam ayat-ayat berikut :

وَقُلْنَا يَـٰٓـَٔادَمُ ٱسْكُنْ أَنتَ وَزَوْجُكَ ٱلْجَنَّةَ وَكُلَا مِنْهَا رَغَدًا حَيْثُ شِئْتُمَا وَلَا تَقْرَبَا هَـٰذِهِ ٱلشَّجَرَةَ فَتَكُونَا مِنَ ٱلظَّـٰلِمِينَ ﴿٣٥﴾

Dan Kami berfirman: "Hai Adam, diamilah oleh kamu dan isterimu surga ini, dan makanlah makanan-makanannya yang banyak lagi baik dimana saja yang kamu sukai, dan janganlah kamu dekati pohon ini, yang menyebabkan kamu Termasuk orang-orang yang zalim. (Al-Baqarah: 35).

وَلَا تَقْرَبُوا۟ ٱلزِّنَىٰٓ ۖ إِنَّهُۥ كَانَ فَـٰحِشَةً وَسَآءَ سَبِيلًا ﴿٣٢﴾

Dan janganlah kamu mendekati zina Sesungguhnya zina itu adalah suatu perbuatan yang keji. Dan suatu jalan yang buruk. (Al-Isra': 32)

2) *Hacking* merupakan suatu kegiatan positif, tapi akan menjadi negatif bila ada percobaan untuk menggunakan suatu yang tidak hak dengan melanggar perjanjian perjanjian dari pemilik yang hak. Dalam aspek ini, maka unsur *fiqih muamalah* akan menjadi hukum dasar penyelesaiannya.

Dalam pemakaian *software* sudah umum diketahui *user* telah mengikatkan diri pada sebuah perjanjian dengan programmer atau perusahaan yang menciptakan *software* bersangkutan. Terutama di Indonesia, penggunaan *software* bajakan sangat mengkhawatirkan, karena mudahnya memperoleh *software* bajakan yang berawal dari

permintaan pasar (terutama dari kalangan yang tidak mampu) peluang tersebut kemudian dimanfaatkan oleh *cracker* yang memiliki kemampuan untuk membobol keamanan dari sebuah *software*.

Software bajakan yang bisa berupa dalam berbagai macam dan bentuk (*patch, keygen*) adalah hasil akhir dari proses yang dilakukan oleh *cracker*. Seperti yang telah dijelaskan di atas, bahwa menggunakan *software* bajakan terdapat unsur kesengajaan melanggr perjanjian yang tentunya dilarang secara agama. Karena posisi perjanjian dalam pemakaian *software* adalah menjaga agar tidak dirusak, diubah, dimodifikasi, dan digunakan sesuai aturan main yang telah ditetapkan si pemilik.

Maka, memfasilitasi dengan cara membuat peranti lunak untuk membajak, mendistribusikan agar *software* bisa digunakan secara tidak sah tentunya lebih terlarang lagi. Karena, esensi sebuah perjanjian itu harus dijaga, tidak bisa dilanggar dan menjaga agar perjanjian tidak dirusak sama dengan hukumnya menjaga barang (kerusakan atau manipulasi) sesuai kaidah *fiqhiyyah* berikut :

الحريملهحكمماهوحريمله

Yang menjaga sesuatu hukumnya sama dengan apa yang dijaga.

Tetapi apabila seseorang menggunakn metode *hacking* untuk kebaikan dan untuk melindungi kebersamaan (mencari *bug* atau *hole*) maka dalam Al-Qur'an dibolehkan berdasarkan ayat berikut :

إِنَّمَا حَرَّمَ عَلَيۡكُمُ ٱلۡمَيۡتَةَ وَٱلدَّمَ وَلَحۡمَ ٱلۡخِنزِيرِ وَمَآ أُهِلَّ بِهِۦ لِغَيۡرِ ٱللَّهِۖ فَمَنِ ٱضۡطُرَّ غَيۡرَ بَاغٖ وَلَا عَادٖ فَلَآ إِثۡمَ عَلَيۡهِۚ إِنَّ ٱللَّهَ غَفُورٞ رَّحِيمٌ ١٧٣

Sesungguhnya Allah hanya mengharamkan bagimu bangkai, darah, daging babi, dan binatang yang (ketika disembelih) tidak disebut (nama) selain Allah. Tetapi barang siapa dalam keadaan terpaksa

(memakannya) sedang dia tidak menginginkannya dan tidak (pula) melampaui batas, Maka tidak ada dosa baginya. Sesungguhnya Allah Maha Pengampun lagi Maha Penyayang. (Al-Baqarah:173).

Dari penjabaran diatas, *hacking* yang pada awal mulanya lebih merupakan kegiatan positif untuk mengembangkan teknologi informasi sehingga melahirkan produk-produk seperti komputer dan internet. Lama kelamaan dalam aktivitas *hacking* tidak terlepas dari perbuatan yang terlarang atau memungkinkan dalam proses *hacking* itu meyebabkan dikerjakannya perbuatan terlarang. Perlu digarisbawahi perbuatan terlarang dalam kegiatan *hacking* itu akan lebih maksimal dengan menjalankan beberapa perbuatan terlarang yang telah dijelaskan pada beberapa penjelasan sebelumnya. Hal ini mendasarkan bahwa melakukan perbuatan terlarang tersebut akan menimbulkan kebaikan yang lebih besar atau mencegah keburukan yang lebih besar (*saddu az-zari'ah*). Hal ini sesuai dengan tujuan ditetapkan hukum atas mukallaf, yaitu untuk mencapai kemaslahatan dan menjauhkan diri dari kerusakan.

BAB EMPAT
PENUTUP

A. Kesimpulan

Dari hasil penelitian yang telah penulis lakukan dalam penulisan skripsi ini maka ada beberapa yang dapat penulis simpulkan yaitu:

a. Pada dasarnya *Hacking* merupakan suatu seni dalam menembus sistem komputer untuk mengetahui seperti apa sistem tersebut dan bagaimana berfungsinya. Hacking dapat dibedakan dalam dua kategori yaitu hacking yang baik dan hacking yang jahat yang membedakan keduanya adalah dari cara dan akibat yang ditimbulkannya apabila akibat yang ditimbulkan dari aktivitas hacking nya adalah merusak maka itu dikategorikan hacking jahat dan pula sebaliknya.
b. Salah satu aktivitas *hacking* yang sering diperdebatkan adalah penyusupan untuk tujuan tertentu dalam suatu sistem teknologi informasi. Perlu digarisbawahi aspek terpenting dalam pembahasan *hacking* di sini adalah penyusupan yang berupa percobaan menjebol, menerobos melampaui sistem proteksi dari suatu sistem atau *software*. Sebab dengan berhasilnya seseorang menyusup dan menjebol proteksi sistem atau *software* maka akan terbuka lebar peluang untuk melakukan kejahatan seperti pencurian data penting, password, nomor kartu kredit atau sengan lain yang berupa *deface* dan lain sebagainya.

Undang-undang tentang Informasi dan Transaksi Elektronik mengatur hal tersebut dalam Pasal 30 ayat 1 sampai 3, yang dengan tegas melarang penyusupan (mengakses sistem atau software orang lain) dalam bentuk apapun kecuali dengan izin dari sang pemilik.

Dalam pasal tersebut terdapat kata “melawan hukum” yang mengandung berbagai pertanyaan dan sering diperdebatkan.

Sebagai contoh permasalahan, untuk mencari kelemahan sistem (*bug* atau *hole*), *programmer* atau *admin* suatu jaringan komputer skala kecil akan menerapkan metode *hacking* dengan mencoba menyusup untuk menguji keamanan sistem yang dimilikinya. Dan juga tanpa permintaan penyusupan dari pihak institusi hukum seperti tertera dalam Pasal 31 yang menyatakan aktivitas *hacking* membolehkan intersepsi atau penyadapan dilakukan atas permintaan institusi hukum (kejaksaan atau kepolisian). Jadi segala bentuk aktivitas *hacking* hanya diperbolehkan jika atas permintaan melalui institusi yang ditetapkan Undang-undang. Bila yang dimaksud dengan “melawan hukum” seperti penjelasan di atas. Maka Pasal 30 dapat dimaknai *hacking* merupakan aktivitas yang hanya boleh dilakukan oleh pihak-pihak tertentu saja.

c. Dalam hukum Islam lebih tegas lagi dalam menyikapi fenomena *hacking* ini. Dua aspek mendasar dari kegiatan *hacking* yang perlu digarisbawahi adalah: *hacking* merupakan kegiatan yang positif tapi berubah negatif ketika pelaku tidak memiliki hak untuk mengakses komputer tujuan. Ditinjau dari aspek ini maka hukum yang dapat dikenakan atau dijadikan pedoman adalah fiqih jinayah. Tindakan penyusupan secara mutlak dilarang kecuali ada izin dari yang berhak. Dapat disimpulkan bahwa *hacking* tanpa izin walaupun hanya sekedar melihat isi dari properti yang dituju tetap dilarang. Jadi aspek niat si pelaku tidak dapat dijadikan alasan pembenaran dalam

menerapkan penyusupan tanpa izin, karena niat merupakan suatu yang abstrak dan hanya bisa diketahui bila dijabarkan secara lisan

B. Saran

1. Pemerintah perlu mengeluarkan aturan main hacking dengan mengeluarkan peraturan pemerintah selain untuk menjelaskan beberapa pasal yang masih mengambang (salah perspektif) juga untuk memudahkan bagi profesional yang bergerak dalam bidang teknologi informasi, serta memberikan pendidikan kepada masyarakat melalui peraturan yang ada. Sehingga aktifitas mereka tetap terlindungi hukum.
2. Sedangkan dalam hukum islam, perlu lebih dikembangkan lagi dengan meggalakkan penelitian dalam bidang teknologi komunikasi informasi dengan menggunakan metodologi hukum Islam yang berkaitan dengan hacking. Karena banyak dari umat islam sewaktu menghadapi masalah kontenporer terutama di bidang teknologi kominikasi dan informasi dapat memiliki pedoman, sekaligus produk hukum itu sendiri dapat dijadikan pembanding bagi hukum positif yang berlaku.

DAFTAR PUSTAKA

Arief, Barda Nawawi. 2007. *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia.* Jakarta: PT. Raja Grafindo Persada.

Ash-Shidqie, Hasbi. 1979. *Filsafat Hukum Islam.* Jakarta: Bulan Bintang.

Ariyus, Dony. 2005. *Kamus Hacker*. Yogyakarta: Andi.

Anam, Khairul.2010. *Hacking VS Hukum Positif & Hukum Islam.* Yogyakarta: Sunan Kalijaga Press.

Anwar, Syamsul.2007. *Hukum Perjanjian Syari'ah*: Studi *tentang Teori Akad dalam Fiqih Muamalat*. Jakarta: Raja Grafindo Persada.

Chazawi, Adami. 2005. *Pelajaran Hukum Pidana 2.* Jakarta: Raja Grafindo Persada.

Efendi, Satria. 2013. *Ushul Fiqh.* Jakarta: Rajawali Pers.

Haroen , Nasrun. 1996. *Ushul FiqihI.* Ciputat: Logos publishing House.

H.A Jazuli. 1997. *fiqih Jinayah Upaya Menanggulangi Kejahatan dalam Islam*. Jakarta: Raja Grafindo.

M. Ramli, Ahmad. 2004. *Cyber Law dan HAKI dalam Sistem Hukum Indonesia.* Bandung: PT. Refika Aditama.

Maskun. 2013. *Kejahatan Siber Cyber Crime Suatu Pengatar*. Jakarta: Kencana Prenada Media Group.

Masyrofah, H. M. Nurul Irfan. 2005. *Fiqih Jinayah.* Jakarta: Amzah.

Nata, Abuadin. 2013. *Metodologi Studi Islam.* Jakarta: Rajawali Pers.

Nazir, Muhammad. 2004. *Metode Penelitian*. Jakarta: Ghalia Indonesia.

Putra, Rahmat.2007. *The Secret of Hacker Mengungkap Cara Kerja Hacker dan melindungi Diri dari Serangan Mereka.* Jakarta selatan: Mediakita.

Riswandi, Budi Agus. 2003. *Hukum dan Internet di Indonesia*. Yogyakarta: UII Press.

Rahman, H. Asjmuni. 1976. *Qaidah-Qaidah fiqih.* Jakarta: Bulan Bintang.

Suparni, Niniek. 2009. *Cyberspace Problematika & Antisipasi Pengaturannya.* Jakarta: Sinar Grafika.

Soekanto, Soerjono. 2006. *Pengantar Penelitian Hukum.*Jakarta: Universitas Indonesia.

Sunggono, Bambang. 2007. *Pengantar Metodologi Penelitian Hukum.* Jakarta: PT. Raja Grapindo Persada.

Surakhmad, Winarno. 1978. *Dasar dan Teknik Research.*Bandung: Tarsito.

S'to. 2016. *Seni internet Hacking*. Jakarta: Jasakom.

Sutarwan. 2007. *Cyber Crime Modus Operandi dan Penanggulangannya*. Jogjakarta: Laks Bang Pressindo.

Suhrawadi k. Lubis, H. Chairuman Pasaribu. 2004. *Hukum Perjanjian dalam Islam*, cet. 3. Jakarta: Sinar Grafika.

Thomas, Tom. 2005. *Network Security First-Step,*terj. Yogyakarta: Andi.

Utdirartatmo, Firrar.2004. *Awas Ada Hacker*. Yogyakarta: Gava Media.

http://*cetak*.kompas.com/read/xml/2008/04/17/02300074.

http://www.kompas.com/read/xml/2008/06/13/2004422/merangkul.

http://tekno.kompas.com/read/xml/2008/03/24/22062449.

https://www.google.com/amp/s/m.liputan6.com/amp/97375/perang-ihackeri indonesia malaysia dinilai-merugikan-situs?espv=1