

**ANALISIS HUKUM POSITIF DAN FIQIH JINAYAH
TENTANG SANKSI PIDANA KEJAHATAN SIBER
DENGAN METODE *DDOS ATTACK* TERHADAP
*WEBSITE***

SKRIPSI

Diajukan Untuk Memenuhi Tugas Dan Melengkapi Syarat
Guna Memperoleh Gelar Sarjana Strata Satu (S.1)
Pada Fakultas Syari'ah dan Hukum



Disusun oleh :

Eko Wahyu Ramadani

1802026009

**HUKUM PIDANA ISLAM
FAKULTAS SYARIAH DAN HUKUM
UNIVERSITAS ISLAM NEGERI WALISONGO
SEMARANG
2022**



KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI WALISONGO SEMARANG
FAKULTAS SYARI'AH DAN HUKUM
Jl. Prof. Dr. Hamka, km 2 (Kampus 3 UIN Walisongo) Ngaliyan,
Semarang, 50185, telp (024) 7601291)

NOTA PERSETUJUAN PEMBIMBING

Lamp : 4 (empat) eks.
Hal : Naskah Skripsi
An. Sdr. Eko Wahyu Ramadani
Kepada Yth.
Dekan Fakultas Syari'ah dan Hukum UIN Walisongo
di Semarang

Assalamu'alaikum Wr. Wb.

Setelah saya meneliti dan mengadakan perbaikan seperlunya, bersama ini saya kirim naskah skripsi Saudara :

Nama : Eko Wahyu Ramadani
NIM : 1802026009
Prodi : Hukum Pidana Islam
Judul : Analisis Hukum Positif Dan Fiqih Jinayah Tentang Sanksi Pidana
Kejahatan Siber Dengan Metode *DDoS Attack* Terhadap *Website*

Dengan ini saya mohon kiranya skripsi Saudara tersebut dapat segera dimunaqasyahkan. Demikian harap menjadikan maklum.

Wassalamu'alaikum Wr. Wb.

Semarang, 18 April 2022

Pembimbing I

Pembimbing II

Rustam D.K.A.H, M.Ag.
NIP. 196907231998031005

Riza Fibrizani, S.H., M.H.
NIP. 198902112019032015



KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI WALISONGO
FAKULTAS SYARIAH DAN HUKUM

Jl. Prof. Dr. Hamka Kampus III Ngaliyan (024) 7601291 Fax. 7624691

Semarang 50185

PENGESAHAN

Skripsi Saudara : Eko Wahyu Ramadani
NIM : 1802026009
Judul : Analisis Hukum Positif dan Fiqih Jinayah Tentang Sanksi Pidana
Kejahatan Siber Dengan Metode *DDoS Attack* Terhadap *Website*

Telah dimunaqasahkan oleh Dewan Penguji Fakultas Syaria'ah dan Hukum
Universitas Islam Negeri Walisongo Semarang, dan dinyatakan lulus dengan
predikat cumlaude / baik / cukup, pada tanggal : 22 April 2022
dan dapat diterima sebagai syarat guna memperoleh gelar Sarjana Strata 1
tahun akademik 2021/2022

Ketua Sidang

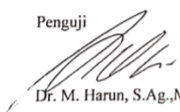

Ahmad Munif, M.S.I.
NIP 198603062015031006

Semarang, 27 April 2022

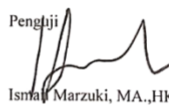
Sekretaris Sidang


Rustam D.K.A.H, M.Ag.
NIP196907231998031005

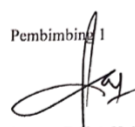
Penguji


Dr. M. Harun, S.Ag.,M.H.
NIP 197508152008011017


Penguji


Isma Marzuki, MA.,HK.
NIP 198308092015031002

Pembimbing 1


Rustam D.K.A.H, M.Ag.
NIP 196907231998031005

Pembimbing 2


Riza Fijriani, S.H., M.H.
NIP 198902112019032015

MOTTO

وَلَا تُفْسِدُوا فِي الْأَرْضِ بَعْدَ إِصْلَاحِهَا وَادْعُوهُ حَوْفًا وَقَطْمَعًا ۗ

“Dan janganlah kamu berbuat kerusakan di bumi setelah
(diciptakan) dengan baik”
(Q.S Al-A'raf: 56)

HALAMAN PERSEMBAHAN

Skripsi ini penulis persembahkan pada :

1. Kedua orang tua penulis, Bapak Budi Iswanto dan Ibunda Suprpti Intan Sari yang dengan tulus mendidik dan membesarkan penulis dengan kasih sayang, serta memberikan motivasi dan curahan do'a yang selalu mengalir mengiringi setiap langkah perjuangan penulis, terutama saat penulis menyelesaikan skripsi ini.
2. Adik penulis Andrean Fernando dan Abyan Fakhrrurizky yang selalu memberikan dukungan baik moril maupun materil saat penulis menempuh studi.
3. Kepada Saudara-saudara Penulis M. Effendi Zakarsih, S.Pd., M. Bion As'ari, Tyas Ayu Ningrum, S.E., dan Riki Febriansyah, S.Pd. yang selalu memberikan masukan kepada penulis dalam menyelesaikan skripsi ini.
4. Bapak Rustam Dahar Karnadi Apollo Harahap, M.Ag. Selaku Pembimbing I dan Ibu Riza Fibriani, S.H., M.H., selaku pembimbing II yang dengan ikhlas memberikan bimbingan, dukungan semangat, masukan, kritik, dan saran terhadap penelitian skripsi penulis.
5. Rahma Cahya M yang selalu memahami dan mendoakan penulis.
6. Segenap Dosen dan civitas akademika UIN Walisongo Semarang khususnya Fakultas Syari'ah dan Hukum Jurusan Hukum Pidana Islam.

DEKLARASI

Dengan penuh kejujuran dan tanggung jawab, penulis menyatakan bahwa skripsi saya yang berjudul “**ANALISIS HUKUM POSITIF DAN FIQH JINAYAH TENTANG SANKSI PIDANA KEJAHATAN SIBER DENGAN METODE *DDOS ATTACK TERHADAP WEBSITE***” tidak berisi materi yang telah ditulis oleh orang lain atau diterbitkan. Demikian pula skripsi ini tidak berisi satu pun pikiran-pikiran orang lain, kecuali informasi yang terdapat dalam referensi yang dijadikan bahan rujukan.

Semarang, 17 April 2022

Deklarator



Eko Wahyu Ramadani

1802026009

PEDOMAN TRANSLITERASI ARAB-LATIN

Transliterasi huruf Arab ke dalam huruf latin yang dipakai dalam penulisan skripsi ini berpedoman pada Surat Keputusan Bersama Menteri Agama dan Menteri Pendidikan dan Kebudayaan Republik Indonesia Nomor: 158/1987 dan Nomor: 05936/U/1987.

I. Konsonan Tunggal

Huruf Arab	Nama	Huruf Latin	Nama
ا	Alif	Tidak dilambangkan	Tidak dilambangkan
ب	Ba	b	be
ت	Ta	t	te
ث	Sa	š	es (dengan titik di atas)
ج	Jim	j	je
ح	Ha	ḥ	ha (dengan titik di bawah)
خ	Kha	kh	ka dan ha
د	Dal	d	de
ذ	Dza	dz	zet (dengan titik diatas)
ر	Ra	r	er
ز	Za	z	zet
س	Sin	s	es
ش	Syin	sy	es dan ye
ص	Sad	š	es (dengan titik di bawah)
ض	Dad	ḍ	de (dengan titik di bawah)
ط	Tha	ṭ	te (dengan titik di bawah)
ظ	Zha	ẓ	zet (dengan titik dibawah)
ع	‘ain	‘	koma terbalik di atas
غ	Gain	g	ge

ف	Fa'	f	ef
ق	Qa	q	qi
ك	Kaf	k	ka
ل	Lam	'l	'el
م	Mim	'm	'em
ن	Nun	'n	'en
و	Wau	w	w
ه	Ha	H	ha
ء	Hamzah	,	apostrof
ي	Ya	Y	ye

II. Ta'marbutah di Akhir Kata

Bila dimatikan ditulis h

حكمة	Ditulis	Hikmah
جزية	Ditulis	Jizyah

Bila diikuti dengan kata sandang 'al' serta bacaan kedua itu terpisah, maka ditulish

كرامة الاولياء	Ditulis	Karamah al-Auliya'
----------------	---------	--------------------

Bila ta'marbutah hidup atau dengan harakat, fathah, kasrah, dan dammah ditulis t

زكاة الفطر	Ditulis	Zakaatul fitri
------------	---------	----------------

III. Vokal Pendek

(َ)	Fathah	Ditulis	a
(ِ)	Kasrah	Ditulis	i
(ُ)	Dammah	Ditulis	u

IV. Vokal pendek yang berurutan dalam satu kata dipisahkan dengan apostrof

انتم	Ditulis	a'antum
اعدت	Ditulis	'u'iddat

V. Kata Sandang Alif +Lam

Bila diikuti huruf Qomariyah ditulis L (el)

القران	Ditulis	al-Qur'an
القياس	Ditulis	al-Qiyas

Bila diikuti huruf syamsiyah ditulis dengan menggunakan huruf syamsiyah yang mengikutinya, serta menghilangkan huruf l (el) nya.

السماء	Ditulis	as-Samaa'
الشمس	Ditulis	asy-Syams

VI. Penulisan kata-kata dalam rangkaian kalimat

بديعة المجتهد	Ditulis	bidayatul mujtahid
سد الذريعة	Ditulis	sadd adz dzariah

VII. Pengecualian

Sistem Translaterasi tidak berlaku pada:

- a. Kosa kata Arab yang lazim dalam Bahasa Indonesia dan terdapat dalam Kamus Umum Bahasa Indonesia, misalnya: Al-Qur'an, hadis, mazhab, lafaz.
- b. Judul buku yang menggunakan kata Arab, namun sudah dilatinkan oleh penerbit, seperti judul buku *Ushul al-Fiqh al-Islami, Fiqh Munakahat*.
- c. Nama pengarang yang menggunakan nama Arab, tapi berasal dari negara yang menggunakan huruf latin, misalnya Nasrun Haroen, Wahbah al-Zuhaili, As- Sarakhi.
- d. Nama penerbit di Indonesia yang menggunakan kata Arab, misalnya Toko Hidayah, Mizan.

KATA PENGANTAR

Alhamdulillah, puji syukur kehadiran Allah SWT karena atas berkat, rahmat, dan karunia-Nya sehingga penulis dapat menyelesaikan penulisan skripsi ini. Pada kesempatan ini, perkenankanlah penulis menghaturkan ucapan terimakasih yang sedalam-dalamnya kepada:

1. Bapak Rustam Dahar Karnadi Apollo Harahap, M.Ag. Selaku Pembimbing I dan Ibu Riza Fibriani, S.H., M.H., selaku pembimbing II yang dengan ikhlas memberikan bimbingan, dukungan semangat, masukan, kritik, dan saran terhadap penelitian skripsi penulis. Kerelaan beliau dalam mengorbankan waktu, tenaga, dan pikiran merupakan salah satu faktor keberhasilan penulis dalam menyelesaikan skripsi ini.
2. Kedua orang tua penulis, Bapak Budi Iswanto dan Ibunda Suprapti Intan Sari yang dengan tulus mendidik dan membesarkan penulis dengan kasih sayang, serta memberikan motivasi dan curahan do'a yang selalu mengalir mengiringi setiap langkah perjuangan penulis, terutama saat penulis menyelesaikan skripsi ini.
3. Adik penulis Andrean Fernando dan Abyan Fakhurriszky yang selalu memberikan dukungan baik moril maupun materil saat penulis menempuh studi.
4. Kepada Saudara-saudara Penulis M. Effendi Zakarsih, M. Bion As'ari, Tyas Ayu Ningrum, dan Riki Febriansyah yang selalu memberikan masukan kepada penulis dalam menyelesaikan skripsi ini.

5. Bapak Prof. Imam Taufik selaku rektor UIN Walisongo dan segenap jajarannya.
6. Bapak Dr. Arja Imroni selaku dekan UIN Walisongo beserta segenap jajarannya.
7. Bapak Rustam Dahar Karnadi Apollo Harahap, M.Ag. selaku Ketua Jurusan Hukum Pidana Islam UIN Walisongo Semarang.
8. Bapak Dr. H. Ja'far Baehaqi, S.Ag., M.H. selaku sekretaris Jurusan Hukum Pidana Islam UIN Walisongo Semarang.
9. Segenap dosen dan civitas akademika UIN Walisongo Semarang khususnya Fakultas Syari'ah dan Hukum Jurusan Hukum Pidana Islam.
10. Rekan-rekan dari Lembaga Riset dan Debat (LRD), terkhusus pembimbing LRD Ibu Dr. Novita Dewi Masyithoh, S.H., M.H., dan ibu Briliyan Ernawati, S.H., M.H. yang telah mengasah kemampuan penulis baik melalui diskusi-diskusi hukum maupun kompetisi-kompetisi debat semasa penulis menjalani perkuliahan. Pengalaman berharga bersama rekan-rekan tidak akan penulis lupakan.
11. Teman-teman Hukum Pidana Islam 2018 khususnya kelas HPI-A 2018 yang tak bisa penulis sebutkan satu-persatu. Terima kasih telah menemani dan memberikan support dalam perjalanan menuntut ilmu semasa berkuliah di UIN Walisongo Semarang.
12. Semua pihak yang tidak sempat penulis sebutkan satu persatu yang telah membantu penulis khususnya dalam penulisan skripsi, terimakasih. Semoga semua kebaikan

kalian berbalas dengan pahala dari Allah Yang Maha Kuasa. Penyusun menyadari dalam penulisan skripsi ini masih banyak terdapat kekurangan dan kesalahan maka segala sesuatu yang baik itu datangnya dari Allah dan segala keluputan ataupun kesalahan adalah berasal dari penulis. Semoga penelitian ini bermanfaat dan dapat memberikan kontribusi terhadap perkembangan ilmu pengetahuan.

Semarang, 17 April 2022

A handwritten signature in black ink, appearing to read 'Eko Wahyu Ramadani', with a stylized flourish at the end.

Eko Wahyu Ramadani
1802026009

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN MOTTO	iv
HALAMAN PERSEMBAHAN.....	v
HALAMAN DEKLARASI.....	vi
PEDOMAN TRANSLITERASI ARAB-LATIN.....	vii
KATA PENGANTAR.....	xi
DAFTAR ISI.....	xiv
ABSTRAK	xviii
BAB I PENDAHULUAN	
A. Latar Belakang	1
B. Rumusan Masalah	18
C. Tujuan dan Manfaat Penelitian	19
D. Tinjauan Pustaka.....	20
E. Metode Penelitian.....	25
F. Sistematika Penulisan	28
BAB II TINJAUAN UMUM SANKSI PIDANA KEJAHATAN SIBER DALAM HUKUM POSITIF DAN FIQH JINAYAH	
A. Kejahatan Siber (<i>Cybercrime</i>) Dengan Metode <i>DDos Attack</i>	30
1. Definisi Kejahatan Siber (<i>Cybercrime</i>)	30
2. Bentuk-Bentuk Kejahatan Siber (<i>Cybercrime</i>)....	31
3. Unsur-Unsur Kejahatan Siber Dengan Metode <i>DDos Attack</i>	34

B. Tindak Pidana Kejahatan Siber Dalam Hukum Positif	35
1. Pengertian, Asas, Dan Unsur Tindak Pidana	35
a. Pengertian Tindak Pidana	35
b. Asas-Asas Hukum Pidana	39
c. Unsur-Unsur Tindak Pidana	43
2. Bentuk Dan Sanksi Pidana Kejahatan Siber Dalam Hukum Positif	49
a. Bentuk Dan Sanksi Pidana Dalam Hukum Positif	49
b. Delik Dan Sanksi Pidana Kejahatan Siber Dengan Metode <i>Ddos Attack</i> Dalam Kitab Undang-Undang Hukum Pidana (Kuhp) Serta Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.	50
C. Sanksi Pidana Kejahatan Siber Dalam Fiqih Jinayah	56
1. Pengertian Fiqih Jinayah	56
2. Asas-Asas Fiqih Jinayah	57
3. Pengertian <i>Jarimah Ta'zir</i>	63
4. Unsur-unsur <i>Jarimah Ta'zir</i>	69
5. Perbedaan <i>Jarimah Hudud</i> Dan <i>Jarimah Ta'zir</i> .	71
6. Macam-Macam Hukuman <i>Ta'zir</i>	73
7. Syarat-Syarat Penerapan <i>Jarimah</i>	77
8. Sanksi Pidana Kejahatan Siber Dengan Metode <i>DDoS Attack</i> Dalam Fiqih Jinayah	80

BAB III KEJAHATAN SIBER DENGAN METODE *DDOS* ATTACK TERHADAP *WEBSITE*

A. Kejahatan Siber Dengan Metode <i>DDoS Attack</i>	85
1. Pengertian Kejahatan Siber (<i>Cybercrime</i>).....	85
2. Kejahatan Siber Dengan Metode <i>DDoS Attack</i> ...	86
3. Data Serangan <i>DDoS Attack</i>	90
4. Faktor Terjadinya Serangan <i>DDoS Attack</i>	98
5. Jenis-Jenis Metode Serangan <i>DDoS Attack</i>	100
B. <i>Website</i> Sebagai Target Serangan Siber Dengan Metode <i>DDoS Attack</i>	122
1. Pengertian <i>Website</i>	122
2. Struktur <i>Website</i>	124
3. Akibat Serangan <i>DDoS Attack</i> Terhadap <i>Website</i>	127

BAB IV ANALISIS HUKUM POSITIF DAN FIQH JINAYAH TENTANG SANKSI PIDANA KEJAHATAN SIBER DENGAN METODE *DDOS* ATTACK TERHADAP *WEBSITE*

A. Analisis Hukum Positif Tentang Sanksi Pidana Kejahatan Siber Dengan Metode <i>DDoS Attack</i> Terhadap <i>Website</i>	129
B. Analisis Fiqh Jinayah Tentang Sanksi Pidana Kejahatan Siber Dengan Metode <i>DDoS Attack</i> Terhadap <i>Website</i>	144

BAB V PENUTUP

A. Simpulan..... 162

B. Saran 163

DAFTAR PUSTAKA..... 165

DAFTAR RIWAYAT HIDUP 169

ABSTRAK

Kejahatan siber dengan metode *DDoS attack* terhadap *website* merupakan kejahatan yang digunakan untuk melumpuhkan *website* dengan cara membanjiri *traffic webserver* sehingga *webserver* mengalami *overload* dan berakibat pada kerusakan sistem *website*. Ancaman serangan siber dengan metode ini sangat nyata namun penegakan hukum di Indonesia tidak secara maksimal dapat menuntaskan kejahatan siber ini salah satu penyebabnya adalah karena belum jelasnya aturan sanksi pidana dalam hukum positif di Indonesia, maka dari itu penelitian ini berusaha untuk menganalisis Hukum Positif tentang bagaimana sanksi pidana kejahatan siber *DDoS Attack* terhadap *website*, kemudian dalam rangka mengisi kekosongan hukum dalam Fiqih Jinayah penelitian ini juga berusaha untuk menganalisis Fiqih Jinayah tentang bagaimana sanksi pidana *DDoS attack* terhadap *website*.

Penelitian ini menggunakan metode penelitian hukum kualitatif, metode pengumpulan data yang digunakan dalam skripsi ini menggunakan metode dokumentasi/studi pustaka dengan data primer yang bersumber dari Kitab Undang-undang Hukum Pidana (KUHP), Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dan kitab *Al-Qawâ'id wal-Ushûl al-Jûmi'ah wal-Furûq wat-Taqâsîm al-Badî'ah an-Nâfi'ah*, karya Syaikh 'Abdur-Rahmân as-Sa'di, tahqiq: Dr. Khalid bin 'Ali bin Muhammad al-Musyaiqih, Darul wathan, cetakan II, data sekunder dalam penelitian ini bersumber dari pendapat atau tulisan para ahli dalam bidang *cyber* dan fiqih jinayah dan data tersier bersumber dari kamus hukum, terminologi dan lain sebagainya.

Sanksi Pidana kejahatan siber dengan metode *DDoS attack* terhadap *Website* dalam Hukum positif terdapat dalam Pasal 406 ayat (1) Kitab Undang-undang Hukum Pidana (KUHP), dan Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 30 ayat (3) Jo Pasal 46 ayat (3) dengan ancaman pidana penjara paling lama 8 (delapan) tahun dan/atau

denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah) serta Pasal 33 Jo Pasal 49 dengan ancaman pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000,00 (sepuluh miliar rupiah). Adapun dalam fiqih jinayah sanksi pidananya dapat dirumuskan berdasarkan kaidah fiqih ke-13 (tiga belas) yang terdapat dalam kitab *Al-Qawâ'id wal-Ushûl al-Jûmi'ah wal-Furûq wat-Taqâsîm al-Badî'ah an-Nâfi'ah*, karya Syaikh 'Abdur-Rahmân as-Sa'di, tahqiq: Dr. Khalid bin 'Ali bin Muhammad al-Musyaiqih, Darul wathan, cetakan II. yang menghasilkan sanksi pidana yaitu *Jarimah ta'zir* berupa hukuman denda (*Ghuramah*) dan hukam penjara jika hukuman denda (*Ghuramah*) menurut hakim belum maksimal.

Kata kunci: *DDoS attack, Hukum Positif, Fiqih Jinayah*

BAB I

PENDAHULUAN

A. Latar Belakang

Kejahatan siber di era modern sekarang ini sangat sering terjadi terutama dalam bidang penyampaian informasi yang dilakukan menggunakan media *Website*. Metode serangan siber terus berkembang seiring dengan berkembangnya kemajuan teknologi, salah satu metode serangan yang menjadikan *Website* sebagai target utama adalah *DDoS attack*. *DDoS Attack* adalah salah satu jenis tindak kriminal dunia maya yang serangannya ditujukan untuk membuat komputer atau jaringan komputer tidak dapat menyediakan layanan secara normal. Pada umumnya serangan *DDoS Attack* menargetkan serangan pada *bandwidth* jaringan komputer atau koneksi jaringan (*connectivity*).¹ Serangan ini menyebabkan server *Website* yang dituju mengalami *Overload* (kelebihan kapasitas) dan dampaknya *Website* tersebut tidak dapat diakses oleh masyarakat karena terjadi *Down, hang*, bahkan *crash*.²

Kemajuan teknologi telah mengubah banyak hal dalam kehidupan masyarakat modern salah satunya adalah media untuk memperoleh informasi. Masyarakat terdahulu memperoleh informasi melalui media cetak seperti koran,

¹ Rudi Hermawan, "Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos)," *Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos)*, 5.1 (2013), 1–14.

² *Ibid* Hermawan.

surat kabar dan pamphlet yang ditempel di tepi jalan. Sedangkan saat ini, setelah adanya teknologi dan lahirnya internet masyarakat modern dapat memperoleh informasi dengan mudah menggunakan media *Website* yang terhubung melalui internet. *Website* atau *Web* merupakan suatu dokumen berupa sekumpulan halaman yang berisi berbagai informasi dalam bentuk digital. Informasi tersebut dapat berupa teks, gambar, animasi, dan video.³ Internet (*Interconnected Network*) adalah sebuah sistem komunikasi global yang menghubungkan komputer-komputer dan jaringan-jaringan komputer diseluruh dunia.⁴

Website menjadi salah satu media informasi yang penting di era modern, sebagian besar instansi pemerintahan, pendidikan, dan kesehatan menyampaikan informasinya melalui *Website*. *Website* memudahkan instansi untuk menyalurkan informasi dan mempermudah masyarakat dalam mengakses informasi hanya dengan memanfaatkan mesin pencari seperti *google*, *yahoo*, *bing* dan *yandex*. *Website* dikembangkan oleh Tim Berners-Lee pada bulan oktober tahun 1990, Tim

³ Bilal Syahid, "Pengertian Website – Sejarah, Jenis, Manfaat, Unsur, Tahapan, Fungsi, Para Ahli," 07 November, 2021, hal. 1 <<https://www.gurupendidikan.co.id/pengertian-website/>> [diakses 20 Agustus 2021].

⁴ Puskominfo Unsurya, 'Definisi Dan Perbedaan Internet, Intranet Dan Extranet', 25 February, 2014, p. 1 <<https://universitassuryadarma.ac.id/definisi-dan-perbedaan-internet-intranet-dan-extranet/>> [diakses 20 August 2021].

Berners-Lee membuat suatu sistem informasi manajemen, di mana teks dapat berisi link dan referensi ke dokumen lain yang dapat memungkinkan pembaca untuk cepat melompat dari satu dokumen ke dokumen lain. Tim Berners-Lee juga telah menciptakan server untuk penerbitan dokumen, program ini disebut (*hypertext*) serta program untuk membacanya yang disebut *WorldWideWeb*. Perangkat lunak ini pertama kali dirilis pada tahun 1991.⁵

Era modern seperti sekarang ini masyarakat dapat membuat Website menggunakan *platform* pembuat Website seperti *blogspot.com*, *Wordpress.com*, *Wix.com*, *Weebly.com* dan lain sebagainya. Lahirnya teknologi Website ini kemudian memunculkan suatu dunia baru yaitu Dunia Maya (*Cyberspace*). *Cyberspace* atau Dunia maya adalah ruang elektronik dalam jaringan komputer yang banyak digunakan untuk kebutuhan komunikasi satu arah maupun dua arah secara online (terhubung langsung). *Cyberspace* merupakan integrasi dari berbagai peralatan teknologi komunikasi dan jaringan komputer berupa sensor, transduser, koneksi, transmisi, prosesor, *signal*, kontroler yang dapat menghubungkan peralatan komunikasi seperti

⁵ W3C Community, "The History Of The Web," 4 March, 2012, hal. 1 <w3.org/community/webed/wiki/The_history_of_the_Web> [diakses 20 Agustus 2021].

computer, laptop, handphone dan peralatan elektronik lainnya yang terhubung ke internet.⁶

Dunia maya (*Cyberspace*) memberikan ruang munculnya fenomena kejahatan baru yaitu kejahatan dunia maya (*Cybercrime*). *Cybercrime* dalam buku yang berjudul *Investigating Computer-Related Crime*.⁷ Peter Sthepenson menjelaskan bahwa *Cybercrime* adalah sebuah kejahatan yang ditujukan pada sebuah *computer* atau *system computer*. Peter memberikan penjelasan bahwa sifat kejahatan *cyber* sangat kompleks, dari hal sederhana seperti penyadapan atau pengintaian ke dalam sistem komputer dimana kita tidak memiliki otorisasi terhadap komputer tersebut, atau kejahatan misalnya berupa penyebaran virus yang dilakukan oleh seorang karyawan yang merasa tidak puas terhadap kebijakan dalam organisasinya.

Kemudahan membuat *Website* juga beriringan dengan kemudahan untuk melakukan serangan siber (*Cyber Attack*) terhadap *Website*. Salah satu bentuk dari *Cyber attack* terhadap *Website* yang banyak digunakan oleh penyerang (*Attacker*) adalah metode *DDoS attack* (*Distributed Denial of Service Attack*). Serangan *DDoS*

⁶ Abdul Azmi Fadillah, "Aktivitas Komunikasi Lingkar Ganja Nusantara Bandung Melalui Cyberspace," Program Studi Ilmu Komunikasi, Fakultas Sosial Politik, Universitas Komputer Indonesia.

⁷ Spada Kemendikbud, "Definisi Cyber Crime," 24 March, 2021 <<https://lmsspada.kemdikbud.go.id/mod/page/view.php?id=57347&forceview=1>> [diakses 20 Agustus 2021].

attack secara sederhana bisa dilakukan dengan menggunakan perintah *ping* yang dimiliki oleh system operasi *Windows*. Pada dasarnya sebuah komputer dapat mengirimkan data sebesar 32 bytes/detik ke situs yang dituju. Misalnya, jika terdapat 10.000 komputer yang melakukan perintah *ping* secara bersamaan, maka data yang diterima oleh *Website* yang dituju akan sebesar 312 Mega Bytes/detik. Selanjutnya, server akan merespon kiriman data yang dikirim dari 10.000 komputer secara bersamaan. Jika 312 MB/detik data yang harus di proses oleh server, dalam 1 menit saja server harus memproses kiriman data sebesar $312 \text{ MB} \times 60 \text{ detik} = 18720 \text{ MB}$. Maka hasilnya situs yang diserang dengan metode ini akan mengalami *overload* (kelebihan data), sehingga tidak sanggup memproses kiriman data yang datang terus-menerus.⁸

Serangan *DDoS Attack* terbagi kedalam 3 (tiga) jenis serangan yaitu⁹:

1) Serangan berbasis *bandwidth*

Serangan *DDoS* jenis ini mengirim pesan data sampah secara masal untuk menyebabkan *overload*, yang juga mengakibatkan berkurangnya *bandwidth* jaringan yang

⁸ *Op Cit* Hermawan.

⁹ Septian Geges dan Waskitho Wibisono, "Pengembangan Pencegahan Serangan Distributed Denial of Service (Ddos) Pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis Dan Client Puzzle," *JUTI: Jurnal Ilmiah Teknologi Informasi*, 13.1 (2015), 53
<<https://doi.org/10.12962/j24068535.v13i1.a388>>.

tersedia atau berkurangnya sumber daya perangkat jaringan. Seringkali router, server dan firewall yang diserang memiliki sumber daya yang terbatas. Serangan overload menyebabkan kegagalan perangkat jaringan untuk menangani akses yang normal, sehingga terjadi penurunan yang signifikan dalam kualitas layanan atau kelumpuhan total sistem (*DoS*).

2) Serangan berbasis lalu lintas jaringan

Bentuk yang paling umum adalah serangan yang membanjiri lalu lintas jaringan. Serangan ini dilakukan dengan cara mengirimkan sejumlah besar paket TCP, paket UDP, paket ICMP yang tampaknya sah kepada host/server target. Beberapa serangan dengan basis ini juga dapat menghindari pemindaian sistem deteksi dengan teknologi kamufase alamat asal. Permintaan yang sah pada akhirnya tidak terlayani karena begitu banyak paket serangan yang beredar di jaringan. Serangan ini juga dapat semakin merusak jika dikombinasikan dengan kegiatan ilegal lainnya, seperti eksploitasi menggunakan malware yang menyebabkan kebocoran informasi atau pencurian data sensitif pada komputer target.

3) Serangan berbasis aplikasi

Serangan jenis ini biasanya mengirim pesan data pada tingkat layer aplikasi sesuai dengan fitur bisnis yang spesifik (menggunakan fungsi aplikasi yang tampaknya legal dan operasional, seperti akses database), serangan ini menyebabkan semakin berkurangnya sumber daya

tertentu pada lapisan aplikasi (seperti jumlah pengguna dan koneksi aktif yang diperbolehkan) dan layanan sistem tidak lagi tersedia. Serangan seperti ini biasanya tidak dilancarkan dalam volume yang terlalu besar, serangan dengan lalu lintas tingkat rendah pun dapat menyebabkan gangguan serius pada sistem atau bahkan kelumpuhan kinerja sistem bisnis.

Faktor terjadinya serangan siber jenis ini bermacam-macam mulai dari ketidaksukaan kepada pemilik *Website*, ingin menunjukkan eksistensi sebagai *cracker*, karena tidak setuju dengan kebijakan pemerintah, dan melakukan serangan atas perintah orang lain dengan imbalan uang. Motif pelaku *cybercrime* pada umumnya memiliki kesamaan satu sama lain. Motif-motif tersebut berkembang seiring dengan berkembangnya teknologi dan berkembangnya jenis tindak kejahatan yang dapat dilakukan. Serangan *DDoS Attack* pada umumnya banyak dilancarkan untuk melumpuhkan system informasi pemerintah, perbankan, layanan *hosting*, media digital dan situs jual beli saham juga kerap menjadi target serangan *DDoS Attack*.

Sampai saat ini *DDoS Attack* masih menjadi metode serangan siber yang cukup ampuh untuk melumpuhkan *Website*, hal ini dapat dilihat dari data serangan siber dunia yang mana pada januari 2016 situs *Hackmageddon* melaporkan bahwa serangan *DDoS* menempati urutan kedua dari 9 serangan populer.

Walaupun serangan ini umurnya telah mencapai 20 tahun tetapi masih tren bagi para *attacker*. Cisco memprediksi pada tahun 2023 jumlah serangan DDoS akan meningkat 15,4 juta secara global.¹⁰ Kemudian pada tahun 2020 *NSFOCUS* mendeteksi 152.000 serangan *DDoS* dengan volume gabungan 386.500 TB (*terabyte*). Angka-angka ini mewakili penurunan *Year-on-Year* (YoY) masing-masing sebesar 16,16% dan 19,67%.¹¹

Salah satu contoh kasus *DDoS* di Indonesia yang terjadi belakangan ini yaitu diserangnya Website Project Multatuli pada tanggal 06 Oktober 2021 Pukul 18.00 Wib, serangan tersebut mengakibatkan situs Website <https://projectmultatuli.org> tidak dapat diakses oleh pembaca selama beberapa waktu.¹² Serangan serupa juga pernah terjadi dalam beberapa tahun terakhir, sedikitnya dalam kurun waktu Januari 2019 hingga Oktober 2021 terdapat 13 (Tiga Belas) laporan

¹⁰ Endah Octaviana Nasution dan Achmad Basuki, “Implementasi Algoritme C5 . 0 Untuk Klasifikasi Serangan DDoS,” 5.1 (2021), 389–95. hlm 390. Lihat juga Cisco, 2020. Cisco Annual Internet Report (2018–2023) White Paper. [online]. Tersedia di <https://www.cisco.com>

¹¹ NS FOCUS, 2020 *DDOS ATTACK LANDSCAPE*, 2020 <<https://nsfocusglobal.com/company-overview/resources/2020-ddos-attack-landscape-report/>>.

¹² Project Multatuli, *Kami mohon maaf. Situs kami tak bisa diakses penuh lantaran serangan DDoS sejak semalam, usai menerbitkan artikel “Tiga Anak Saya Diperkosa,” 06 Oktober, 2021* <https://twitter.com/projectm_org> [diakses 20 Oktober 2021].

gangguan system yang tercatat dalam situs Direktorat Tindak Pidana Siber (*Dittipidsiber*)¹³, adapun data yang terdapat dalam situs tersebut diperoleh dari laporan Polisi dan jumlah kasus selesai yang dilaporkan oleh *Subagbinops Ditreskrimsus* seluruh polda di Indonesia.

No	Sumber	Tahun	Data Serangan	Keterangan
1.	<i>Hackmageddon</i>	2016	-	Menyatakan bahwa DDoS attack berada dalam urutan ke 9 serangan Populer
2.	<i>Cisco Annual Internet Report (2018-2023)</i>	2020	Prediksi 15,4 juta	Prediksi serangan <i>DDoS attack</i> secara global yang akan terjadi tahun 2023
3.	<i>NSFocus</i>	2020	152.000 serangan dengan volume	Angka-angka ini mewakili penurunan Year-on-

¹³ Siber Polri, "Data Statistik Laporan Masyarakat Melalui Portal Patroli Siber," 20 Oktober, 2021, hal. 1 <<https://patrolisiber.id/statistic>> [diakses 20 Oktober 2021].

			gabungan 386.500 <i>TB</i> (<i>terabyte</i>) .	Year (YoY) masing-masing sebesar 16,16% dan 19,67%.
4.	Project Multatuli.org	2021	-	Serangan ini mengakibatkan website project multatuli mengalami gangguan selama beberapa waktu.
5.	Direktorat Tindak Pidana Siber (<i>Dittipidsiber</i>)	2019- 2021	13 Serangan	Serangan gangguan sistem

Tabel 1.1 Data serangan DDoS attack

Berdasarkan data tersebut ancaman serangan *DDoS attack* masih sangat mengkhawatirkan sehingga perlu adanya tindakan lebih lanjut untuk dapat menanggulangi ancaman serangan *DDoS attack* dimasa mendatang. Walaupun kuantitas serangannya terbilang tidak terlalu tinggi tetapi metode serangan ini efektif dan mudah digunakan untuk melumpuhkan

Website, metode serangan ini akan terus berkembang seiring berkembangnya era digital, saat ini serangan *DDoS* bukan hanya dilancarkan kepada *Website* namun juga ke perangkat elektronik yang terhubung ke jaringan Internet. Intensitas serangan yang terjadi secara fluktuatif dapat menjadi bom waktu bagi keamanan siber sehingga membuat serangan ini perlu diwaspadai serta perlu dirumuskan suatu sanksi pidana sebagai upaya untuk mencegah seseorang melakukan tindakan penyerangan dan sebagai dasar penegakan hukum terhadap tindak pidana serangan siber tersebut. Dalam hukum positif Indonesia tindakan ini termasuk tindakan melawan hukum sebagaimana diatur dalam Pasal 406 ayat (1) Kitab Undang-undang Hukum Pidana (KUHP) yang menyatakan bahwa:

“Barangsiapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, 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”.

Selain pasal tersebut terdapat aturan hukum lain yang dapat dikenakan kepada pelaku *DDoS attack* yaitu pasal 30 ayat (3) dan pasal 33 Undang-undang No. 19

Tahun 2016 tentang Perubahan atas Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Pasal 30 ayat (3) menyatakan bahwa:

“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.”

Pasal 33 menyatakan bahwa:

“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.

Aturan hukum positif yang dapat digunakan kepada pelaku tindak pidana serangan siber dengan menggunakan metode *DDoS attack* adalah pasal 30 ayat (3) dan pasal 33 Undang-undang No. 19 Tahun 2016 tentang Perubahan atas Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Celah yang dapat mendorong para pelaku untuk terus melancarkan serangan sampai saat ini yaitu karena belum adanya upaya penegakan hukum yang serius dari para penegak hukum yang dipengaruhi oleh belum jelasnya aturan hukum dan sanksi pidana *DDoS* sehingga para pelaku *DDoS* masih merasa aman dan leluasa ketika melancarkan serangan. Hal ini berbeda dengan Amerika Serikat yang sudah memiliki Hukum Siber khusus, beberapa waktu lalu pengadilan Amerika Serikat melakukan tindakan penegakan hukum terhadap pelaku kejahatan siber dengan metode *DDoS Attack*. Penegakan hukum tersebut dilakukan terhadap Austin Thomson (Nomor kasus: 3:18-CR-04775-JLS) yang dijatuhi hukuman 27 bulan penjara oleh pengadilan Distrik California Selatan karena melakukan serangkaian tindakan *Distributed Denial of Service Attack (DDoS attack)* terhadap banyak korban antara tahun 2013 dan 2014 dan dikenakan denda sebesar \$95.000 kepada salah satu korban.¹⁴

Islam sebagai Agama *rahmatanlil'alam* tentunya memiliki solusi atas tindak pidana baru yang lahir dimasa modern, solusi tersebut lahir melalui pintu ijtihad para ulama yang kemudian berperan besar dalam

¹⁴ Department of Justice U.S. Attorney's Office Southern District of California, "Utah Man Sentenced for Computer Hacking Crime," 2 July, 2019, hal. 1 <<https://www.justice.gov/usao-sdca/pr/utah-man-sentenced-computer-hacking-crime>> [diakses 21 Oktober 2021].

melahirkan kaidah-kaidah fiqh guna menjawab problematika umat islam dimasa modern khususnya dalam bidang fiqh jinayah. Menurut Ahmad Wardi Muslich, Fiqih Jinyah adalah ilmu tentang hukum syara', yang berkaitan dengan perbuatan yang dilarang (jarimah) dan hukumannya, yang diambil dari dalil-dalil yang terperinci.¹⁵ Ruang lingkup Jinayah meliputi, *Hudud, Qishas/Diyat, dan Ta'zir*. Di dalam hukum Islam, suatu perbuatan tidak dapat dihukum, kecuali jika terpenuhi semua unsur-unsurnya, baik unsur umum maupun unsur khusus. Unsur-unsur umum tersebut ialah:

1. Rukun *Syar'i* (yang berdasarkan Syara') atau disebut juga unsur formal, yaitu adanya nas Syara' yang jelas melarang perbuatan itu dilakukan dan jika dilakukan akan dikenai hukuman. Nas Syara' ini menempati posisi yang sangat penting sebagai azaz legalitas dalam hukum pidana Islam, sehingga dikenal suatu prinsip la hukma liaf'al al-uqala' qal wurud an-nass (tidak ada hukum bagi perbuatan orang yang berakal sebelum datangnya nas).

¹⁵ Muhammad Nur, *Pengantar dan Asas-asas Hukum Pidana Islam*, 2020.

2. Rukun *maddi* atau disebut juga unsure material, yaitu adanya perbuatan pidana yang dilakukan.
3. Rukun adabi yang disebut juga unsur moril, yaitu pelaku perbuatan itu dapat diminta pertanggung jawaban hukum, seperti anak kecil, orang gila atau orang terpaksa, tidak dapat dihukum.

Sedangkan unsur khusus adalah unsur-unsur tersebut berbeda-beda sesuai dengan tindak pidananya. Unsur yang terkandung di dalam pencurian tidak sama dengan unsur yang terkandung di dalam perzinahan.¹⁶ *DDoS attack* termasuk kedalam kategori *jarimah Ta'zir* karena kejahatan siber dengan metode *DDoS attack* dalam islam merupakan tindak pidana baru dan tidak ada ketentuan hukumnya dalam Al-Qur'an maupun Hadits. *Ta'zir* itu adalah hukuman atas tindakan pelanggaran dan kriminalitas yang tidak diatur secara pasti dalam hukum had. Hukuman ini berbeda-beda, sesuai dengan perbedaan kasus dan pelakunya. Dari satu segi, *Ta'zir* ini sejalan dengan hukum *Had*; yakni ia adalah tindakan yang dilakukan untuk memperbaiki perilaku manusia, dan untuk mencegah orang lain agar

¹⁶ Marsaid, *Al-Fiqh Al-Jinayah (Hukum Pidana Islam)*, ed. oleh Jauhari, 1 ed. (Palembang: RAFFAH Press, 2020).

tidak melakukan tindakan yang sama seperti itu.¹⁷ Adapun dasar hukum yang dapat digunakan dalam hal ini yaitu kaidah fiqih ke-13 (tiga belas) yang menyatakan bahwa:

الإِتْلَافُ يَسْتَوِي فِيهِ الْمُتَعَمِّدُ وَالْجَاهِلُ وَالنَّاسِي

Artinya:

“Perbuatan merusakkan barang orang lain hukumnya sama, apakah terjadi karena kesengajaan, ketidaktahuan, atau karena lupa”

Kaidah ini memberikan patokan dalam perbuatan seseorang yang melakukan perusakan, baik kepada jiwa ataupun harta orang lain. Kaidah ini juga menjelaskan bahwa barangsiapa yang merusakkan barang orang lain tanpa alasan yang benar, maka ia wajib mengganti barang yang ia rusakkan tersebut atau membayar ganti rugi kepada pemilik harta. Sama saja, apakah kerusakan tersebut terjadi karena kesengajaan olehnya, atau karena tidak tahu atau karena lupa.¹⁸ Kejahatan siber

¹⁷ *Ibid*, Marsaid.

¹⁸ Al Manhaj, “Kaidah Ke. 13 : Perbuatan Merusakkan Barang Orang Lain Hukumnya Sama,” *Al-Qawâ'id wal-Ushûl al-Jûmi'ah wal-Furûq wat-Taqâsîm al-Badi'ah an-Nâfi'ah*, karya Syaikh 'Abdur-Rahmân as-Sa'di, Tahqîq: Dr. Khâlid bin 'Ali bin Muhammad al-Musyaiqih, Dârul-Wathan, Cetakan II, Tahun 1422 H – 2001 M, hal. 1 <<https://almanhaj.or.id/2512-kaidah-ke-13-perbuatan->

dengan menggunakan metode *DDoS attack* ini pada dasarnya bertujuan untuk melakukan pengrusakan secara kepada *Website* yang diserang, serangan ini sering digunakan dalam kegiatan perang siber (*Cyberwar*) karena efektifitas serangan dalam melumpuhkan *Website* sangat tinggi. Adapun kaidah ke-13 diatas adalah kaidah yang menjelaskan larangan untuk melakukan perbuatan pengrusakan terhadap barang orang lain maka secara tersurat maupun tersirat kaidah ini dapat digunakan sebagai dasar hukum dalam tindak pidana *DDoS attack* terhadap *Website*.

Pelaku *DDoS attack* secara keseluruhan telah memenuhi unsur-unsur yang telah disebutkan diatas, hal ini didasarkan pada alasan berikut; Pertama, bahwa tindakan ini telah dilarang berdasarkan kaidah fiqih ke-13 (tiga belas) sehingga unsur Rukun syar'i terpenuhi secara jelas. Kedua, tindakan ini nyata adanya hal ini didasarkan atas data-data serangan siber yang terjadi dan tindakan ini dapat dilakukan oleh siapa saja yang mempunyai keahlian dalam bidang komputer atau system elektronik sehingga rukun maddi (unsur material) terpenuhi. Ketiga, tindakan ini hanya dapat dilakukan oleh orang yang memiliki keahlian dalam bidang Komputer atau system elektronik, yang mana keahlian tersebut hanya dimiliki oleh orang dewasa,

[merusakkan-barang-orang-lain-hukumnya-sama.html](#)> [diakses 18 September 2021].

bukan orang dalam gangguan jiwa (ODGJ), dan tindakan ini dilakukan dengan tidak terpaksa (unsur adabi), berdasarkan alasan-alasan tersebut maka pelaku tindakan *DDoS attack* dapat diminta pertanggungjawaban hukum.

Berdasarkan hukum positif, kaidah fiqih dan unsur-unsur dalam hukum Islam yang telah dijelaskan diatas maka hukum positif dan fiqih jinayah dapat berkontribusi atas kekosongan hukum yang terjadi saat ini yaitu belum adanya rumusan sanksi pidana kejahatan siber dengan metode *DDoS attack* terhadap *Website*. Maka dari itu, berdasarkan latar belakang diatas menarik minat penulis untuk menyusun skripsi dengan judul **“Analisis Hukum Positif dan Fiqih Jinayah Tentang Sanksi Pidana Kejahatan Siber Dengan Metode *DDoS Attack* Terhadap *Website*”**

B. Rumusan Masalah

Berdasarkan latar belakang masalah diatas maka pokok permasalahan penelitian ini adalah sebagai berikut:

1. Bagaimana analisis Hukum Positif tentang sanksi pidana kejahatan siber dengan metode *DDoS Attack* terhadap *Website*?
2. Bagaimana analisis Fiqih Jinayah tentang sanksi pidana kejahatan siber dengan metode *DDoS Attack* terhadap *Website*?

C. Tujuan dan Manfaat Penelitian

1. Tujuan Penelitian:

- a) Untuk mengetahui analisis Hukum Positif tentang sanksi pidana kejahatan siber dengan metode *DDoS Attack* terhadap *Website*.
- b) Untuk mengetahui analisis Fiqih Jinayah tentang sanksi pidana pelaku *DDoS Attack* terhadap *Website*.

2. Manfaat Penelitian:

- a) Manfaat teoritis, penelitian ini diharapkan dapat berguna dalam memperkaya kajian Hukum Pidana Islam, Khususnya di bidang Fiqih kontemporer yang berkaitan dengan Hukum serangan siber dengan metode *Distributed Denial of Service Attack (DDoS attack)* terhadap *Website*.
- b) Manfaat Praktis, untuk selanjutnya penelitian ini dapat bermanfaat bagi:
 - 1) Pemerintah, pemerintah dapat meninjau kembali aturan hukum terkait tindak pidana serangan siber dengan metode *Distributed Denial of Service Attack (DDoS attack)* terhadap *Website*.
 - 2) Mahasiswa, penelitian ini dapat dijadikan sebagai rujukan bagi mahasiswa lain

dalam melakukan penelitian lanjutan terkait dengan serangan siber sehingga dapat mendorong terciptanya pembaharuan hukum yang beriringan dengan kemajuan teknologi.

- 3) Masyarakat, penelitian ini kiranya dapat memberikan kejelasan terkait sanksi pidana serangan siber dengan metode *DDoS attack* terhadap *Website*, sehingga masyarakat dapat melakukan upaya hukum jika menjadi korban serangan siber dengan jenis tindak pidana serangan siber tersebut.

D. Tinjauan Pustaka

Dalam mendukung penelitian ini, penulis menggunakan beberapa karya tulis ilmiah berupa skripsi, jurnal dan Website yang pernah ditulis oleh para penulis sebelumnya yang berkaitan dengan penulisan judul skripsi ini sebagai rujukan. Meskipun berkaitan, terdapat perbedaan sudut pandang, objek pembahasan, judul maupun pokok masalah kajian terhadulu sehingga tidak terdapat kesamaan didalam penyusunan skripsi ini. Beberapa penelitian yang diteliti oleh para penulis terdahulu yang dijadikan skripsi, diantaranya yaitu:

1. Thesis karya Iswandi Walad, Mahasiswa Program Studi S2 Teknik Informatika Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara Tahun 2020 yang berjudul “*Analisis Denial Of Service Attack Pada Sistem Keamanan Web*” Thesis ini membahas mengenai serangan Denial of Service attack (*DoS*) pada system keamanan web dengan metode serangan *DoS type SYN Attack, Ping of Death, Land Attack, Smurf Attack dan UDP Flood*. Persamaan Thesis ini dengan penelitian yang akan dilakukan penulis adalah mengenai jenis serangan yang digunakan yang mana DoS merupakan bentuk awal dari serangan DDoS, selain itu juga persamaan lainnya yaitu dalam hal objek serangannya yaitu keamanan web. Perbedaan Thesis ini dengan penelitian yang akan ditulis dalam penelitian ini yaitu dalam hal focus pembahasan yang mana dalam Thesis tersebut hanya berfokus kepada metode serangan *DoS* pada system keamanan web sedangkan penelitian yang akan dilakukan adalah menganalisa sanksi hukuman atas kejahatan siber dengan metode serangan *DDoS attack terhadap website*.
2. Skripsi karya Risky Arfah, Mahasiswa Fakultas Syariah dan Hukum UIN Sumatera Utara tahun 2019 yang berjudul “*Sanksi Tindak Pidana Hacking (Studi Analisis Undang-undang ITE dan Hukum Pidana Islam)*”. Skripsi ini membahas tentang sanksi tindak pidana hacking secara umum berdasarkan seluruh

jenis *Cybercrime* kemudian ditinjau menggunakan Undang-undang ITE dan Hukum Pidana Islam. Persamaan skripsi ini dengan penelitian yang akan dilakukan penulis adalah sama-sama meneliti mengenai sanksi tindak pidana hacking dalam perspektif hukum positif dan hukum Islam. Perbedaan skripsi ini dengan penelitian yang akan ditulis oleh penulis yaitu dalam hal ruang lingkup dan jenis tindakan *Cybercrime*, yang mana penulis memfokuskan pembahasan kepada jenis tindakan *DDos attack* terhadap Website guna menemukan rumusan sanksi pidana yang tepat berdasarkan dasar hukum yang jelas.

3. Skripsi M. Ade Cairuddin Najib, Mahasiswa Fakultas Syariah dan Hukum UIN Raden Fatah Palembang tahun 2018 yang berjudul "*Sanksi Terhadap Tindak Pidana Defacing Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Dengan Perspektif Hukum Islam*". Skripsi ini membahas tentang sanksi pidana terhadap tindak pidana Cybercrime dengan metode defacing kemudian ditinjau menggunakan undang-undang Nomor 19 Tahun 2016 dan Hukum Islam. Persamaan skripsi ini dengan penelitian yang akan dilakukan penulis terletak dalam penggunaan tinjauan hukum sama-sama menggunakan tinjauan hukum positif berupa Undang-undang ITE. Perbedaan skripsi ini dengan penelitian yang akan ditulis penulis adalah terkait dengan

tindakan yang dilakukan oleh pelaku *Cybercrime*, dalam skripsi ini tindakan yang dianalisis adalah tindakan Defacing sedangkan penulis akan membahas tentang sanksi pidana tindakan *DDos attack* terhadap *Website*.

4. Jurnal Hukum yang ditulis oleh Rizka Cahaya Putri dan Lushiana Primasari Mahasiswa Fakultas Hukum Universitas Sebelas Maret, berjudul "*Tindak Pidana siber dengan Modus Distributed Denial Of Service Attack For Bitcoin dalam Pengaturan Hukum di Indonesia*". Pembahasan dalam jurnal ini yaitu mengenai analisis tindak pidana siber dengan modus *DDos attack for Bitcoin* yang didalamnya memuat tentang mekanisme penyerangan menggunakan modus *DDoS Attack* untuk kemudian menyerang e-mail korban dan meminta tebusan berupa Bitcoin, Pembahasan selanjutnya yaitu mengenai rumusan hukum positif Indonesia yang dapat dikenakan kepada pelaku *DDos for Bitcoin*. Penelitian yang dimuat di *Reclidive* jurnal ini memberikan kesimpulan bahwa pengaturan hukum pidana di Indonesia belum dapat mengatur secara tegas mengenai tindak pidana siber dengan modus *Distributed Denial Of Service Attack For Bitcoin*. Pengaturan hukum pidana yang berlaku hanya menyatakan secara implisit mengenai tindak pidana siber *DDoS attack for Bitcoin*, sehingga peraturan-peraturan tersebut tidak bisa dijadikan pedoman secara terus menerus mengingat suatu

kejahatan pasti akan selalu berkembang dengan modus dan sarana teknologi yang lebih canggih. Persamaan penelitian ini dengan penelitian yang akan dilakukan penulis adalah mengenai modus/metode tindak pidana yang dilakukan pelaku kejahatan yaitu metode serangan siber *DDos Attack*. Perbedaan penelitian ini dengan penelitian yang akan dilakukan penulis adalah mengenai objek serangannya, yang mana objek serangan dalam penelitian ini adalah *e-mail* sedangkan objek serangan yang akan dibahas oleh penulis adalah *Website*.

5. Artikel Hukum yang ditulis oleh Abdul Rahim Wahab, Faris Ali Sidqi dan M. Yursan Bin Darham Mahasiswa Universitas Islam Kalimantan (UNISKA), Artikel Hukum tersebut berjudul "*Analisis Yuridis Tentang Pertanggungjawaban Pidana Terhadap Pelaku cybercrime*". Artikel ini membahas tentang ketentuan hukum tentang tindak pidana *cyber crime* di Indonesia dan membahas tentang bentuk pertanggungjawaban pidan pelaku *cyber crime*. Persamaan Artikel Hukum ini dengan penelitian yang akan dilakukan dalam penelitian ini yaitu tentang penggalan ketentuan hukum untuk mengetahui ketentuan hukum mana saja yang dapat dikenakan kepada pelaku *cyber crime*. Perbedaan Artikel Hukum ini dengan penelitian yang akan dilakukan oleh penulis yaitu dalam ruang lingkup pembahasan *cyber crime*, yang mana penulis dalam penelitian ini memfokuskan pembahasan pada salah

satu metode serangan yang dilakukan untuk melakukan tindakan *cyber crime*, serta mengklasifikasikan sanksi pidana berdasarkan jenis serangan yang dilakukan.

E. Metode Penelitian

1. Jenis Penelitian

Penelitian merupakan kegiatan pemeriksaan, penyelidikan, pengumpulan, pengolahan, analisis dan penyajian data yang dilakukan secara sistematis dan objektif untuk memecahkan suatu permasalahan / menguji suatu hipotesis untuk mengembangkan prinsip-prinsip umum.¹⁹ Jenis penelitian yang digunakan penulis dalam penyusunan skripsi ini adalah penelitian Hukum Kualitatif.

2. Sumber Data

Jenis data yang digunakan adalah jenis data kualitatif, data kualitatif adalah data yang tidak berbentuk angka, melainkan suatu uraian atau penjelasan yang menggambarkan tentang keadaan, proses atau peristiwa tertentu. Data yang dianalisis

¹⁹ Suteki dan Galang Taufani, *Metodologi Penelitian Hukum (Filsafat, Teori, dan Praktik)*, 3 ed. (Depok: Raja Grafindo Persada, 2020).

adalah Kitab Undang-undang Hukum Pidana, Undang-undang Nomor 19 Tahun 2016 dan Fiqih Jinayah terhadap pelaku tindak pidana *DDoS attack* terhadap *Website*. Kemudian sumber data yang digunakan adalah sebagai berikut;

- 1) Data primer: yaitu data yang bersifat mengikat dan merupakan data pokok yaitu:
 - a. Kitab Undang-undang Hukum Pidana (KUHP)
 - b. Undang-undang Nomor 19 Tahun 2016 Tentang
 - c. Kitab *Al-Qawâ'id wal-Ushûl al -Jûmi'ah wal-Furûq wat-Taqâsîm al-Badî'ah an-Nâfi'ah*, karya Syaikh 'Abdur-Rahmân as-Sa'di, Tahqîq: Dr. Khalid bin 'Ali bin Muhammad al-Musyaiqih, Dârul-Wathan, Cetakan II.
- 2) Data sekunder: Merupakan bahan-bahan hukum yang diambil dari pendapat atau tulisan para ahli dalam bidang *DDoS attack* dan Fiqih Jinayah, adapun data yang digunakan adalah data yang memberikan penjelasan mengenai data primer sehingga membuat data primer menjadi jelas.
- 3) Data tersier, yaitu data yang memberikan petunjuk maupun penjelasan terhadap data primer dan skunder, seperti kamus hukum, terminology dan lain sebagainya.

3. Metode Pengumpulan Data

Guna mencari kebenaran dari sebuah laporan ilmiah maka metode pengumpulan data yang akan digunakan penulis adalah metode dokumentasi/studi pustaka yakni mencari data mengenai hal-hal berupa catatan, transkrip, jurnal, buku, surat kabar, majalah, notulen, agenda dan lain sebagainya yang berhubungan dengan penelitian penulis.

4. Metode Analisis Data

Proses analisis merupakan hal yang penting dalam memecahkan masalah penelitian dan mencapai tujuan akhir penelitian, analisis dilakukan setelah proses pengelompokan atau pengumpulan data.²⁰ Metode Analisis data yang akan digunakan oleh penulis dalam melakukan penelitian ini adalah metode deskriptif yaitu mendeskripsikan data yang diperoleh sehingga tergambar objek permasalahan secara jelas dan terperinci dan menghasilkan pemahaman yang konkrit dan jelas. Sedangkan alur berfikir yang digunakan dalam penelitian ini adalah alur deduktif yaitu penelitian yang berangkat dari

²⁰ Joko Subagyo, *Metode Penelitian dalam Teori dan Praktek* (Jakarta: PT. Rineka Cipta, 2006).

factor yang bersifat umum kemudian ditarik kedalam factor yang bersifat khusus.

F. Sistematika Penulisan

Guna mempermudah dalam memahami materi penelitian ini, dan sebagai gambaran dari seluruh bab, maka perlu dikemukakan sistematika pembahasan dalam penelitian ini yaitu sebagai berikut:

Bab pertama merupakan pendahuluan yang meliputi latar belakang masalah, rumusan masalah, tujuan dan manfaat penelitian, landasan teori, kajian terdahulu, metode penelitian, dan sistematika penulisan.

Bab kedua merupakan pembahasan tentang kerangka teoritis atau kerangka konseptual yang memuat tentang tinjauan *cybercrime* dengan metode *DDoS attack* yang berisi definisi *cybercrime*, bentuk-bentuk *cybercrime*, unsur-unsur *cybercrime* dengan metode *DDoS attack*, sanksi pidana *cybercrime* dalam hukum positif yang berisi tentang pengertian, asas, dan unsur tindak pidana, bentuk dan sanksi *cybercrime* dalam hukum positif, kemudian sanksi pidana *cybercrime* dalam fiqh jinayah yang berisi tentang pengertian fiqh jinayah, asas hukum pidana islam, unsur tindak pidana dalam fiqh jinayah, syarat penerapan jarimah, bentuk dan sanksi pidana dalam fiqh jinayah, sanksi pidana *cybercrime* dengan metode *DDoS attack* dalam fiqh jinayah.

Bab ketiga merupakan pembahasan tentang *cybercrime* dengan metode *Distributed Denial of Service attack (DDoS attack)* terhadap Website, yang memuat tentang pengertian *cybercrime*, *cybercrime* dengan metode *DDoS attack*, factor terjadinya tindak pidana, factor penyebab terjadinya serangan *DDoS attack*, jenis metode serangan (*DDoS attack*), data serangan *DDoS attack*, kemudian memuat pembahasan tentang Website sebagai target serangan *DDoS attack* yang berisi tentang definisi Website, struktur Website, dan akibat serangan *DDoS attack* terhadap Website.

Bab keempat adalah pembahasan yang memuat tentang analisis sanksi pidana *Distributed Denial of Service Attack (DDoS Attack)* terhadap Website menurut hukum positif, analisis sanksi pidana *Distributed Denial of Service Attack (DDoS Attack)* terhadap Website menurut Fiqih Jinayah, dan persamaan dan perbedaan sanksi pidana *Distributed Denial of Service Attack (DDoS Attack)* terhadap Website menurut Hukum Positif dan Fiqih Jinayah.

Bab kelima adalah penutup yang memuat kesimpulan dan saran.

BAB II
TINJAUAN UMUM SANKSI PIDANA KEJAHATAN
SIBER DALAM HUKUM POSITIF DAN FIQH
JINAYAH

**A. Kejahatan Siber (*Cybercrime*) Dengan Metode
*DDoS Attack***

1. Definisi Kejahatan Siber (*Cybercrime*)

Pada Kongres PBB ke X tahun 2000, definisi dari *cybercrime* dibagi dua, yaitu pengertian sempit, yaitu: *“any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them”*. jika diartikan kedalam Bahasa Indonesia memiliki arti: kejahatan ini merupakan perbuatan bertentangan dengan hukum yang langsung berkaitan dengan sarana elektronik dengan sasaran pada proses data dan sistem keamanan komputer. Selanjutnya dalam pengertian yang lebih luas, *cybercrime* didefinisikan sebagai : *“any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network”*. Artinya, perbuatan yang melawan hukum dengan menggunakan sarana atau berkaitan dengan sistem atau jaringan komputer termasuk kejahatan memiliki secara illegal,

menawarkan atau mendistribusikan informasi melalui sarana sistem atau jaringan komputer. Selain itu, *cybercrime* dapat juga diartikan sebagai “*crime related to technology, computers, and the internet*”. Artinya, kejahatan yang berkaitan dengan teknologi, komputer dan internet.²¹

2. Bentuk-bentuk Kejahatan Siber (*Cybercrime*)

Cybercrime terbagi kedalam 7 (tujuh) bentuk kejahatan yaitu sebagai berikut:

1) *Unauthorized Access to Computer System and Service*

Kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.

²¹ Peresensi M Jamil, “*Resensi : “ Cyber Crime (Akar Masalah , Solusi , Dan Penanggulangannya)*”,” April 2010, 2017, 1–14.

2) *Illegal Contents*

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Misalnya pemuatan suatu berita bohong atau fitnah yang mendiskreditkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan lain sebagainya.

3) *Data Forgery*

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi “salah ketik” yang pada akhirnya akan menguntungkan pelaku.

4) *Cyber Espionage*

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya

tersimpan dalam suatu sistem yang *computerized*.

5) *Cyber Sabotage and Extortion*

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, *virus* komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber-terrorism*.

6) *Offense against Intellectual Property*

Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di

internet yang ternyata merupakan rahasia dagang orang lain.

7) *Infringement of Privacy*

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materiil maupun immateriil, seperti nomor kartu kredit, nomor PIN ATM, informasi penyakit yang dirahasiakan dan sebagainya.²²

3. Unsur-unsur Kejahatan Siber (*Cybercrime*) Dengan Metode *DDoS Attack*

Kejahatan siber dengan metode *DDoS attack* memiliki unsur-unsur tertentu sehingga metode serangan ini dapat dikategorikan sebagai kejahatan siber (*Cybercrime*) adapun unsur-unsur tersebut adalah sebagai berikut:

- 1) Menggunakan komputer dan jaringan *Internet* sebagai alat

²² *Op Cit*, M. Naufal dan M. Sofwan Jannah, "Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif Dan Hukum Islam," *Al-Mawarid Journal of Islamic Law*, 12.1 (2012), 69–84.

- 2) *DDoS attack* dilakukan dalam lingkup *Cyberspace*
- 3) *DDoS attack* bersifat melawan hukum
- 4) *DDoS attack* bersifat merugikan
- 5) *DDoS attack* termasuk kedalam *Cyberextortion*

B. Tindak Pidana Kejahatan Siber Dalam Hukum Positif

1. Pengertian, Asas, dan Unsur Tindak Pidana

a. Pengertian Tindak Pidana

Istilah tindak pidana dalam Bahasa Indonesia berasal dari bahasa Belanda yaitu “*strafbaar feit*”. Pembentuk undang-undang menggunakan kata “*strafbaar feit*” untuk menyebut apa yang di kenal sebagai “tindak pidana” tetapi dalam Undang-Undang Hukum Pidana tidak memberikan suatu penjelasan mengenai apa sebenarnya yang dimaksud dengan perkataan “*strafbaar feit*”. Para pembentuk undang-undang tidak memberikan suatu penjelasan mengenai apa yang sebenarnya dimaksud dengan kata “*strafbaar feit*”, maka timbullah doktrin berbagai pendapat mengenai apa sebenarnya maksud dari kata “*strafbaar feit*”.²³

²³ Andi Sofyan dan Nur Azisa, *Buku Ajar Hukum Pidana*, 1 ed. (Makasar: Pustaka Pena Press, 2020) <<https://doi.org/10.21070/2020/978-623-6833-81-0>>.

Muljatno, mengatakan bahwa perbuatan pidana adalah perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, bagi barangsiapa yang melanggar larangan tersebut. Dapat juga dikatakan bahwa perbuatan pidana adalah perbuatan yang oleh suatu aturan hukum dilarang dan diancam pidana, asal saja dalam pada itu diingat bahwa larangan ditunjukkan kepada perbuatan (yaitu suatu keadaan atau kejadian yang ditimbulkan oleh kelakuan orang), sedangkan ancaman pidananya ditujukan kepada orang yang menimbulkan kejadian itu. Antara larangan dan ancaman pidana ada hubungan yang erat, oleh karena antara kejadian dan orang yang menimbulkan kejadian itu ada hubungan yang erat pula. Yang satu tidak dapat dipisahkan dari yang lain. Kejadian tidak dapat dilarang, jika yang menimbulkan bukan orang, dan orang tidak dapat diancam pidana, jika tidak karena kejadian yang ditimbulkan olehnya. Dan justru untuk menyatakan hubungan yang erat itu, maka di pakailah perkataan perbuatan, yaitu suatu pengertian abstrak yang menunjuk kepada kedua keadaan konkrit: pertama, adanya kejadian yang

tertentu, dan kedua, adanya orang yang berbuat, yang menimbulkan kejadian itu.²⁴

Barda Nawawi Arief, menyatakan bahwa tindak pidana hanya membahas perbuatan secara objektif, sedangkan hal-hal yang bersifat subjektif terkait dengan sikap batin pembuat tindak pidana harus dikeluarkan dari pengertian tindak pidana, karena sikap batin pembuat termasuk dalam lingkup kesalahan dan pertanggungjawaban pidana yang menjadi dasar etik dapat dipidananya si pembuat. Pemisahan tindak pidana dan pertanggungjawaban pidana bertujuan untuk memberikan kedudukan seimbang dalam penjatuhan pidana berdasarkan prinsip *daad en dader strafrecht* yang memerhatikan keseimbangan monodualistik antara kepentingan individu dan masyarakat. Artinya, walaupun telah melakukan tindak pidana, tetapi pembuatnya tidak diliputi kesalahan, oleh karenanya tidak dapat dipertanggungjawabkan. Sifat perbuatan yang dilarang mengandung pengertian bahwa tindak pidana didasarkan pada asas legalitas sebagai dasar utama yang menempatkan perbuatan

²⁴ Suyanto, *Pengantar Hukum Pidana*, 1 ed. (Yogyakarta: deepublish, 2018).

dengan ancaman sanksi sebagai perbuatan yang bersifat melawan hukum.²⁵

Simons, menerangkan bahwa “*strafbaar feit*” adalah kelakuan (*handeling*) yang diancam dengan pidana, yang bersifat melawan hukum, yang berhubungan dengan kesalahan dan yang dilakukan oleh orang yang mampu bertanggung jawab.²⁶

Van hamel, merumuskan “*strafbaar feit*” sebagai kelakuan orang (*menselijke gedraging*) yang dirumuskan dalam wet, yang bersifat melawan hukum, yang patut dipidana (*strafwaardig*) dan dilakukan dengan kesalahan.²⁷

Pompe, menerangkan bahwa “*strafbaar feit*” merupakan suatu pelanggaran norma yang tidak hanya dilakukan dengan sengaja tetapi dapat juga dilakukan dengan tidak sengaja. Sebagai contoh pelanggaran norma yang dilakukan dengan sengaja dirumuskan dalam Pasal 338 KUHP yaitu “Barangsiapa dengan sengaja menghilangkan nyawa orang lain, karena bersalahnya telah melakukan pembunuhan

²⁵ Lukman Hakim, *Asas-Asas Hukum Pidana*, 1 ed. (Jakarta: deepublish publisher, 2020).

²⁶ *Op Cit*, Suyanto. *Pengantar Hukum Pidana*..

²⁷ *Ibid*, Suyanto.

dihukum dengan hukuman penjara selamanya lima belas tahun”.²⁸

b. Asas-asas Hukum Pidana

Pengertian asas dalam kamus besar bahasa Indonesia (KBBI) diartikan sebagai dasar sesuatu yang menjadi tumpuan berpikir atau berpendapat. Setiawan Widagdo dalam bukunya yang berjudul Kamus Hukum memberikan pengertian asas adalah sebagai suatu alam pikiran yang dirumuskan secara luas dan mendasari adanya norma hukum.²⁹ Dalam hukum pidana terdapat beberapa asas yang menjadi dasar pemahaman hukum pidana, asas-asas tersebut adalah sebagai berikut:

a) Asas Legalitas

Asas legalitas dalam Hukum Pidana Indonesia diatur dalam Pasal 1 ayat (1) KUHP, yang menentukan “suatu perbuatan tidak dapat dipidana, kecuali berdasarkan kekuatan perundang-undangan pidana yang telah ada”. Syarat pertama untuk menindak terhadap suatu perbuatan yang tercela, yaitu adanya ketentuan dalam undang-undang

²⁸ *Op Cit*, Sofyan dan Azisa. Buku Ajar Hukum Pidana.

²⁹ Setiawan Widagdo, *Kamus Hukum*, ed. oleh Umi Athelia Kurniati, 1 ed. (Jakarta: PT. Prestasi Pustaka Raya, 2012).

pidana yang merumuskan perbuatan yang tercela itu dan memberikan suatu sanksi terhadapnya.³⁰

Menurut Machteld Boot, asas legalitas mengandung beberapa syarat: pertama, *nullum crimen, noela poena sine lege praevia*, yang berarti, tidak ada perbuatan pidana, tidak ada pidana tanpa undang-undangsebelumnya. Konsekuensi dari makna ini adalah menentukan bahwa hukum pidana tidak boleh berlaku surut. Kedua, *nullum crimen, noela poena sine lege scripta*, artinya, tidak ada perbuatan pidana, tidak ada perbuatan pidana tanpa undang-undang tertulis. Konsekuensi dari makna ini, adalah bahwa semua perbuatan pidana harus tertulis. Ketiga, *nullum crimen, noela poena sine lege certa*, artinya tidak ada perbuatan pidana, tidak ada pidana tanpa aturan undang-undang yang jelas. Konsekuensi dari makna ini, adalah harus jelasnya rumusan perbuatan pidana sehingga tidak bersifat multitafsir yang dapat membahayakan kepastian hukum. Keempat, *nullum crimen, noela poena sine lege stricta*, artinya tidak ada perbuatan

³⁰ *Op Cit*, Lukman Hakim. Asas-asas hukum Pidana

pidana, tidak ada pidana tanpa undang-undang yang ketat. Konsekuensi dari makna ini secara implisit adalah tidak diperbolehkannya analogi. Ketentuan pidana harus ditafsirkan secara ketat, sehingga tidak menimbulkan perbuatan pidana baru.³¹

- b) Asas Tiada Pidana Tanpa Kesalahan (*Geen Straf Zonder Schuld, Actus non facit reum nisi mens sist rea*)

Asas tiada pidana tanpa kesalahan atau yang lebih dikenal sebagai asas dualistis ini berhubungan dengan masalah pertanggungjawaban dalam hukum pidana yang dilandaskan pada presumsi bahwa *schuld* tidak dapat dimengerti tanpa adanya melawan hukum (*wederrechtelijke*), tapi sebaliknya, melawan hukum mungkin tanpa adanya kesalahan. Berdasarkan asas ini, meskipun seseorang telah melakukan perbuatan pidana dan telah memenuhi unsur-unsur yang dirumuskan dalam delik, perlu dibuktikan pula apakah dia dapat dipertanggungjawabkan atau tidak atas

³¹ *Ibid* Hakim.

perbuatannya tersebut, artinya apakah dia mempunyai kesalahan atau tidak.³²

c) Asas Tidak Berlaku Surut

Asas tidak berlaku surut atau dikenal juga dengan istilah “*nonretroaktif*” ini merupakan asas undang-undang hukum pada umumnya dan juga merupakan asas hukum pidana sebagaimana tercantum dalam Pasal 1 ayat 1 Kitab Undang-Undang Hukum Pidana (KUHP) yang berbunyi:

“suatu perbuatan tidak dapat dipidana, kecuali berdasarkan kekuatan ketentuan perundang-undangan pidana yang telah ada”.

Selain itu asas ini juga disebutkan dalam pasal 28I ayat (1) Undang-undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945) yang berbunyi:

“Hak untuk hidup, hak untuk tidak disiksa, hak kemerdekaan pikiran dan hati nurani, hak beragama, hak untuk tidak diperbudak, hak untuk diakui sebagai pribadi di

³² *Ibid* Hakim.

*hadapan hukum, dan hak untuk tidak dituntut atas dasar hukum yang berlaku surut adalah hak asasi manusia yang tidak dapat dikurangi dalam keadaan apapun”.*³³

c. Unsur-unsur Tindak Pidana

Unsur-unsur tindak pidana menurut Moeljatno terdiri dari:

- 1) Kelakuan dan akibat
- 2) Hal ikhwal atau keadaan tertentu yang menyertai perbuatan, yang dibagi menjadi:
 - a) Unsur subyektif atau pribadi, yaitu mengenai diri orang yang melakukan perbuatan, misalnya unsur pegawai negeri yang diperlukan dalam delik jabatan seperti dalam perkara tindak pidana korupsi. Pasal 418 KUHP jo. Pasal 1 ayat (1) sub c UU No. 3 Tahun 1971 atau pasal 11 UU No. 31 Tahun 1999 jo. UU No. 20 Tahun 2001 tentang pegawai negeri yang menerima hadiah. Kalau yang menerima hadiah bukan pegawai

³³ *Ibid* Hakim.

negeri maka tidak mungkin diterapka pasal tersebut.

- b) Unsur obyektif atau non pribadi, yaitu mengenai keadaan di luar si pembuat, misalnya pasal 160 KUHP tentang penghasutan di muka umum (supaya melakukan perbuatan pidana atau melakukan kekerasan terhadap penguasa umum). Apabila penghasutan tidak dilakukan di muka umum maka tidak mungkin diterapkan pasal ini.³⁴

Menurut Lamintang unsur obyektif itu adalah unsur yang ada hubungannya dengan keadaan-keadaan, yaitu di dalam keadaan-keadaan mana tindakan-tindakan dari si pelaku itu harus dilakukan. Unsur obyektif itu meliputi³⁵:

- a) Perbuatan manusia terbagi atas perbuatan yang bersifat positif dan bersifat negatif yang menyebabkan suatu pelanggaran pidana. Sebagai contoh perbuatan yang bersifat positif yaitu pencurian (Pasal 362 KUHP),

³⁴ Takdir, *Mengenal Hukum Pidana*, ed. oleh Tahmid Nur, 1 ed. (Sulawesi selatan: Penerbit Laskar Perubahan, 2013).

³⁵ *Op Cit* Sofyan dan Azisa. *Buku Ajar Hukum Pidana*..

penggelapan (Pasal 372 KUHP), pembunuhan (Pasal 338 KUHP), dan sebagainya. Sedangkan contoh perbuatan negatif yaitu tidak melaporkan kepada pihak yang berwajib padahal dia mengetahui ada komplotan untuk merobohkan negara (Pasal 165 KUHP), membiarkan orang dalam keadaan sengsara, sedangkan ia berkewajiban memberikan pemeliharaan kepadanya (Pasal 304 KUHP). Terkadang perbuatan positif dan negatif terdapat dengan tegas di dalam norma hukum pidana yang dikenal dengan delik formil. Dimana pada delik formil yang diancam hukuman adalah perbuatannya seperti yang terdapat pada Pasal 362 KUHP dan Pasal 372 KUHP, sedangkan terkadang pada suatu pasal hukum pidana dirumuskan hanya akibat dari suatu perbuatan saja diancam hukuman, sedangkan cara menimbulkan akibat itu tidak diuraikan lebih lanjut, delik seperti ini disebut sebagai delik materil yang terdapat pada Pasal 338 KUHP.

- b) Akibat perbuatan manusia, yaitu akibat yang terdiri atas merusaknya atau membahayakan kepentingan-kepentingan hukum, yang menurut norma hukum pidana itu perlu ada supaya dapat dipidana. Akibat ini ada yang timbul seketika bersamaan dengan perbuatannya, misalnya dalam pencurian hilangnya barang timbul seketika dengan perbuatan mengambil, akan tetapi ada juga bahwa akibat itu timbulnya selang beberapa waktu, kadang-kadang berbeda tempat dan waktu dari tempat dan waktu perbuatan itu dilakukan misalnya dalam hal pembunuhan, perbuatan menembak orang yang dibunuh misalnya telah dilakukan pada tempat dan waktu yang tertentu, akan tetapi matinya (akibat) orang itu terjadi baru selang beberapa hari dan di lain tempat.
- c) Keadaan-keadaannya sekitar perbuatan itu, keadaan-keadaan ini biasa terdapat pada waktu melakukan perbuatan, misalnya dalam Pasal 362 KUHP keadaan: “bahwa barang yang dicuri itu kepunyaan orang lain”

adalah suatu keadaan yang terdapat pada waktu perbuatan “mengambil” itu dilakukan, dan bisa juga keadaan itu timbul sesudah perbuatan itu dilakukan, misalnya dalam Pasal 345 KUHP, keadaan : “jika orang itu jadi membunuh diri” adalah akibat yang terjadi sesudah penghasutan bunuh diri itu dilakukan.

- d) Sifat melawan hukum dan sifat dapat dipidana. Perbuatan itu melawan hukum, jika bertentangan dengan undang-undang. Pada beberapa norma hukum pidana unsur “melawan hukum” ini dituliskan tersendiri dengan tegas di dalam satu pasal, misalnya dalam Pasal 362 KUHP disebutkan: “memiliki barang itu dengan melawan hukum (melawan hak)”. Sifat dapat dipidana artinya bahwa perbuatan itu harus diancam dengan pidana, oleh suatu norma pidana yang tertentu. Sifat dapat dipidana ini bisa hilang, jika perbuatan itu, walaupun telah diancam pidana dengan undang-undang tetapi telah dilakukan dalam keadaan.

Adapun unsur-unsur tindak pidana menurut pengertian Rancangan KUHP Nasional adalah:

1. Unsur-unsur formal :
 - a) Perbuatan sesuatu;
 - b) Perbuatan itu dilakukan atau tidak dilakukan;
 - c) Perbuatan itu oleh peraturan perundang-undangan dinyatakan sebagai perbuatan terlarang;
 - d) Peraturan itu oleh peraturan perundang-undangan diancam pidana
2. Unsur-unsur materil:

Perbuatan itu harus bersifat bertentangan dengan hukum, yaitu harus benar-benar dirasakan oleh masyarakat sebagai perbuatan yang tidak patut dilakukan.³⁶

³⁶ *Ibid*, Sofyan dan Azisa. *Buku Ajar Hukum Pidana*.

2. Bentuk dan Sanksi Pidana Kejahatan Siber Dalam Hukum Positif

a. Bentuk dan Sanksi Pidana dalam Hukum Positif

Berdasarkan Pasal 10 Kitab Undang-Undang Hukum Pidana (KUHP) membagi sanksi pidana menjadi dua yaitu, pidana pokok dan pidana tambahan. Pidana pokok terdiri atas pidana mati, pidana penjara, kurungan, dan denda. Kemudian pidana tambahan terdiri atas pencabutan hak-hak tertentu, perampasan barang-barang tertentu, pengumuman putusan hakim.³⁷

Pidana pokok terdiri atas 5 (lima) jenis pidana yaitu:

- a) Pidana mati
- b) Pidana Penjara
- c) Kurungan
- d) Denda

³⁷ Moeljatno, *Kitab Undang-Undang Hukum Pidana* (Jakarta: PT. Bumi Aksara, 2014).

Pidana tambahan terdiri atas 3 (tiga) jenis pidana yaitu:

- a) Pencabutan hak-hak tertentu
- b) Perampasan barang-barang tertentu
- c) Pengumuman putusan hakim

b. Delik Dan Sanksi Pidana Kejahatan Siber Dengan Metode *DDoS Attack* Dalam Kitab Undang-Undang Hukum Pidana (KUHP) Serta Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Barda Nanawi Arief memberikan kategori *cybercrime* sebagai delik dalam empat hal yaitu sebagai berikut:

- 1) Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer termasuk di dalamnya (a) mengakses sistem komputer tanpa hak (*illegal acces*), (b) tanpa hak menangkap/mendengar pengiriman dan pemancaran (*illegal interception*), (c) tanpa hak merusak data (*data interference*), (d) tanpa hak mengganggu sistem (*system interference*),

- (e) menyalahgunakan perlengkapan (misuse of devices).
- 2) Delik-delik yang berhubungan dengan komputer berupa pemalsuan dan penipuan dengan komputer (*computer related offences : forgery and fraud*).
 - 3) Delik-delik yang bermuatan tentang pornografi anak (*content-related offences, child pornography*).
 - 4) Delik-delik yang berhubungan dengan masalah hak cipta (*offences related to infringements of copyright*).

Berdasarkan kategori delik tersebut kejahatan siber dengan metode *DDoS attack* terhadap *Website* masuk ke dalam kategori *system interference* yaitu tanpa hak mengganggu system, hal ini system yang dimaksud adalah system jaringan *Website* yang didalamnya terdapat suatu system pembentuk *Website* yang terstruktur.³⁸

Dasar Hukum yang dapat digunakan terhadap kasus *Cybercrime* yang terdapat dalam KUHP yaitu:

³⁸ *Op Cit*, Jamil. Resensi : “ *Cyber Crime (Akar Masalah , Solusi , Dan Penanggulangannya)*”

- 1) Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di Internet.
- 2) Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di Internet dengan penyelenggara dari Indonesia.
- 3) Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan email kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu mailing list sehingga banyak orang mengetahui cerita tersebut.
- 4) Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku mengetahui rahasia korban.
- 5) Pasal 362 KUHP yang dikenakan untuk kasus carding dimana pelaku mencuri nomor kartu kredit milik orang lain

walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan software card generator di Internet untuk melakukan transaksi di e-commerce. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi.

- 6) Pasal 378 KUHP dapat dikenakan untuk penipuan dengan seolah olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu website sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.³⁹
- 7) Pasal 406 ayat (1) KUHP dapat dikenakan untuk tindakan merusakkan, menghancurkan, membikin tidak dapat dipakai suatu barang. Dalam hal ini barang yang dimaksud dapat berupa perangkat elektronik, *website*, *web server* dan lain

³⁹ *Op Cit*, Naufal dan Jannah.

sebagainya.⁴⁰ Tindakan merusak, menghancurkan atau membuat tidak dipakainya suatu barang ini dapat dilakukan dengan berbagai metode serangan siber salah satunya adalah dengan melakukan serangan *Distributed Denial of Service Attack (DDoS Attack)* serangan ini pada dasarnya dilakukan dengan cara melakukan serangan yang dapat mengakibatkan *server website* kelebihan permintaan data (*Overload*) sehingga website tidak dapat diakses oleh pengguna (*down*).

Adapun dasar hukum *Cybercrime* menurut Undang-undang secara umum termuat dalam Pasal 30 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang berbunyi sebagai berikut;

- 1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses

⁴⁰ Fiorida Mathilda, "Cyber Crime Dalam Sistem Hukum Indonesia Cyber Crime in Indonesia Law System," *SIGMA-Mu - Jurnal Publikasi Hasil Penelitian dan Gagasan Ilmiah Multidisiplin*, 2.2 (2012), 34–45 <<https://jurnal.polban.ac.id/index.php/sigmamu/article/view/870>>.

- komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.
- 2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun 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 milik orang lain dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.⁴¹

Selain dapat diancam dengan pasal 30 tindakan *cybercrime* juga dapat dikenakan Pasal 33 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang menyatakan bahwa:

⁴¹ Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

“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”.

C. Sanksi Pidana Kejahatan Siber Dalam Fiqih Jinayah

1. Pengertian Fiqih Jinayah

Menurut istilah, *Jinayah* adalah semua perbuatan yang diharamkan, yaitu perbuatan yang diberi peringatan dan dilarang oleh syara' karena akan mendatangkan kemudharatan pada agama, jiwa, akal, harta dan kehormatan. Jinayah adalah *masdar* (kata asal) dari kata kerja (fi'il madhi) *janaa* yang mengandung arti suatu kerja yang diperuntukkan bagi satuan laki-laki yang telah berbuat dosa atau salah. Pelaku kejahatan itu sendiri disebut dengan *jaani* yang merupakan bentuk singular bagi satuan laki-laki atau bentuk *mufrad mudzakkar* sebagai pembuat kejahatan atau *isim fa'il*. Adapun sebutan pelaku kejahatan wanita adalah *jaaniah*, yang artinya dia (wanita) yang telah berbuat dosa. Orang yang menjadi sasaran atau objek perbuatan *jaani* atau *jaaniah*.

Jinayah menurut bahasa merupakan nama bagi suatu perbuatan jelek seseorang.⁴²

Istilah hukum jinayah dalam kepustakaan Islam tidak ditemukan, tetapi istilah yang digunakan adalah Syari'at Islam dan dalam penjabarannya disebut Fiqh Jinayah. Ulama-ulama Muta'akhirin menghimpunya dalam bagian khusus yang dinamakan Fiqih Jinayat, yang dikenal dengan istilah Hukum Pidana Islam. Di dalamnya terhimpun pembahasan semua jenis pelanggaran atau kejahatan manusia dengan berbagai sasaran badan, jiwa, harta benda, kehormatan, nama baik, negara, tatanan hidup, dan lingkungan hidup.⁴³

2. Asas-asas Fiqih Jinayah

a) Asas Legalitas

Kata asas berasal dari bahasa Arab *asasun* yang berarti dasar atau prinsip, sedangkan kata legalitas berasal dari bahasa latin yaitu *lex* (kata benda) yang berarti undang-undang, atau dari kata jadian *legalis* yang berarti sah atau sesuai dengan ketentuan undang-undang. Dengan demikian legalitas adalah "*keabsahan sesuatu menurut undang-undang*". Asas legalitas dalam

⁴² *Op Cit*, Muhammad Nur.

⁴³ *Ibid*, Muhammad Nur.

Islam bukan berdasarkan pada akal manusia, tetapi dari ketentuan Tuhan. Sedangkan asas legalitas secara jelas dianut dalam hukum Islam. Terbukti adanya beberapa ayat yang menunjukkan asas legalitas tersebut. Allah tidak akan menjatuhkan hukuman pada manusia dan tidak akan meminta pertanggungjawaban manusia sebelum adanya penjelasan dan pemberitahuan dari Rasul-Nya. Demikian juga kewajiban yang harus diemban oleh umat manusia adalah kewajiban yang sesuai dengan kemampuan yang dimiliki, yaitu taklif yang sanggup di kerjakan.⁴⁴

Dasar hukum asas legalitas dalam Islam antara lain:

Al-Qur'an surat Al-Isra': 15

مَنْ اهْتَدَىٰ فَإِنَّمَا يَهْتَدِي لِنَفْسِهِ ۗ وَمَنْ ضَلَّ
فَأِنَّمَا يَضِلُّ عَلَيْهَا ۗ وَلَا تَزِرُ وَازِرَةٌ وِزْرَ أُخْرَىٰ ۗ وَمَا
كُنَّا مُعَذِّبِينَ حَتَّىٰ نَبْعَثَ رَسُولًا

Barangsiapa yang berbuat sesuai dengan hidayah (Allah), Maka Sesungguhnya Dia

⁴⁴ *ibid.*, Muhammad Nur.

berbuat itu untuk (keselamatan) dirinya sendiri; dan Barangsiapa yang sesat Maka Sesungguhnya Dia tersesat bag(kerugian) dirinya sendiri. dan seorang yang berdosa tidak dapat memikul dosa orang lain, dan Kami tidak akan meng'azab sebelum Kami mengutus seorang Rasul.

Al-Qur'an surat Al-Qashash: 59

وَمَا كَانَ رَبُّكَ مُهْلِكَ الْقُرَىٰ حَتَّىٰ يَبْعَثَ فِي
أَمِّهَا رَسُولًا يَتْلُو عَلَيْهِم آيَاتِنَا ۚ وَمَا كُنَّا مُهْلِكِي
الْقُرَىٰ ۚ إِلَّا وَأَهْلُهَا ظَالِمُونَ

Dan tidak adalah Tuhanmu membinasakan kota-kota, sebelum Dia mengutus di ibukota itu seorang Rasul yang membacakan ayat-ayat Kami kepada mereka; dan tidak pernah (pula) Kami membinasakan kota-kota; kecuali penduduknya dalam Keadaan melakukan kezaliman.

b) Asas Amar Makruf Nahi Munkar

Menurut Maududi pengertian ma'ruf dan munkar sebagai Istilah ma'rûfât (jamak dari ma'rûf) menunjukkan semua kebaikan dan sifat-sifat yang baik sepanjang masa diterima oleh hati nurani manusia sebagai suatu yang baik. Istilah munkarât (jamak dari munkar) menunjukkan semua dosa dan kejahatan sepanjang masa telah dikutuk oleh watak manusia sebagai suatu hal yang jahat. Dalam filsafat hukum Islam dikenal istilah amar makruf sebagai *fungsi social engineering*, sedang nahi munkar sebagai *social control* dalam kehidupan penegakan hukum. Berdasar prinsip inilah di dalam hukum Islam dikenal adanya istilah perintah dan larangan. Islam memberikan kebebasan bagi setiap penganutnya baik kebebasan individu maupun kolektif, kebebasan berpikir, kebebasan berserikat, kebebasan menyampaikan pendapat, kebebasan beragama, kebebasan berpolitik, dan lain sebagainya.⁴⁵

c) Asas Teritorial

Menurut konsepsi hukum Islam Asas teritorial yaitu hukum pidana Islam hanya

⁴⁵ *Ibid*, Muhammad Nur.

berlaku di wilayah di mana hukum Islam diberlakukan. Abu Hanifah berpendapat bahwa Hukum Islam diterapkan atas jarimah (tindak pidana) yang dilakukan di dar as-salam, yaitu tempat-tempat yang masuk dalam kekuasaan pemerintahan Islam tanpa melihat jenis jarimah maupun pelaku, muslim maupun non-muslim. Aturan-aturan pidana Islam hanya berlaku secara penuh untuk wilayah-wilayah negeri muslim.⁴⁶

d) Asas Material

Asas material hukum pidana Islam menyatakan bahwa tindak pidana ialah segala yang dilarang oleh hukum, baik dalam bentuk tindakan yang dilarang maupun tidak melakukan tindakan yang diperintahkan, yang diancam hukum (had atau ta'zir). Berdasarkan atas asas material ini, sanksi hukum pidana Islam mengenal dua macam: hudud dan ta'zir. Hudud adalah sanksi hukum yang kadarnya telah ditetapkan secara jelas berdasarkan teks atau nash, baik al-Qur'an maupun hadits. Sementara ta'zir adalah sanksi hukum yang ketetapanannya tidak ditentukan,

⁴⁶ *Ibid*, Muhammad Nur.

atau tidak jelas ketentuannya, baik dalam al-Qur'an maupun hadits.⁴⁷

e) Asas Moralitas

Ada beberapa asas moral hukum pidana Islam:

- a) Asas *Adamul Uzri* yang menyatakan bahwa seseorang tidak diterima pernyataannya bahwa ia tidak tahu hukum.
- b) Asas *Rufiul Qalam* yang menyatakan bahwa sanksi atas suatu tindak pidana dapat dihapuskan karena alasan-alasan tertentu, yaitu karena pelakunya di bawah umur, orang yang tertidur dan orang gila.
- c) Asas *al-Khath wa Nis-yan* yang secara harfiah berarti kesalahan dan kelupaan. Asas ini menyatakan bahwa seseorang tidak dapat dituntut pertanggungjawaban atas tindakan pidananya jika ia dalam melakukan tindakannya itu karena kesalahan atau karena kelupaan. Asas ini didasarkan atas surat al-Baqarah: 286.
- d) Asas *Suquth al-'Uqubah* yang secara harfiah berarti gugurnya hukuman. Asas ini menyatakan bahwa sanksi hukum dapat gugur karena dua hal : pertama, karena si pelaku dalam melaksanakan

⁴⁷ *Ibid*, Muhammad Nur.

tindakannya melaksanakan tugas; kedua, karena terpaksa. Pelaksanaan tugas dimaksud adalah seperti : petugas eksekusi qishash (aljojo), dokter yang melakukan operasi atau pembedahan. Keadaan terpaksa yang dapat menghapuskan sanksi hukum seperti : membunuh orang dengan alasan membela diri, dan sebagainya.⁴⁸

3. Pengertian *Jarimah Ta'zir*

Jarimah ta'zir menurut 'Audah adalah *jarimah* yang diancam dengan hukuman *ta'zir*. Dan di dalam ketentuan syari'ah, jika tidak ada batasan hukumanya, maka masuk kategori *jarimah ta'zir*, yaitu semua *jarimah* yang belum/tidak ditentukan kadar hukumannya.⁴⁹ Adapun menurut al-Mawardi *jarimah ta'zir* adalah hukuman pendidikan atas perbuatan dosa (tindak pidana) yang belum ditentukan hukuman di dalamnya sebagaimana hukuman *hudud*.⁵⁰

⁴⁸ *Ibid*, Muhammad Nur.

⁴⁹ Rokhmadi, *Hukum Pidana Islam*, 1 ed. (Semarang: CV. Karya Abadi Jaya, 2015). hlm 193.

⁵⁰ *Ibid*, Rokhmadi.

Menurut ‘Audah *ta’zir* dibagi menjadi tiga macam yaitu⁵¹:

- 1) *Ta’zir* karena melakukan perbuatan maksiat.

Yang dimaksud maksiat adalah semua perbuatan yang tidak boleh dilakukan atau wajib untuk tidak melakukannya. Para ulama’ telah sepakat bahwa *ta’zir* adalah setiap perbuatan maksiat yang tidak dijatuhi hukuman (*had*) maupun *kaffarat*, baik maksiat yang menyinggung hak Allah maupun hak adami. *Ta’zir* yang menyinggung hak Allah adalah semua perbuatan yang berkaitan dengan kepentingan dan kemaslahatan umum. Sedangkan *ta’zir* yang menyinggung hak adami adalah setiap perbuatan yang mengakibatkan kerugian kepada orang tertentu, bukan orang banyak.

- 2) *Ta’zir* untuk kepentingan umum.

Sedangkan lingkup *ta’zir* untuk memelihara kepentingan umum adalah semua perbuatan yang dapat merugikan atau membahayakan kepentingan umum meskipun perbuatannya bukan maksiat. Perbuatan-perbuatan yang masuk kategori

⁵¹ *Ibid*, Rokhmadi.

ini tidak dapat ditentukan, karena perbuatan tersebut tidak diharamkan karena zatnya, melainkan karena sifatnya. Jika sifat tersebut ada, maka perbuatannya diharamkan, dan jika sifat tersebut tidak ada, maka perbuatannya tergolong *mubah*. Sifat yang menjadi alasan dikenakannya hukuman atas perbuatan tersebut adalah membahayakan atau merugikan kepentingan umum. Jika dalam suatu perbuatan terdapat unsur merugikan kepentingan umum, maka perbuatan tersebut dianggap tindak pidana dan pelakunya dikenakan hukuman. Akan tetapi, jika dalam perbuatan tersebut tidak terdapat unsur merugikan kepentingan umum, maka perbuatan tersebut bukan tindak pidana dan pelakunya tidak dapat dikenakan hukuman.

3) *Ta'zir* karena pelanggaran.

Ta'zir karena melakukan pelanggaran adalah melakukan perbuatan yang diharamkan dan meninggalkan perbuatan yang diwajibkan.

Abdul Aziz Amir membagi *jarimah ta'zir* secara rinci kepada beberapa bagian, yaitu:

- 1) *Jarimah ta'zir* yang berkaitan dengan pembunuhan

Pembunuhan diancam dengan hukuman mati, apabila hukuman mati (*Qishash*) dimaafkan maka hukumannya diganti dengan diyat. Apabila hukuman diyat dimaafkan juga maka ulil amri berhak menjatuhkan hukuman ta'zir apabila hal itu dipandang lebih maslahat.

- 2) *Jarimah ta'zir* yang berkaitan dengan pelukaan

Menurut Imam Malik, hukuman *ta'zir* dapat digabungkan dengan *qishash* dalam jarimah pelukaan, karena *qishash* merupakan hak adami, sedangkan *ta'zir* sebagai imbalan atas hak masyarakat. Disamping itu *ta'zir* juga dapat dikenakan terhadap jarimah pelukaan apabila *qishahsnya* dimaafkan atau tidak bisa dilaksanakan karena suatu sebab yang dibenarkan oleh syara'.

- 3) *Jarimah ta'zir* yang berkaitan dengan kejahatan terhadap kehormatan dan kerusakan akhlak

Jarimah ta'zir ini berkaitan dengan *jarimah zina*, menuduh zina dan penghinaan. Di antara kasus perzinahan yang diancam dengan *ta'zir* adalah

perzinahan yang tidak memenuhi syarat untuk dikenakan hukuman *hadd*, atau terdapat syubhat dalam pelakunya, perbuatannya, atau tempat (objeknya). Demikian pula kasus percobaan zina dan perbuatan-perbuatan *prazina*, seperti meraba-raba, berpelukan dengan wanita yang bukan istrinya, tidur bersama tanpa hubungan seksual, dan sebagainya.

4) *Jarimah ta'zir* yang berkaitan dengan harta

Jarimah yang berkaitan dengan harta adalah *jarimah* pencurian dan perampokan. Apabila kedua *jarmah* tersebut syarat-syaratnya telah dipenuhi maka pelaku dikenakan hukuman *hadd*, akan tetapi apabila syarat-syarat untuk dikenakan hukuman *hadd* tidak terpenuhi maka pelaku tidak dikenakan hukuman *hadd*, melainkan hukuman *ta'zir*. Jariman yang termasuk jenis ini antara lain seperti percobaan pencurian, pencopetan, pencurian yang tidak mencapai batas nisbah, meng-*ghasab*, dan perjudian. Termasuk, juga ke dalam kelompok *ta'zir*, pencurian karena adanya syubhat, seperti pencurian oleh keluarga dekat.

5) *Jarimah ta'zir* yang berkaitan dengan kemaslahatan individu

Jarimah ta'zir yang termasuk kelompok ini, antara lain seperti saksi palsu, berbohong (tidak memberikan keterangan yang benar) di depan sidang pengadilan, menyakiti hewan, melanggar hak *privacy* orang lain (misalnya masuk rumah orang lain tanpa izin).

6) *Jarimah ta'zir* yang berkaitan dengan keamanan umum.

Jarimah ta'zir yang termasuk dalam kelompok ini yaitu:

- a) *Jarimah* yang mengganggu keamanan negara/pemerintah, seperti sepijone dan percobaan kudeta;
- b) Suap;
- c) Tindakan melampaui batas dari pegawai atau pejabat atau lalai dalam menjalankan kewajiban. Contohnya seperti penolakan hakim untuk mengadili suatu perkara, atau kesewenang-wenangan hakim dalam memutuskan suatu perkara;
- d) Pelayanan yang buruk dari aparaturn pemerintah terhadap masyarakat;
- e) Melawan petugas pemerintah dan membangkang terhadap peraturan,

seperti melawan petugas pajak, penghinaan terhadap pengadilan, dan menganiaya polisi.⁵²

4. Unsur-unsur *Jarimah Ta'zir*

Di dalam hukum Islam, suatu perbuatan tidak dapat dihukum, kecuali jika terpenuhi semua unsur-unsurnya, baik unsur umum maupun unsur khusus. Unsur-unsur umum tersebut ialah:

- a) *Ar-rukn asy-syar'i* adalah nash-nash atau aturan-aturan yang berkaitan dengan tindakan *jarimah*. Aturan-aturan tersebut merupakan larangan syari'at yang mengandung sanksi hukum, yang dapat dikategorikan kepada tiga bentuk. Pertama, aturan-aturan mengenai hudud, kedua aturan-aturan mengenai *qishash* dan *diyat* dan ketiga aturan-aturan mengenai *ta'zir*. Aturan mengenai *hudud*, *qishash* dan *diyat* merupakan aturan yang telah ditentukan oleh Allah hukuman atau sanksinya, sedangkan aturan mengenai *ta'zir* ditentukan oleh penguasa atau hakim. Oleh karena itu sesuai dengan asas legalitas bahwa hukuman tidak boleh

⁵² Ahmad Wardi Muslich, *Hukum Pidana Islam*, cetakan ke (Jakarta: Sinar Grafika Offset, 2016).

dilakukan kecuali setelah ada ketentuan yang mengaturnya. Berikut ini dikemukakan beberapa dalil yang mengatur tentang *hudud*, *qishash* dan *diyat*.

- b) *Ar-ruk'n al-maddi* (unsur materil) adalah perbuatan yang dilakukan oleh pelaku tindak pidana. Perbuatan tersebut merupakan pelanggaran terhadap aturan syari'at yang mengandung sanksi. Pelanggaran itu bisa dalam bentuk melakukan yang dilarang maupun meninggalkan yang disuruh. Ruang lingkup pembicaraan dalam unsur materil ini adalah seputar jarimah tammah yaitu tindak pidana yang selesai dilakukan secara sempurna, percobaan dalam melakukan tindak pidana, bekerjasama dalam melakukan tindak pidana.
- c) *Ar-ruk'n al-adabi* (unsur moril) adalah pelaku pidana yang bertanggung jawab atas perbuatan jarimahnyanya, dalam hal ini adalah *mukallaf*. Ada dua hal penting yang termasuk kedalam unsur moril. Pertama, seputar pertanggungjawaban

pidana, dan yang kedua hilangnya pertanggungjawaban pidana tersebut.⁵³

5. Perbedaan *Jarimah Hudud* dan *Jarimah Ta'zir*

Jarimah hudud adalah *jarimah* yang hukumannya telah ditentukan oleh syara' sedangkan *jarimah ta'zir* adalah *jarimah* yang hukumannya belum ditentukan oleh syara' dan diserahkan kepada pemerintah (*ulil amri*) untuk menetapkannya. Dari pengertian ini jelaslah bahwa antara *hudud* dan *ta'zir* terdapat beberapa perbedaan. Syaid Sabiq mengemukakan perbedaan tersebut sebagai berikut:

- 1) Hukuman *hudud* diberlakukan secara sama untuk semua orang (pelaku), sedangkan hukuman *ta'zir* pelaksanaannya dapat berbeda antara satu pelaku dengan pelaku lainnya, tergantung kepada perbedaan kondisi masing-masing pelaku. Apabila seseorang yang terhormat dan baik-baik, suatu ketika tergelincir melakukan tindak pidana *ta'zir* maka kondisinya itu dapat dijadikan pertimbangan untuk membebaskannya

⁵³ Zainuddin, *Pengantar Hukum Pidana Islam* (Yogyakarta: CV. Budi Utama, 2019).

atau menjatuhkan hukuman yang lebih ringan.

- 2) Dalam Jarimah hudud tidak berlaku pembelaan (*Syafa'at*) dan pengampunan apabila perkaranya sudah dibawa ke pengadilan. sedangkan untuk *jarimah ta'zir*, kemungkinan untuk memberikan pengampunan terbuka lebar, baik oleh individu maupun *ulil amri*.
- 3) Orang yang mati karena dikenakan hukuman *ta'zir*, berhak memperoleh ganti rugi. sedangkan untuk jarimah hudud hal ini tidak berlaku. akan tetapi menurut Imam Malik dan Imam Abu Hanifah, kematian akibat hukuman *ta'zir* tidak mengakibatkan ganti rugi apapun, karena dalam hal ini *ta'zir* dan *had* itu sama. Alasan pertama adalah tindakan Khalifah Umar yang menggertak seorang wanita. Wanita itu kemudian merasa perutnya mulas (sakit) dan janinnya gugur dalam keadaan mati. Khalifah Umar kemudian menanggung dan membayar diat janin tersebut.⁵⁴

⁵⁴ *Op Cit*, Wardi Muslich. *Hukum Pidana Islam*

6. Macam-Macam Hukuman *Ta'zir*

Hukuman *ta'zir* pada dasarnya terbagi kedalam beberapa jenis hukuman, macam-macam hukuman *ta'zir* adalah sebagai berikut:

a) Hukuman Mati

Dalam jarimah *ta'zir* hukuman mati ini diterapkan oleh para *fuqaha* secara beragam, sebagian *fuqaha* safi'iyah membolehkan hukuman mati sebagai *ta'zir* dalam kasus peyebaran aliran-aliran sesat yang menyimpang dari ajaran al-Quran dan as-Sunnah. Hukuman mati untuk *jarimah ta'zir* hanya dilaksanakan dalam *jarimah-jarimah* yang sangat berat dan berbahaya, sengan syarat-syarat sebagai berikut:

- 1) Bila pelaku adalah residivis yang tidak mempan oleh hukuman-hukuman hudud selain hukuman mati.
- 2) Harus dipertimbangkan betul-betul dampak kemaslahatan terhadap masyarakat dan pencegahan terhadap kerusakan yang menyebar dibumi.

b) Hukuman *Jilid*

Hukuman *jilid* (cambuk) merupakan hukuman pokok dalam syariat islam untuk jarimah *hudud*, namun hanya ada beberapa jarimah yang dikenakan hukuman *jilid*, seperti *zina*, *qadzaf*, dan minum *khamar*.

Hukuman *jilid* untuk *ta'zir* ini tidak boleh melebihi hukuman *jilid* dalam *hudud*. Namun mengenai batas maksimalnya tidak ada kesepakatan di kalangan *fuqaha*. Hal ini dikarenakan hukuman *had* dalam *jarimah* hudud itu berbeda-beda antara satu *jarimah* dengan *jarimah* yang lainnya. Zina hukuman jilidnya seratus kali, *Qadzaf* delapan puluh kali, sedangkan *syurbul khamar* ada yang mengatakan empat puluh kali dan ada yang delapan puluh kali.

c) Hukuman Penjara

Pemenjaraan secara *syar'i* adalah menghalangi atau melarang seseorang untuk mengatur dirinya sendiri. Baik itu dilakukan di dalam negeri, rumah, masjid, di dalam penjara, atau di tempat-tempat lain. Hukuman penjara dalam syariat islam dibagi dalam dua bagian yaitu:

- 1) Hukuman penjara yang dibatasi waktunya
- 2) Hukuman penjara yang tidak dibatasi waktunya.

d) Hukuman Pengasingan

Hukuman pengasingan merupakan salah satu jenis hukuman *ta'zir*. untuk jarimah-jarimah selain zina hukuman ini diterapkan

apabila perbuatan pelaku dapat menjaral atau merugikan orang lain.

e) Hukuman Pemboikotan

Pemboikotan yang dimaksud dalam hal ini yaitu seorang penguasa menginstruksikan masyarakat untuk tidak berbicara dengan seseorang dengan batas waktu tertentu. Hal ini dilakukan berdasarkan dalil pada peristiwa yang menimpa tiga orang sahabat yang tidak ikut berperang. Ketika mengetahui hal itu, Rasulullah saw melarang kaum muslim untuk berbicara dengan mereka.

f) Hukuman Salib

Hukuman salib ini berlaku dalam satu kondisi, yaitu jika sanksi bagi pelaku kejahatan adalah hukuman mati. Terhadapnya boleh dijatuhi hukuman salib. Masa penyaliban ini tidak boleh lebih dari tiga hari dan ia (terhukum) tidak dilarang untuk makan, minum, wudu, dan salat dengan isyarat.

g) Hukuman Denda (*Ghuramah*)

Hukuman denda bisa merupakan hukuman pokok yang berdiri sendiri dan dapat pula digabungkan dengan hukuman pokok lainnya. Penjatuhan hukuman denda Bersama-sama dengan hukuman lain bukan

merupakan hal yang dilarang bagi seorang hakim yang mengadili perkara jarimah *ta'zir*, karena hakim diberi kebebasan yang penuh dalam masalah ini. Dalam hal ini hakim dapat mempertimbangkan berbagai aspek, baik yang berkaitan dengan jarimah, pelaku, situasi, maupun kondisi tempat dan waktunya. Syariat islam tidak menetapkan batas terendah atau tertinggi dari hukuman denda. Hal ini sepenuhnya diserahkan kepada hakim dengan mempertimbangkan berat ringannya jarimah yang dilakukan pelaku. Apabila seorang hakim telah menetapkan sanksi tertentu, maka ia tidak boleh membatalkan ketetapanannya. Dalam kondisi terpidana tidak mampu membayar ghuramah (ganti rugi), maka ditunggu sampai terpidana memiliki harta, baru kemudian ghuramah (ganti rugi) tersebut diserahkan kepada negara.

h) Hukuman Lainnya

Disamping hukuman-hukuman yang telah disebutkan, terdapat hukuman-hukuman *ta'zir* yang lain, hukuman-hukuman tersebut adalah sebagai berikut:

- 1) Peringatan keras.
- 2) Dihadirkan di hadapan sidang.
- 3) Nasihat.

- 4) Celaan.
- 5) Pengucilan.
- 6) Pemecatan.
- 7) Pengumuman kesalahan secara terbuka.⁵⁵

7. Syarat-syarat Penerapan *Jarimah*

Dalam rangka menerapkan hukuman terhadap pelaku tindak pidana haruslah memenuhi kriteria penerapan *Jarimah*. Setelah syarat-syarat penerapan jarimah terpenuhi barulah kemudian pelaksanaan *jarimah* terhadap pelaku dapat dilakukan, adapun syarat tersebut meliputi:

1. *Mukallaf*

Mukallaf adalah orang yang telah mempunyai kewajiban menjalankan syari'at atau hukum Islam. Dengan kata lain dapat juga disebut dengan orang yang telah dibebani hukum syari'at. Seseorang dikatakan *mukallaf* apabila telah *balig* dan berakal. *Balig* adalah mencapai usia tertentu yang telah ditetapkan, sedangkan berakal adalah tidak terganggu pikiran oleh sesuatu yang mengakibatkan hilangnya akal, seperti gila atau mabuk. *Balig* dan berakal merupakan syarat bagi pencuri untuk

⁵⁵ *Op Cit*, Marsaid.

dijatuhi hukuman *hadd*, karena pidana tidak dapat dihadapkan kepada orang yang tidak balig dan tidak berakal. Kebaligan seseorang dapat ditentukan melalui dua cara. Pertama, melalui tanda-tanda, kedua melalui umur atau usia. Kebaligan melalui tanda-tanda dapat diketahui dengan keluar mani, tumbuh rambut pada kemaluan, haid, dan kehamilan.

Kebaligan yang ditentukan melalui usia, ada beberapa batasan yang dikemukakan oleh para *fuqaha*. Menurut Syafi'iyah, Hanabilah dan Abu Yusuf usia balig bagi laki-laki dan wanita adalah 15 (lima belas) tahun. Menurut Abu Hanifah 18 (delapan belas) tahun bagi laki-laki, 15 (lima belas) tahun bagi wanita. Dalam suatu riwayat dikatakan Abu Hanifah menetapkan 19 (sembilan belas) tahun. Dari kalangan Malikiyah ada beberapa versi. Ada yang mengatakan usia 15 (lima belas), 16 (enam belas), 17 (tujuh belas) dan ada pula yang mengatakan 19 (sembilan belas) tahun.

2. Mempunyai kebebasan atau kemauan sendiri (tidak ada unsur keterpaksaan)
Fuqaha menetapkan bagi pencuri yang akan dijatuhi *hadd* itu ada unsur kebebasan atau kemauan sendiri, dengan arti kata tidak ada

unsur keterpaksaan. Dalam hukum Islam ada dua istilah yang dipakai untuk kata “*keterpaksaan*”, yaitu *ikrah* dan *dharurah*. *Ikrah* adalah membebani seseorang secara tidak benar terhadap urusan (perkara) yang tidak disukainya. Sedangkan, *Dharurah* adalah takut atas kebinasaan atau kemudaratannya yang sangat berbahaya yang menyangkut salah satu kepentingan (yang mendasar) bagi jiwa atau yang lain atas dasar keyakinan atau persangkaan yang berat. Jika seseorang tidak berbuat (untuk mengatasi), maka kebinasaan dan kemudaratannya yang berbahaya itu tidak akan terhindar.

3. Dikenai aturan hukum syara’ (*multazim*). Untuk dapat dijatuhi hukuman *hadd* seorang pencuri disyaratkan orang yang dikenai aturan hukum syara’ atau disebut dengan *multazim li al-ahkam*. Hal ini berbeda dengan persyaratan yang pertama, yaitu *mukallaf*. *Mukallaf* adalah orang muslim yang sudah dibebani hukum syara’. Pada *mukallaf* pembicaraan difokuskan kepada orang muslim saja, yaitu mengenai baligh dan berakal. Sedangkan *multazim* belum tentu orang muslim saja, tetapi boleh jadi non muslim. Dalam hal ini non muslim

dibedakan dalam tiga bentuk, yaitu *zimmi*, *musta'min* dan *harbi*.

4. Adanya unsur kesengajaan atau niat melakukan pidana

Niat atau kesengajaan merupakan unsur utama dalam setiap perbuatan. Dalam seluruh perbuatan ibadah niat dijadikan sebagai rukun. Artinya, apabila ibadah tidak mempunyai niat dianggap tidak sah. Demikian juga halnya dalam tindakan pidana, niat sangat menentukan apakah seseorang melakukan tindakan pidana secara sempurna atau tidak.⁵⁶

8. Sanksi Pidana Kejahatan Siber dengan metode *Distributed Denial of Service attack (DDoS attack)* dalam Fiqih Jinayah

Jarimah *ta'zir* dapat digunakan untuk tindak pidana baru yang belum memiliki aturan hukum karena pada dasarnya ada 2 (dua) bentuk pidana yang dapat dijatuhi hukuman *ta'zir*. Pertama hukuman pidana hudud yang tidak memenuhi kriteria untuk dijatuhi hukuman *hudud*. Kedua, segala bentuk pidana atau pelanggaran yang tidak ditentukan oleh Allah dan Rasul. *DDos*

⁵⁶ *Op Cit*, Zainuddin.

attack merupakan sebuah tindak pidana baru maka jarimah yang digunakan adalah *Jarimah ta'zir* karena *DDoS attack* lahir atas kemajuan zaman sehingga ketentuan hukumnya belum terdapat didalam Al-Quran dan Hadits. *DDoS attack* termasuk kedalam kategori *jarimah ta'zir* karena aturan yang mengatur larangan melakukan tindakan pengrusakan suatu barang terdapat dalam Kaidah Fiqih yang menyatakan bahwa:

الإِتْلَافُ يَسْتَوِي فِيهِ الْمُتَعَمِّدُ وَالْجَاهِلُ وَالنَّاسِي

Artinya:

*Perbuatan merusakkan barang orang lain hukumnya sama, apakah terjadi karena kesengajaan, ketidaktahuan, atau karena lupa.*⁵⁷

Kaidah ini memberikan patokan bahwa dalam perbuatan seseorang yang melakukan perusakan, baik kepada jiwa ataupun harta orang lain dihukumi sama. Kaidah ini juga menjelaskan bahwa barangsiapa yang merusakkan barang orang lain tanpa alasan yang benar, maka ia wajib

⁵⁷*Op Cit*, Manhaj.

mengganti barang yang ia rusakkan tersebut atau membayar ganti rugi kepada pemilik harta. Sama saja, apakah kerusakan tersebut terjadi karena kesengajaan olehnya, atau karena tidak tahu atau karena lupa.⁵⁸

Para ulama berbeda pendapat tentang dibolehkannya hukuman *ta'zir* dengan cara mengambil harta. Menurut Imam Abu Hanifah, hukuman *ta'zir* dengan cara mengambil harta tidak dibolehkan. Pendapat ini diikuti oleh muridnya, yaitu Muhammad ibn Hasan, tetapi muridnya yang lain yaitu, Imam Abu Yusuf membolehkannya apabila dipandang membawa masalahat. Pendapat ini diikuti Imam Malik, Imam Syafi'i, dan Imam ibn Hanbal.⁵⁹

Hukuman denda bisa merupakan hukuman pokok yang berdiri sendiri dan dapat pula digabungkan dengan hukuman pokok lainnya. Contoh yang pertama, seperti hukuman penjatuhan denda terhadap orang yang duduk-duduk di bar tempat minuman keras, atau denda terhadap orang yang mencuri buah-buahan dari pohonnya, atau mencuri kambing sebelum sampai di penggembalaannya. sedangkan hukuman yang kedua adalah hukuman denda bersama-sama

⁵⁸ *Ibid*, Manhaj.

⁵⁹ *Op Cit*, Wardi Muslich. *Hukum Pidana Islam*.

dengan *jilid* bagi pelaku tindak pidana yang disebutkan di atas. Penjatuhan hukuman denda dengan hukuman lain bukan merupakan hal yang dilarang bagi seorang hakim yang mengadili perkara *jarimah ta'zir* karena hakim diberi kebebasan penuh masalah ini.⁶⁰

Syariat Islam tidak menetapkan batas terendah atau tertinggi dari hukuman denda. Hal ini sepenuhnya diserahkan kepada hakim dengan mempertimbangkan berat ringannya jarimah yang dilakukan pelaku. selain denda hukuman *ta'zir* yang berupa harta adalah penyitaan atau perampasan harta. Namun hukuman ini diperselisihkan oleh para *fuqaha*. Jumhur ulama membolehkannya apabila persyaratan untuk mendapat jaminan atas harta tidak dipenuhi. syarat-syarat tersebut adalah sebagai berikut:

- 1) Harta diperoleh dengan cara yang halal.
- 2) Harta itu digunakan sesuai dengan fungsinya.
- 3) penggunaan harta itu tidak mengganggu hak orang lain.⁶¹

⁶⁰ *Ibid*, Wardi Muslich.

⁶¹ *Ibid*, Wardi Muslich.

Apabila persyaratan tersebut tidak dipenuhi, misalnya harta didapat dengan jalan yang tidak halal, atau tidak digunakan sesuai dengan fungsinya maka dalam keadaan demikian *ulil amri* berhak untuk menerapkan hukuman *ta'zir* berupa penyitaan atau perampasan sebagai sanksi terhadap perbuatan yang dilakukan oleh pelaku.⁶²

⁶² *Ibid*, Wardi Muslich.

BAB III
KEJAHATAN SIBER DENGAN METODE
DISTRIBUTED DENIAL OF SERVICE ATTACK
(DDOS ATTACK) TERHADAP WEBSITE

A. Serangan Siber dengan Metode *Distributed Denial of Service Attack*

1. Pengertian Kejahatan Siber (*Cybercrime*)

Cybercrime berasal dari kata *cyber* yang berarti dunia maya atau internet dan *crime* yang berarti kejahatan. Dengan kata lain, *cybercrime* adalah segala bentuk kejahatan yang terjadi di dunia maya atau internet. *Cybercrime* merupakan tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. *Cybercrime* yaitu kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet.⁶³

⁶³ *Op Cit*, Naufal dan Jannah. Naufal dan Jannah.

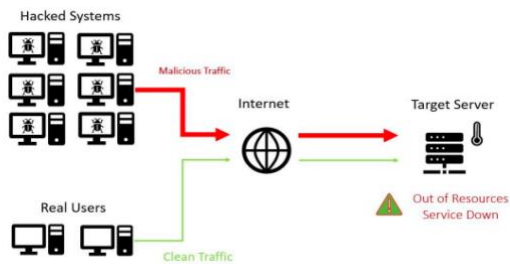
2. Kejahatan Siber Dengan Metode *DDoS* Attack

Serangan *Distributed Denial of Service* (*DDoS*) adalah serangan untuk melumpuhkan sistem jaringan komputer web (website) dengan cara membanjiri *server* korban dengan banyak lalu lintas data atau melakukan banyak *request* data ke sebuah *server* sehingga *server* tidak lagi dapat memberikan layanan sehingga terjadi *crash*. Pada umumnya serangan *DDoS* menargetkan serangan pada *bandwidth* jaringan komputer atau koneksi jaringan (*connectivity*). Serangan ini menyebabkan *server website* yang dituju mengalami *Overload* (kelebihan kapasitas) dan dampaknya website tersebut tidak dapat diakses oleh masyarakat karena terjadi *Down*, *hang*, bahkan *crash*.⁶⁴

Serangan *DDoS* secara sederhana dapat dilakukan dengan menggunakan perintah ping yang dimiliki oleh system operasi Windows. Sedangkan untuk serangan tingkatnya lebih tinggi biasanya menggunakan program khusus yang dirancang untuk melakukan serangan *DDoS* tingkat tinggi. Pada dasarnya sebuah komputer dapat mengirimkan data sebesar 32 *bytes/detik* ke

⁶⁴ *Op Cit*, Hermawan.

situs yang dituju. Misalnya, jika terdapat 10.000 komputer yang melakukan perintah ping secara bersamaan, maka data yang diterima oleh situs (*website*) yang dituju akan sebesar 312 *Mega Bytes/detik*. Selanjutnya, *server* akan merespon kiriman data yang dikirim dari 10.000 komputer secara bersamaan. Jika 312 MB/detik data yang harus di porses oleh *server*, dalam 1 menit saja server harus memproses kiriman data sebesar 312 MB x 60 detik = 18720 MB. Maka hasilnya situs yang diserang dengan metode ini akan mengalami overload (kelebihan data), sehingga tidak sanggup memproses kiriman data yang datang terus-menerus.⁶⁵



Gambar 3. 1 Mekanisme DDoS Attack

(sumber: *polito.it*)

⁶⁵ *Ibid*, Hermawan.

Berdasarkan kategori serangannya, serangan *DDoS* terbagi kedalam 3 (tiga) kategori serangan yaitu:

1) Serangan berbasis *bandwidth*

Serangan *DDoS* jenis ini mengirim pesan data sampah secara masal untuk menyebabkan *overload*, yang juga mengakibatkan berkurangnya *bandwidth* jaringan yang tersedia atau berkurangnya sumber daya perangkat jaringan. Seringkali *router*, *server* dan *firewall* yang diserang memiliki sumber daya yang terbatas. Serangan *overload* menyebabkan kegagalan perangkat jaringan untuk menangani akses yang normal, sehingga terjadi penurunan yang signifikan dalam kualitas layanan atau kelumpuhan total sistem.

2) Serangan berbasis lalu lintas jaringan

Bentuk yang paling umum dari *DDoS attack* adalah serangan yang membanjiri lalu lintas jaringan. Serangan ini dilakukan dengan cara mengirimkan paket dalam jumlah yang besar misalnya, paket TCP, paket UDP, paket ICMP yang tampaknya sah kepada *host/server* target. Beberapa serangan dengan basis ini juga dapat menghindari pemindaian sistem

deteksi dengan teknologi kamuflase alamat asal. Permintaan yang sah pada akhirnya tidak terlayani karena begitu banyak paket serangan yang beredar di jaringan. Serangan ini juga dapat semakin merusak jika dikombinasikan dengan kegiatan ilegal lainnya, seperti eksploitasi menggunakan malware yang menyebabkan kebocoran informasi atau pencurian data sensitif pada komputer target.

3) Serangan berbasis aplikasi

Serangan jenis ini biasanya mengirim pesan data pada tingkat layer aplikasi sesuai dengan fitur bisnis yang spesifik (menggunakan fungsi tampaknya legal dan operasional, seperti akses database), sehingga semakin berkurangnya sumber daya tertentu pada lapisan aplikasi (seperti jumlah pengguna dan koneksi aktif yang diperbolehkan) dan layanan sistem tidak lagi tersedia. Serangan seperti ini biasanya tidak dilancarkan dalam volume yang terlalu besar, serangan dengan lalu lintas tingkat rendah pun dapat menyebabkan gangguan serius pada sistem atau bahkan kelumpuhan kinerja

sistem bisnis.⁶⁶

3. Data Serangan *DDoS Attack*

Sampai saat ini *DDoS Attack* masih menjadi metode serangan siber yang cukup ampuh untuk melumpuhkan website, hal ini dapat dilihat dari data serangan siber dunia yang mana pada januari 2016 situs *Hackmageddon* melaporkan bahwa serangan *DDoS* menempati urutan kedua dari 9 serangan populer. Walaupun serangan ini umurnya telah mencapai 20 tahun tetapi masih menjadi *tren* bagi para *attacker*. *Cisco* memprediksi pada tahun 2023 jumlah serangan *DDoS* akan meningkat 15,4 juta secara global.⁶⁷ Berikut adalah prediksi *Cisco* yang termuat dalam *Cisco Annual Internet Report (2018-2023) White Paper*:

“Globally, there was a 776% growth in attacks between 100 Gbps and 400 Gbps Y/Y from 2018 to 2019, and the total number of DDoS attacks will

⁶⁶ *Op Cit*, Geges dan Wibisono.

⁶⁷ Nasution dan Basuki. hlm 390. *Lihat juga Cisco, 2020. Cisco Annual Internet Report (2018–2023) White Paper.* [online]. Tersedia di <https://www.cisco.com>

*double from 7.9 million in 2018 to 15.4 million by 2023*⁶⁸

Pada tahun 2020 *NSFOCUS* mendeteksi 152.000 serangan DDoS dengan volume gabungan 386.500 TB (terabyte). Angka-angka ini mewakili penurunan *Year-on-Year* (YoY) masing-masing sebesar 16,16% dan 19,67%.⁶⁹

Menurut laporan *Kaspersky Labs*⁷⁰ data serangan *Distributed Denial of Service (DDoS)* pada tahun 2021 adalah sebagai berikut:

- a) Pada kuartal pertama tahun 2021 jumlah serangan DDoS turun sebanyak 29% (terjadi 71,53% serangan) dibandingkan dengan periode yang sama tahun 2020.

⁶⁸ Cisco.com, “*Cisco Annual Internet Report (2018-2-23) White Paper,*” 09 March, 2020, hal.1 <https://www.cisco.com/c/en/us/solutions/collateral/executive_perspectives/annual-internet-report/white-paper_c11741490.html?dtid=ossdc000283> [diakses 7 Januari 2022].

⁶⁹ *Op Cit*, FOCUS.

⁷⁰ *Kaspersky Labs* merupakan perusahaan keamanan siber global yang didirikan pada tahun 1997 yang bermarkas di Moskwa Rusia, Perusahaan ini bergerak dalam bidang keamanan siber dengan menawarkan produk antivirus dan layanan keamanan khusus untuk melawan ancaman digital yang terus berkembang. Kaspersky bertransformasi menjadi solusi dan layanan keamanan inovatif untuk melindungi bisnis, infrastruktur penting, pemerintah, dan konsumen di seluruh dunia. Kaspersky dapat diakses melalui laman <https://www.kaspersky.com/>

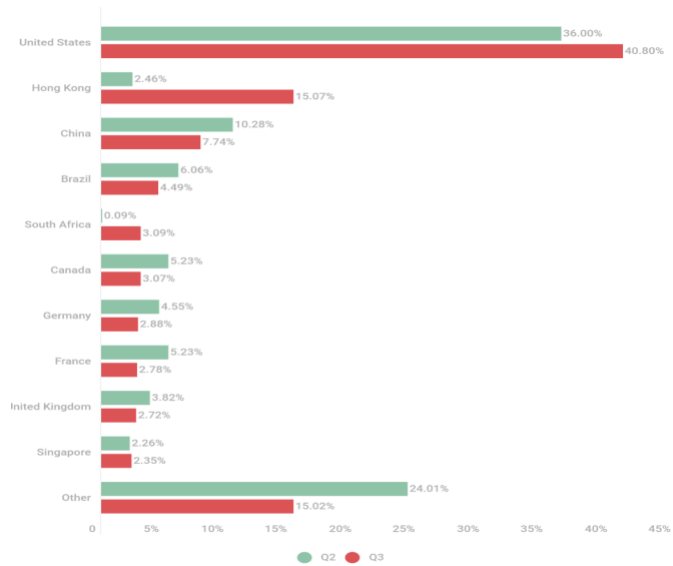
- b) Pada kuartal kedua (Q2) pada tahun 2021 jumlah serangan DDoS Mengalami penurunan sebesar 38,8% dibandingkan dengan Q2 tahun 2020. Sepanjang Q2 jumlah serangan DDoS berfluktuasi dengan rentang 500 hingga 800 per hari.
- c) Pada kuartal ketiga (Q3) tahun 2021 serangan DDoS meningkat hampir 24% dari tahun 2020 sedangkan total serangan *Smart DDoS* (Serangan DDoS tertarget) meningkat sebesar 31% dibandingkan dengan Q3 tahun 2020. Serangan Smart DDoS merupakan serangan yang lebih canggih dan cenderung bertarget, serangan ini tidak hanya digunakan untuk mengganggu layanan tetapi juga membuat sumber daya tertentu tidak dapat diakses. Sebagian besar serangan DDoS di Q3 berbentuk *SYN flooding*.⁷¹

Secara *Geografis* pada Q3 tahun 2021 pangsa serangan terhadap sumber daya yang berbasis di Amerika Serikat meningkat sebesar 40,80%. Amerika Serikat mempertahankan tempat pertama dengan jumlah serangan *DDoS*.

⁷¹ Alexander Gutnikov, Oleg Kupreev, dan Yaroslav Shemeley, “DDoS Attack In Q3 2021,” *scurelist.com*, 2021, hal. 1 <<https://scurelist.com/ddos-attacks-in-q3-2021/104796/>> [diakses 5 Januari 2022].

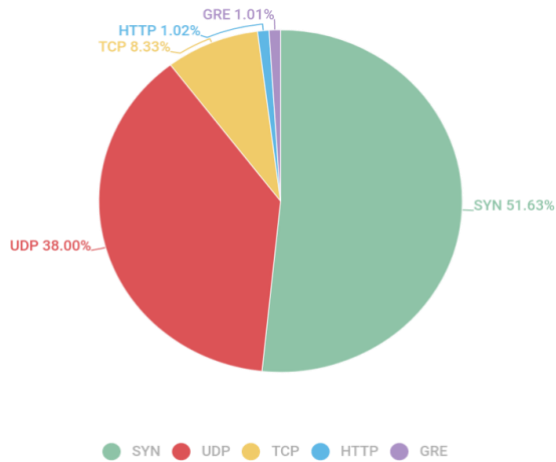
Daerah Administratif Khusus Hong Kong naik ke posisi kedua (15,07%). Setelah periode tenang di Q1 dan Q2, pangsa serangan di kawasan itu tumbuh sekaligus sebanyak 12,61. Padahal, pangsa China (7,74%) kembali menyusut, menempatkan negara itu di urutan ketiga. Tempat keempat masih dipegang oleh Brasil (4,49%), pangasanya sedikit berkurang. Afrika Selatan naik ke urutan kelima (3,09%) dan mendorong Kanada (3,07%) ke urutan keenam. Kanada diikuti oleh Jerman (2,88%), Prancis (2,78%) dan Inggris (2,72%), dengan Singapura di peringkat bawah (2,35%).⁷²

⁷² *Ibid*, Gutnikov, Kupreev, dan Shemeley.



Gambar 3. 2 Data DDoS attack Q3 berdasarkan Geografis sumber: Kaspersky.com

Berdasarkan jenis serangan *DDoS* yang dilakukan pada Q3 jenis serangan *Syn Flood* adalah yang paling sering dilakukan dengan presentase serangan 51,63%, *UDP Flood* berada diposisi kedua dengan presentase serangan 38,00%, *TCP Flood* berada diposisi ketiga dengan presentase serangan 8,33%, *HTTP Flood* berada diposisi keempat dengan presentase 1,02%, pada posisi terakhir adalah jenis serangan *GRE* dengan presentase 1,01%.



Gambar 3. 3 Data DDoS attack Q3 berdasarkan jenis serangan sumber: Kaspersky.com

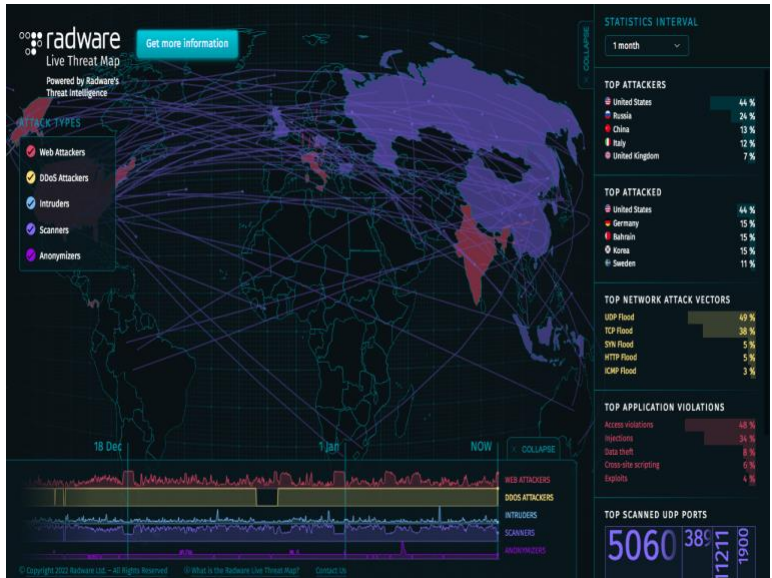
Salah satu contoh kasus *DDoS* di Indonesia yang terjadi belakangan ini yaitu diserangnya Website Project Multatuli pada tanggal 06 Oktober 2021 Pukul 18.00 Wib, serangan tersebut mengakibatkan situs website <https://projectmultatuli.org> tidak dapat diakses oleh pembaca selama beberapa waktu.⁷³ Serangan serupa juga pernah terjadi dalam beberapa tahun terakhir, sedikitnya dalam kurun waktu Januari 2019 hingga Oktober 2021 terdapat 13 (tiga belas) laporan gangguan system yang tercatat dalam situs

⁷³ *Op Cit*, Multatuli.

Direktorat Tindak Pidana Siber (*Dittipidsiber*).⁷⁴ Adapun data yang terdapat dalam situs tersebut diperoleh dari laporan Polisi dan jumlah kasus selesai yang dilaporkan oleh *Subagbinops Ditreskrimsus* seluruh polda di Indonesia.

Data serangan *DDoS* yang telah dipaparkan diatas menunjukkan bahwa *DDoS* merupakan salah satu serangan siber yang perlu diwaspadai karena serangan ini dapat digunakan secara efektif untuk melumpuhkan website dengan cara menyerang *server* dan menghabiskan *bandwith* korban. Berdasarkan data yang diperoleh dari situs <https://livethreatmap.radware.com/> periode bulan januari 2022 menempatkan serangan *DDoS* sebagai serangan yang populer digunakan untuk melakukan serangan antar negara dengan jenis serangan *UDP Flood* sebagai serangan yang banyak digunakan dengan presentase 49%, *TCP Flood* 38%, *SYN Flood* 5%, *Http Flood*, 5%, *ICMP Flood* 3%.

⁷⁴ *Op Cit*, Polri.



Gambar 3. 4 Data Live Threat Map periode Januari 2022
sumber: livethreatmap.redware.com⁷⁵

⁷⁵ *Livethreatmap.redware.com* adalah situs yang memberikan informasi mengenai sebaran serangan siber secara langsung, informasi yang diperoleh didapatkan melalui system keamanan/aplikasi keamanan yang ter-*install* di computer korban. informasi dari system keamanan tersebut kemudian dilaporkan secara global melalui situs livethreatmap.

4. Faktor Terjadinya Serangan *DDoS Attack*

Motif dilakukannya serangan *DDoS* terhadap *website* dapat dilatarbelakangi oleh beberapa hal diantaranya yaitu:

a) Ketidaksukaan kepada pemilik website

Ketidaksukaan kepada pemilik website dapat terjadi karena adanya persaingan dalam hal eksistensi konten-konten website, hal ini dapat terjadi lantaran semakin tinggi eksistensi konten website maka akan semakin besar kemungkinan pemilik website untuk mendapatkan penghasilan dari website melalui *adsense* yang tampil pada website website.

b) Menunjukkan Eksistensi sebagai *Cracker* (perusak)

Cracker adalah sebutan untuk mereka yang masuk ke sistem orang lain untuk tujuan melakukan pengrusakan dan *cracker* lebih bersifat destruktif daripada *Hacker*. *Cracker* biasanya melakukan aksinya di jaringan komputer dengan melakukan tindakan-tindakan pengrusakan diantaranya yaitu melakukan *bypass password* atau lisensi program komputer, secara sengaja melawan keamanan komputer, mendeface (merubah halaman muka web) milik orang lain bahkan

hingga menghapus data orang lain, dan mencuri data dari sistem. Dalam dunia *cyber* umumnya para *cracker* tergabung didalam kelompok kecil atau forum yang dibentuk untuk berbagi informasi dan sebagai tempat untuk menunjukkan eksistensinya dengan menunjukkan hasil kegiatan *cracking*-nya.

- c) Adanya motif ketidaksetujuan terhadap kebijakan pemerintah

Website adalah sebuah media yang memuat segala informasi yang berada di internet, di era digital seperti sekarang ini informasi banyak disalurkan melalui website salah satunya adalah informasi mengenai pemerintahan. Situs website pemerintah seringkali dirusak oleh para *cracker* hanya karena ketidaksetujuan terhadap kebijakan pemerintah. Metode *DDoS* merupakan tindakan yang sering dilakukan selain *Deface* karena mudah dilakukan dan menghasilkan dampak yang dapat membuat website menjadi *crash*.

- d) Melakukan serangan dengan imbalan uang

Cracker biasanya juga melakukan tindakan *DDoS* terhadap suatu situs

website dengan imbalan berupa uang, hal ini dikarenakan persaingan media digital yang ketat sehingga terkadang para pemilik website memilih cara-cara tertentu untuk mengganggu system jaringan website pesaing dengan memberikan sejumlah uang kepada para cracker untuk menyerang website pesaing.

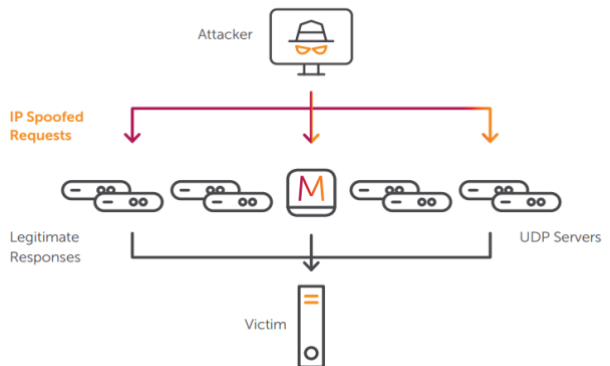
5. Jenis-jenis Metode Serangan *DDoS Attack*

Serangan siber dengan metode *DDoS Attack* berkembang seiring dengan majunya system keamanan komputer, sehingga serangan *DDoS Attack* masih digunakan sampai saat ini untuk melancarkan serangan terhadap website-website yang menjadi target operasi para penyerang, hal ini dikarenakan metode serangan *DDoS* tidak hanya memiliki satu jenis serangan namun memiliki berbagai jenis serangan yang dapat digunakan untuk menyerang *webserver*, dan target serangannya pun tidak terbatas kepada *Website* namun juga dapat digunakan untuk menyerang perangkat *Internet-connected (IoT)*, berbagai metode serangan tersebut yaitu:

1. *Memcached Amplification Attack*

Serangan *memcached* adalah jenis penguatan dari *User Datagram Protocol*

(UDP) *reflected amplification attack* serangan ini menggunakan server *memcached* rentan yang diekspos di Internet. Penyerang pertama memuat database server *memcached* kemudian mengirimkan permintaan melalui *UDP* menggunakan alamat IP palsu (target) ke ribuan server *memcached* yang terbuka di Internet. Server kemudian merespons dengan mengirimkan banyak paket *UDP* yang berasal dari port 11211 kepada target.



Gambar 3. 5 Memcached Amplification Attack

(sumber: Allot.com)

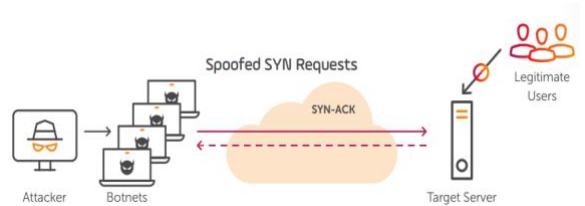
2. SYN Flood

SYN flood adalah serangan yang sering dibuat menggunakan *botnet*, serangan ini

dirancang untuk mengkonsumsi sumber daya server korban seperti *firewall* atau perimeter lainnya dalam elemen pertahanan dengan upaya untuk membanjiri batas kapasitasnya dan menurunkannya. Tujuan *synflood* adalah menerima paket SYN dengan kecepatan yang sangat tinggi yang kemudian akan cepat mengisi tabel status koneksi, yang akan berdampak terhadap pemutusan dan menjatuhkan *legitimate traffic packets*, atau bahkan lebih buruk dapat menyebabkan elemen pertahanan reboot.

SYN Flood bekerja dengan cara mengeksploitasi *TCP (Transmission Control Protocol) three-way handshake process* (proses jabat tangan tiga arah) untuk menyerang. Serangan ini kemudian membanjiri beberapa port *TCP* pada sistem target dengan pesan *SYN* yang meminta untuk memulai koneksi antara sistem sumber dan sistem sasaran. Target merespons dengan pesan *SYN-ACK* untuk setiap pesan *SYN* menerima dan membuka, sementara komunikasi port untuk koneksi yang diminta menunggu pesan *ACK* terakhir dari sumber sebagai

tanggapan untuk setiap pesan *SYN-ACK*. Penyerang tidak pernah mengirimkan *ACK* terakhir dan oleh karena itu koneksi tidak pernah selesai sehingga akan menyebabkan *timeout* dan system target akan kewalahan dalam mengatasi permintaan.



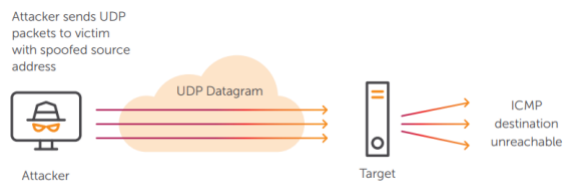
Gambar 3. 6 syn flood

(sumber: Allot.com)

3. *UDP Flood*

UDP Flood adalah serangan dengan skenario penyerang mengirim *small spoofed UDP packets* dengan kecepatan tinggi ke port acak di sistem korban menggunakan berbagai macam IP. Tindakan ini mengkonsumsi sumber daya pada elemen jaringan korban yang kewalahan oleh sejumlah besar paket *UDP* yang masuk. Biasanya server korban mulai membalas dengan *ICMP destination unreachable packets*.

Serangan *UDP* sulit untuk dideteksi dan diblokir karena sering tidak cocok dengan pola pertahanan yang konsisten, dan karena itu serangan ini efektif dalam menguras sumber daya jaringan hingga *offline*.

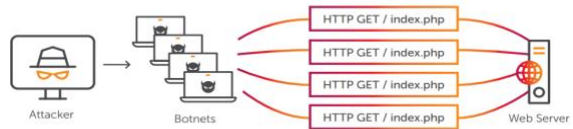


Gambar 3. 7 Udp flood
(sumber: Allot.com)

4. *HTTP Flood*

HTTP Flood membuat pengguna normal tidak dapat menggunakan sumber daya *webserver* dengan mengirimkan pesan *HTTP GET request* dengan jumlah yang besar kepada *website* yang ditargetkan. Pada kasus ini, *webserver* mencoba untuk melakukan respon terhadap *request* dari penyerang (*attacker*), tetapi penyerang tidak memproses pemberitahuan dan membiarkan *webserver* menunggu. Akibatnya *webserver* mempertahankan koneksi tunggu tersebut dengan cara

mengalokasikan sumber daya tetap untuk masing-masing koneksi selama periode waktu tertentu dan memeriksa pemberitahuan tersebut. penyerang membuat banyak *HTTP Get request* untuk *webservice* dan tidak mengembalikan pemberitahuan. Dengan demikian, *webservice* yang diserang tersebut menggunakan semua sumber daya komunikasi yang dimilikinya dan user normal tidak dapat mengakses layanan *website*.



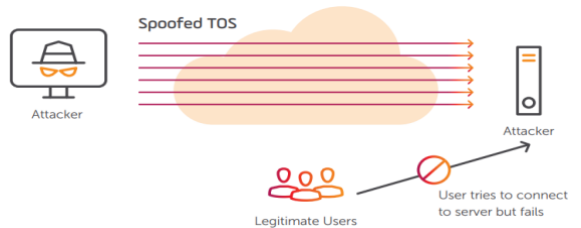
Gambar 3. 8 *http flood*

(sumber: Allot.com)

5. *TOS Flood*

TOS flood (Type of Service) merupakan serangan dengan skenario penyerang memalsukan bidang '*TOS*' dari header IP paket yang digunakan untuk *Explicit Congestion Notification (ECN)* dan *Differentiated Services (DiffServ) flags*. Terdapat dua jenis skenario serangan *TOS* yang diketahui. Pertama, penyerang

menipu *flag ECN*, yang mengurangi *throughput* koneksi individu sehingga *DDoS Allot Secure* menyebabkan server tampak tidak berfungsi atau tidak responsif. Kedua, penyerang menggunakan *flag* kelas *DiffServ* di bidang *TOS* untuk meningkatkan prioritas serangan lalu lintas melalui lalu lintas yang sah untuk mengintensifkan dampak serangan *DDoS*.



Gambar 3. 9 Tos Flood
(sumber: Allot.com)

6. NTP Amplification

NTP (Network Time Protocol) Amplification, adalah serangan dengan skenario penyerang menggunakan Infrastruktur NTP milik korban dan mengirimkan permintaan NTP kecil ke server di Internet kemudian menghasilkan volume respons NTP yang sangat tinggi. Sejak penyerang melakukan spoof

infrastruktur NTP korban semua *reflected/amplified* yang diperkuat membanjiri server NTP korban. Paket respons NTP yang menyerupai NTP asli lalu lintas, membuat serangan ini sulit dideteksi. Itulah sebabnya faktor amplifikasi dapat mencapai 50 kali sehingga menghasilkan *massive flooding* yang dapat mengambil server NTP atau seluruh jaringan *offline*.



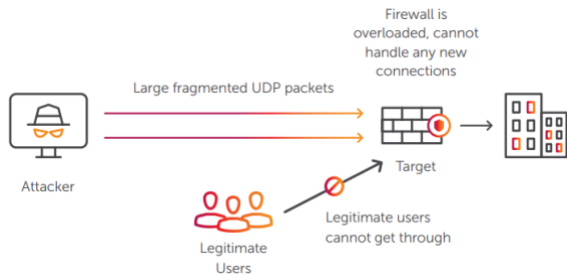
Gambar 3. 10 Ntp amplification

(sumber: Allot.com)

7. UDP Fragmentation

Serangan *UDP Fragmentation* adalah serangan yang bertujuan untuk mengirim paket UDP sekala besar (1500+ byte) kepada target yang mana hal ini kemudian akan mengkonsumsi lebih banyak *bandwidth* jaringan. Paket yang terfragmentasi biasanya tidak dapat dipasang kembali, serangan ini

mengonsumsi sumber daya yang signifikan pada perangkat *stateful* seperti *firewall* di sepanjang jalur *traffic*. Ketika serangan ini dikombinasikan dengan jenis serangan lain dapat mengakibatkan penurunan lalu lintas yang sah oleh server tujuan karena kebanjiran *traffic*.



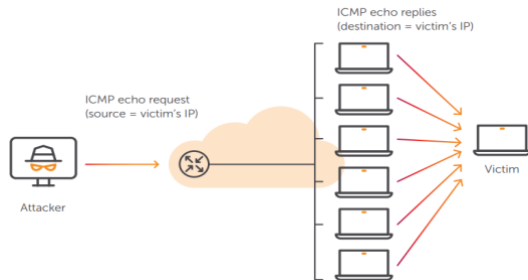
Gambar 3. 11 Udp Fragmentation

(sumber: Allot.com)

8. Ping Flood

Ping Flood adalah serangan dengan skenario penyerang mengirimkan *ICMP echo request (pings)* palsu dengan kecepatan tinggi dari *broadcast IP* atau menggunakan alamat IP korban. Sebagian besar perangkat di jaringan akan secara *default* menanggapi ping dengan mengirimkan balasan ke alamat IP sumber. Jika banyak titik akhir di jaringan yang menerima dan menanggapi ping ini,

alamat IP korban akan dibanjiri *traffic* dan perangkat/komputer/server mereka akan menjadi tidak dapat digunakan.



Gambar 3. 12 Ping flood

(sumber: Allot.com)

9. ACK Flood

ACK flood adalah serangan dengan skenario penyerang mencoba membebani server dengan paket TCP ACK. Seperti serangan *DDoS* lainnya, tujuan dari *ACK flood* adalah untuk menolak layanan ke pengguna lain dengan memperlambat atau menghancurkan target menggunakan data sampah. Server yang ditargetkan harus memproses setiap paket ACK yang diterima, yang menggunakan begitu banyak daya komputasi sehingga tidak dapat melayani pengguna yang sah.

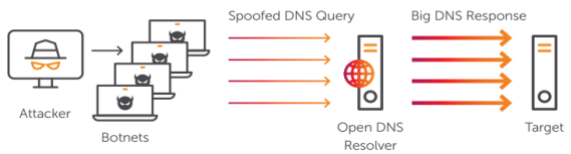


Gambar 3. 13 ACK flood

(sumber: Allot.com)

10. *DNS Flood*

DNS Flood adalah serangan dengan skenario penyerang mengirimkan permintaan DNS palsu dengan kecepatan tinggi dari berbagai *IP addresses* ke jaringan target. Pada saat permintaan tersebut terlihat sebagai permintaan valid, kemudian server DNS korban akan merespons untuk semua permintaan palsu sehingga kapasitasnya akan kewalahan oleh banyaknya permintaan. Serangan ini bertujuan untuk menghabiskan banyak *bandwidth* dan sumber daya jaringan. Pada akhirnya, serangan ini melemahkan infrastruktur DNS sampai down, mengambil *internet access* korban (WWW) dan menyebabkan *host* situs *offline*.

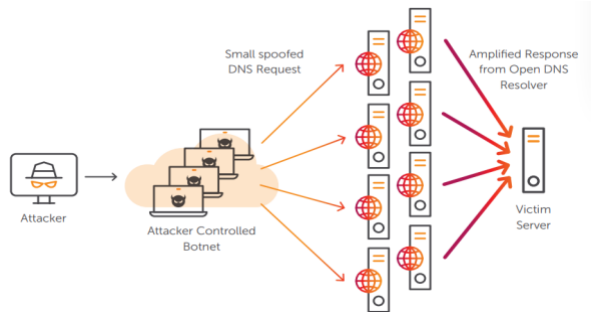


Gambar 3. 14 DNS flood

(sumber: Allot.com)

11. Amplified DNS Flood

Amplified DNS Flood adalah serangan DNS pada steroid. Serangan ini mengambil keuntungan dari *Open Recursive DNS server infrastructure* untuk membanjiri korban dengan *volume traffic* palsu yang berjumlah besar. Penyerang mengirim *small DNS requests* dengan alamat IP palsu ke *open DNS resolvers* di *Internet*. DNS resolvernya kemudian membalas alamat IP palsu dengan tanggapan yang jauh lebih besar dari permintaan. Semua *reflected/amplified responses* kembali membanjiri DNS Korban yang kemudian membuat korban *Offline*.



Gambar 3. 15 Amplified DNS flood
(sumber: Allot.com)

12. RST/FIN Flood

RST/FIN Flood adalah serangan dengan ilustrasi komunikasi sebagai berikut, ketika di TCP, paket FIN mengatakan, "Kami sudah selesai berbicara, tolong aku" dan menunggu tanggapan ACK. Paket RST mengatakan, "Sesi selesai" dan me-reset koneksi tanpa ACK. Dalam *RST/FIN flood*, penyerang mengirim *spoofed* tingkat yang tinggi *RST Packets* atau *FIN* dalam upaya untuk menghabiskan sumber daya pada sasaran. Karena paket palsu bukan milik sesi siapapun, mereka memerlukan server korban atau firewall yang mengandalkan *stateful traffic inspection*, untuk terus-menerus mencari dan mencoba mencocokkannya dengan sesi yang ada.

Pencarian sia-sia ini akhirnya membuat sumber daya sistem habis terbuang.



Gambar 3. 16 RST/FIN flood

(sumber: Allot.com)

13. SSDP Reflected Amplification Attack

Simple Service Discovery Protocol (SSDP) adalah protokol jaringan yang memungkinkan melakukan *universal plug and play (UPnP)* untuk mengirim dan menerima informasi menggunakan *UDP* pada port 1900. Sebagai protokol terbuka dan tidak aman, *SSDP* adalah target yang menarik dan rentan untuk diluncurkan serangan *DDoS*. Penyerang menggunakan bot yang terinfeksi mesin untuk mengirim paket *UPnP "discovery"* dengan alamat IP palsu dari jaringan korban. Perangkat yang rentan seperti router rumah, firewall, printer, access points dan sejenisnya. Dengan layanan *UPnP* terbuka untuk Internet (1900 port *UDP*) merespons dengan *UPnP* paket "reply" dikirim ke

alamat IP palsu dari jaringan korban. Hasilnya efektif dengan tiga puluh kali lipat (30X) Reflected Amplification DDoS attack.



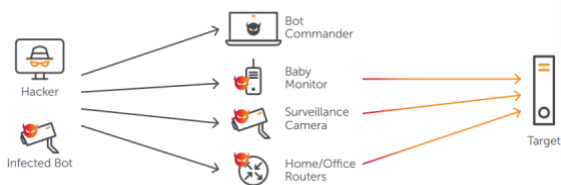
Gambar 3. 17 SSDP Reflected Amplification Attack

(sumber: Allot.com)

14. IoT Botnet Attack

Botnet IoT dibuat saat peretas menginfeksi banyak perangkat yang terhubung ke *Internet (Internet of Things)* dan merekrut mereka untuk meluncurkan serangan *DDoS* skala besar yang telah diukur dalam Terabit/dtk. Serangan ini sulit untuk di deteksi dan dilakukan mitigasi karena mereka menggunakan taktik tabrak lari yang berasal dari banyak *vektor IoT* yang didistribusikan di banyak lokasi. *Botnet IoT* menggunakan *malware source code* yang bocor pada awal 2015 dan telah disebarkan ke banyak varian. Yang paling terkenal dari ini disebut

"Mirai." Dalam serangan botnet Mirai, penyerang memindai perangkat IoT yang rentan seperti kamera pengintai digital, modem, dan pemutar DVR (dengan L4 port terbuka), dan menggunakan urutan kata sandi yang diketahui untuk mendapatkan akses. Begitu masuk, penyerang mengunduh kode berbahaya, yang memungkinkan kendali jarak jauh perangkat dan kemampuan merekrutnya untuk serangan.



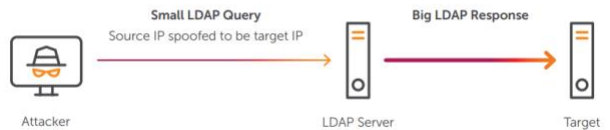
Gambar 3. 18 IOT Botnet Attack

(sumber: Allot.com)

15. LDAP Amplification Attack

LDAP Amplification Attack adalah serangan dengan skenario penyerang memanfaatkan *Lightweight Directory Access Protocol* (LDAP) yang digunakan oleh *Microsoft Active Directory* dan jutaan organisasi untuk memverifikasi informasi nama pengguna dan kata sandi

dan izin akses ke aplikasi. Penyerang mengirim permintaan kecil ke server LDAP rentan yang tersedia untuk umum dengan port TCP terbuka 389 untuk menghasilkan balasan besar ke server target. Penyerang menipu alamat IP sumber sehingga permintaan tampaknya berasal dari server target, sehingga membuat server LDAP "membalas" ke target. Penyerang memilih kueri yang akan menghasilkan balasan terbesar yang menghasilkan penguatan reflektif lima puluh kali lipat (50X) yang efektif untuk serangan *DDoS*.



Gambar 3. 19 LDAP Amplification Attack

(sumber: Allot.com)

16. CLDAP Reflection Attack

CLDAP Reflection Attack adalah serangan yang mengeksploitasi Akses *Connectionless Lightweight Directory Access Protocol* (CLDAP), yang efisien

alternatif untuk kueri LDAP melalui UDP. Penyerang mengirimkan permintaan CLDAP ke LDAP server dengan alamat IP pengirim palsu (ke IP target). Server merespons dengan respons massal ke IP target yang menyebabkan terjadinya *Reflection Attack*. Pada akhirnya, Mesin korban tidak dapat memproses data CLDAP dalam jumlah besar sekaligus. Serangan Refleksi CLDAP sangat kuat (hingga amplifikasi 70X) dan durasi pendek (*hit and run*) dan sering mengakibatkan pemadaman layanan. Mereka juga digunakan sebagai pengalih untuk pintu belakang serangan yang berusaha untuk mendapatkan data pengenalan pribadi di LDAP basis data (port 389).



Gambar 3. 20 CLDAP Reflected Attack

(sumber: Allot.com)

17. *Chargen Reflective Flood*

Chargen Reflective Flood memanfaatkan *Character Generation Protocol*. *Character Generation Protocol* awalnya dirancang untuk pemecahan masalah yang memungkinkan pengiriman nomor acak karakter. Penyerang mengirim puluhan ribu permintaan *Chargen* dengan memanfaatkan *botnet* ke satu atau lebih sistem yang dapat diakses publik yang menawarkan layanan *Chargen*. Permintaan menggunakan protokol UDP dan alamat IP palsu dari target. Layanan *Chargen* kemudian mengirimkan balasan atas permintaan tersebut dengan mengirim puluhan ribu balasan ke target. Karena protokol mengizinkan balasan ukuran acak akan ada faktor amplifikasi yang berpotensi mencapai 1024X yang kemudian hal ini akan mengganggu system target.

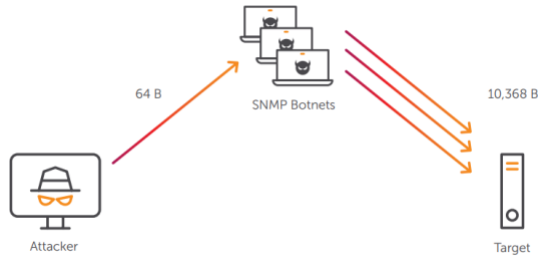


Gambar 3. 21 *Chargen Reflective flood*

(sumber: Allot.com)

18. *SNMP Reflected Amplification Attack*

SNMP Reflected Amplification Attack adalah serangan yang memanfaatkan *Simple Network Management Protocol* (SNMP) digunakan untuk mengkonfigurasi dan mengumpulkan informasi dari perangkat jaringan seperti *server, switch, router, dan printer*. Serangan ini mirip dengan serangan refleksi lainnya, penyerang menggunakan *SNMP* untuk memicu banjir/kelebihan tanggapan terhadap target. Penyerang mengirimkan sejumlah besar *kueri SNMP* dengan alamat IP palsu (target) ke banyak perangkat yang terhubung. Yang kemudian pada gilirannya perangkat akan membalas alamat palsu yang dikirimkan tersebut. *Volume* serangan akan bertambah seiring semakin banyak perangkat yang terus membalas sampai pada target jaringan diturunkan/down di bawah volume kolektif tanggapan SNMP. Tanggapan (*responses*) itu sendiri dapat sangat diperkuat dan dapat menghasilkan *volume* lalu lintas yang lebih tinggi hal ini karena adanya faktor amplifikasi yang bisa setinggi 1700.



Gambar 3. 22

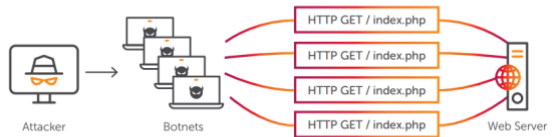
SNMP Reflected Amplification Attack

(sumber: Allot.com)

19. *Tsunami Syn Flood*

Tsunami Syn Flood adalah Serangan dengan skenario membanjiri system dengan beberapa pesan TCP SYN yang meminta untuk memulai koneksi antara sistem sumber dan target. Kemudian mengisi tabel statusnya dan menguras sumber dayanya yang dimiliki target. Serangan *Tsunami Syn Flood* merupakan serangan paket SYN yang berisi sekitar 1.000 byte per paket dibandingkan dengan jejak data yang rendah dari paket SYN biasa dan biasanya paket tersebut akan diisi oleh penyerang dengan data tertentu. Karena RFC TCP tidak membatasi jumlah data yang dapat dibawa oleh paket SYN, peretas dapat menambahkan data dan

menghasilkan paket yang lebih besar dengan faktor 25.⁷⁶



Gambar 3. 23 Tsunami flood

(sumber: Allot.com)

⁷⁶ Allot Communications, *DDoS Attack Handbook* (Allot Communications, 2018).

B. Website Sebagai Target Serangan Siber dengan Metode *DDoS Attack*

1. Pengertian Website

Secara sederhana *website* atau web dapat diartikan sebagai suatu dokumen berupa sekumpulan halaman yang berisi berbagai informasi dalam bentuk digital. Informasi tersebut dapat berupa teks, gambar, animasi, dan video.⁷⁷ Semua informasi yang terdapat pada website berada didalam jaringan internet. Internet (*Interconnected Network*) adalah sebuah sistem komunikasi global yang menghubungkan komputer-komputer dan jaringan-jaringan komputer diseluruh dunia.⁷⁸ *Website* dapat diakses menggunakan program mesin pencari (*Web Browser*) yang terdapat dalam system operasi perangkat elektronik seperti komputer dan *Smartphone*. Program yang biasa digunakan untuk mengakses *website* adalah *Google, Bing, Yandek, Firefox, Opera, Internet Exploler* dan sebagainya.

Secara lebih lanjut situs *web* atau *website* adalah sebutan untuk sekumpulan halaman *web* (*web page*), yang umumnya merupakan bagian dari suatu nama domain (*domain name*) atau

⁷⁷ *Op Cit*, Syahid.

⁷⁸ *Op Cit*, Unsurya.

subdomain pada *World Wide Web (WWW)* di Internet. Sebuah halaman website (*web page*) adalah dokumen yang ditulis dalam format *HTML (Hyper Text Markup Language)*, yang dapat diakses melalui *protocol HTTP*, yaitu protokol yang menyampaikan informasi dari *server website* untuk ditampilkan kepada para pengguna internet melalui *web browser* baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait dimana masing-masing dihubungkan dengan jaringan-jaringan halaman (*hyperlink*).⁷⁹

Website menjadi salah satu media informasi yang penting di era modern, sebagian besar instansi pemerintahan, pendidikan, dan kesehatan menyampaikan informasinya melalui website. Website memudahkan instansi untuk menyalurkan informasi dan mempermudah masyarakat mengakses informasi hanya dengan memanfaatkan mesin pencari seperti google, yahoo, bing dan yandex. *Website* dikembangkan oleh Tim Berners – Lee pada bulan oktober tahun 1990, Tim Berners - Lee membuat suatu

⁷⁹ Rudika Harminingtyas, “*Analisis Layanan Website Sebagai Media Promosi, Media Transaksi Dan Media Informasi Dan Pengaruhnya Terhadap Brand Image Perusahaan Pada Hotel Ciputra Di Kota Semarang,*” *Jurnal STIE SEMARANG*, 6.3 (2014), 37–57.

sistem informasi manajemen, di mana teks dapat berisi link dan referensi ke dokumen lain yang dapat memungkinkan pembaca untuk cepat melompat dari satu dokumen ke dokumen lain. Tim Berners – Lee juga telah menciptakan server untuk penerbitan dokumen, program ini disebut (*hypertext*) serta program untuk membacanya yang disebut *WorldWideWeb*. Perangkat lunak ini pertama kali dirilis pada tahun 1991.⁸⁰

2. Struktur Website

Website memiliki bagian-bagian yang harus ada dalam strukturnya yang mana hal itu satu sama lain fungsinya saling terikat untuk membuat website tersebut berfungsi, adapun unsur-unsur website adalah sebagai berikut⁸¹:

1. *Domain name/URL – Uniform Resource Locator*

Nama domain atau biasa disebut dengan *Domain Name* atau *URL* adalah alamat unik di dunia internet yang digunakan untuk mengidentifikasi sebuah website, atau dengan kata lain domain name adalah alamat yang digunakan untuk menemukan sebuah website pada dunia internet.

⁸⁰ *Op Cit, Community.*

⁸¹ *Op Cit, Harminingtyas.*

Berikut contoh domain name atau Url:
<https://Panduanhukum.id/>

2. *Web hosting*

Web Hosting dapat diartikan sebagai ruangan yang terdapat dalam harddisk tempat menyimpan berbagai data, file-file, gambar, video, data email, statistik, database dan lain sebagainya yang akan ditampilkan di website. Besarnya data yang bisa dimasukkan tergantung dari besarnya web hosting yang disewa/dipunyai, semakin besar web hosting semakin besar pula data yang dapat dimasukkan dan ditampilkan dalam website.

3. *Scripts Program*

Scripts Program adalah bahasa yang digunakan untuk menerjemahkan setiap perintah dalam website yang pada saat diakses. Jenis bahasa program sangat menentukan statis, dinamis atau interaktifnya sebuah website. Semakin banyak ragam bahasa program yang digunakan maka akan terlihat website semakin dinamis, dan interaktif serta terlihat bagus. Beragam bahasa program saat ini telah hadir untuk mendukung kualitas website. Jenis jenis bahasa

program yang banyak dipakai para desainer website antara lain *HTML, ASP, PHP, JSP, Java Scripts, Java applets, XML, Ajax* dsb.

4. *Web Server*

Web Server adalah sebuah sistem komputer yang menyediakan layanan tertentu dalam satu jaringan komputer. Fungsinya adalah untuk menjalankan fungsi perangkat lunak yang mengontrol akses untuk masuk ke dalam jaringan dan sumber daya yang terdapat di dalamnya. Server harus selalu disimpan di sebuah data center yang didukung oleh fasilitas lengkap agar mesin server dapat bekerja optimal saat diakses dari seluruh dunia dan tidak mudah rusak sehingga dapat bertahan lama.⁸² Pada dasarnya server adalah perangkat keras dengan banyak program perangkat lunak yang berisi daftar kode yang diperlukan untuk membuat situs web / data tersedia bagi pengguna. *Web server* akan bekerja ketika ada permintaan dari klien. Klien yang

⁸² Dicoding Intern, "Apa Itu Web Server dan Fungsinya," 27 Januari, 2021, hal. 1 <<https://www.dicoding.com/blog/apa-itu-web-server-dan-fungsinya/>> [diakses 11 Januari 2022].

dimaksud adalah pengguna pada saat melakukan akses internet melalui browser

3. Akibat Serangan *DDoS Attack* terhadap *Website*

Webserver adalah target utama dari serangan siber dengan metode *DDoS attack*, serangan ini bertujuan untuk melumpuhkan system jaringan *website* dengan cara mengirim *request* terus menerus untuk membanjiri *server* yang pada akhirnya mengakibatkan server menjadi *down, hang, bahkan crash*.

- 1) *Server Down* adalah kondisi dimana Server mengalami kegagalan system yang menyebabkan server tidak bisa diakses.
- 2) *Server hang (Hangup)* adalah kondisi dimana server tidak responsive secara local maupun jaringan.
- 3) *Server Crash* adalah kondisi dimana server mengalami kerusakan internal pada perangkat yang digunakan sebagai mesin server.

Jika server (*webservice*) mengalami kondisi *down, hang* atau *crash* maka secara otomatis *website* akan terganggu dan tidak dapat diakses oleh pengguna internet. Walaupun telah terdapat system keamanan jaringan computer

yang digunakan untuk melakukan proteksi terhadap *website* yang dirancang khusus untuk mengatasi serangan *DDoS* seperti halnya *Cloudflare*, namun hingga saat ini serangan *DDoS* masih banyak digunakan oleh para *attacker* karena serangan ini masih memiliki daya efektivitas yang cukup tinggi untuk melumpuhkan website-website yang memiliki kerentanan terhadap serangan *DDoS*.

Adapun kerugian secara materil akibat dari serangan *DDoS* tersebut adalah kerugian financial berupa biaya perbaikan *webserver*, biaya perbaikan layanan, biaya penggantian perangkat keras yang dijadikan sebagai piranti *server* dan lain sebagainya yang jumlah nominalnya tidak sedikit. Kemudian kerugian lainnya yaitu tersendatnya distribusi informasi kepada masyarakat yang mengakibatkan informasi public terhambat.

BAB IV
ANALISIS HUKUM POSITIF DAN FIQH JINAYAH
TENTANG SANKSI PIDANA KEJAHATAN SIBER
DENGAN METODE *DDOS ATTACK* TERHADAP
WEBSITE

A. Analisis Hukum Positif Tentang Sanksi Pidana
Kejahatan Siber Dengan Metode *DDoS Attack*
Terhadap *Website*

Kitab Undang-undang Hukum Pidana adalah peraturan perundang-undang yang mengatur tentang perbuatan pidana secara materil di Indonesia. Seluruh perbuatan yang masuk dalam kategori tindak pidana diatur dalam KUHP, karena dalam proses penegakan hukum setiap perbuatan pidana harus memiliki aturan dasar yang menjadi landasan atas perbuatan yang dilakukan. Dalam rangka mengidentifikasi bahwa suatu perbuatan tersebut merupakan sebuah tindak pidana atau bukan merupakan tindak pidana dapat dilihat dari adanya aturan dasar yang melarang perbuatan tersebut dan apakah terdapat ancaman pidana kepada subjek hukum atau orang melakukan tindak pidana apabila melakukan perbuatan yang dilarang.

Sehubungan dengan perbuatan pidana Muljatno mendefinisikan bahwa perbuatan pidana adalah perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu,

bagi barangsiapa yang melanggar larangan tersebut. Dapat juga dikatakan bahwa perbuatan pidana adalah perbuatan yang oleh suatu aturan hukum dilarang dan diancam pidana, asal saja dalam pada itu diingat bahwa larangan ditunjukkan kepada perbuatan (yaitu suatu keadaan atau kejadian yang ditimbulkan oleh kelakuan orang), sedangkan ancaman pidananya ditujukan kepada orang yang menimbulkan kejadian itu.

Serangan siber dengan metode *DDoS attack* merupakan suatu perbuatan pidana yang masuk dalam kategori kejahatan siber (*Cybercrime*) hal ini dikarenakan tindakan *DDoS attack* dilakukan dalam lingkup *Cyberspace* yang mana tindakan ini bertujuan untuk membuat gangguan atau pengerusakan terhadap system jaringan computer yang terhubung ke *internet* yang dalam hal ini adalah *webserver*. Tindakan *DDoS attack* dalam perbuatannya telah memenuhi unsur-unsur tindak pidana sebagaimana yang dikemukakan oleh Lamintang yaitu sebagai berikut:

a. Akibat perbuatan manusia

Serangan siber dengan metode *DDoS attack* pada dasarnya adalah perbuatan yang dilakukan oleh manusia walaupun tindakan *DDoS* dilakukan oleh *Botnet* namun pelaku penyerangan yang sebenarnya adalah manusia sehingga manusia sebagai subjek hukum dapat dikenakan pidana.

b. Adanya sifat melawan hukum dan sifat dapat dipidana

Suatu perbuatan dapat dikatakan melawan hukum apabila perbuatan tersebut bertentangan dengan undang-undang. serangan siber dengan metode *DDoS attack* merupakan perbuatan yang memiliki sifat melawan hukum karena perbuatan ini telah jelas melanggar Pasal 406 KUHP.⁸³ Pasal 30 ayat (3) dan Pasal 33 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Dalam KUHP Tindakan pengerusakan terhadap suatu barang ini diatur dalam Bab XXVII Tentang Pengerusakan Barang yang mana diatur dalam Pasal 406 ayat (1) yang menyatakan bahwa:

“Barangsiapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak tiga ratus rupiah”

Adapun unsur-unsur yang terdapat dalam Pasal 406 ayat (1) KUHP tersebut adalah sebagai berikut:

- 1) Barangsiapa

⁸³ *Op Cit*, Mathilda. *Cybercrime dalam system Hukum Indonesia..*

Pengertian “*Barangsiapa*” adalah manusia baik laki-laki maupun perempuan yang merupakan subjek hukum yang diduga ataupun terdakwa yang melakukan perbuatan pidana.

2) Dengan sengaja

Pengertian “*Dengan sengaja*” adalah perbuatan yang dilakukan atas kehendaknya dan dilakukan secara sadar oleh orang yang diduga atau terdakwa sehingga perbuatan tersebut menimbulkan akibat serta tanpa paksaan pihak ketiga.

3) Melawan Hukum

Pengertian “*Melawan Hukum*” adalah setiap perbuatan yang melanggar hukum tertulis berupa peraturan perundang-undangan atau hukum tidak tertulis berupa asas-asas hukum atau kaidah-kaidah hukum.

4) Menghancurkan

Pengertian “*Menghancurkan*” adalah tindakan merusak sehingga sama sekali suatu barang tersebut tidak dapat berfungsi sebagaimana mestinya.

5) Merusakkan

Pengertian “*Merusakkan*” adalah tindakan yang memperlakukan suatu barang namun kurang membinasakan.

6) Membikin tidak dapat dipakai atau menghilangkan barang

Pengertian “*Membikin tidak dapat dipakai atau menghilangkan barang*” adalah tindakan yang dilakukan sedemikian rupa sehingga barang tersebut tidak dapat diperbaiki lagi.

Pasal 406 ayat (1) KUHP tersebut dapat dikenakan kepada pelaku *DDoS Attack* karena unsur-unsur yang terkandung dalam Pasal ini sesuai dengan unsur-unsur tindakan *DDoS Attack* unsur-unsur tersebut adalah sebagai berikut:

- a. Pelaku *DDoS Attack* adalah manusia, walaupun dalam pelaksanaan distribusi serangan dilakukan menggunakan *Bot/computer* yang terinfeksi namun pada dasarnya pelaku dari tindakan tersebut adalah manusia sehingga manusia sebagai subjek hukum memenuhi unsur “*Barangsiapa*”.
- b. Tindakan ini dilakukan dengan sengaja hal ini dapat diketahui dari motif penyerangan yang dilakukan yaitu ketidaksukaan kepada pemilik *website*, menunjukkan eksistensi sebagai *cracker*, ketidaksetujuan terhadap kebijakan pemerintah, dan melakukan serangan dengan imbalan uang. Berdasarkan motif tersebut maka tindakan ini adalah

tindakan yang sengaja dan hal ini memenuhi unsur “*dengan sengaja*”.

- c. Tindakan ini telah jelas melawan hukum karena aturan hukum tentang tindakan pengrusakan barang ini telah termuat dalam KUHP tepatnya dalam Pasal 406 ayat (1) sehingga sesuai dengan asas legalitas.
- d. Tindakan ini dapat mengakibatkan system *webserver* mengalami *Crash* yang artinya tindakan ini bertujuan untuk mengancurkan *webserver*. Oleh karena itu unsur “*mengancurkan*” terpenuhi.
- e. Tindakan ini juga dapat menyebabkan kerusakan yang diakibatkan karena system *web server* mengalami hang (hangup) yang mana hal ini dapat menyebabkan kerusakan pada lalu lintas jaringan *webserver*.
- f. Tindakan ini dalam skala tertentu dapat menyebabkan system *webserver* mengalami *overload* yang kemudian akan berimbas pada rusaknya hardware *server* dan mengakibatkan hardware tidak dapat digunakan dan harus diganti hal ini menjadi alasan unsur unsur “*membikin tidak dapat dipakai atau menghilangkan barang terpenuhi*”.

Terpenuhinya unsur-unsur dalam Pasal 406 ayat (1) KUHP tersebut mengindikasikan bahwa Pasal tersebut tepat digunakan sebagai dasar aturan hukum terhadap tindak pidana *DDoS attack* terhadap *website*. Menurut Pasal ini pelaku tindak pidana dapat dikenakan pidana paling lama 2 (dua) tahun (8) delapan bulan atau denda paling banyak Rp 300,00 (tiga ratus) rupiah.

Aturan hukum yang lebih spesifik terkait dengan tindak pidana *DDoS attack* terhadap *website* termuat dalam Pasal 30 ayat (3) dan Pasal 33 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Undang-undang ini merupakan undang-undang yang disusun guna mendukung kemajuan teknologi informasi melalui infrastruktur hukum sebagaimana yang telah dijelaskan dalam konsiderans Undang-undang Nomor 11 Tahun 2008 yang menyebutkan bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia. Pasal 30 ayat (3) tersebut menyebutkan bahwa:

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau

Sistem Elektronik milik orang lain dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan”

Pasal 30 ayat (3) memiliki unsur-unsur sebagai berikut:

a) Setiap orang

Pengertian “*setiap orang*” dalam Pasal ini dapat diartikan sebagai manusia laki-laki atau perempuan yang merupakan subjek hukum baik individu atau kelompok yang diduga ataupun terdakwa melakukan perbuatan pidana. Dalam hal serangan *DDoS* walaupun serangannya dilakukan menggunakan bot atau program tertentu tetapi serangan tersebut sejatinya dilakukan oleh manusia.

b) Dengan Sengaja

Pengertian “*dengan sengaja*” (*Opzet*) adalah perbuatan yang dilakukan atas kehendaknya dan dilakukan secara sadar oleh diduga atau terdakwa dalam melakukan perbuatan. Pelaku *DDoS* melakukan serangan ini dengan sengaja hal ini melihat motif-motif serangan yang dilakukan oleh pelaku *DDoS* diantaranya ketidaksukaan kepada pemilik *website*, menunjukkan eksistensi sebagai *cracker*, ketidaksetujuan terhadap kebijakan pemerintah, dan melakukan serangan dengan

imbalan uang.

- c) Tanpa hak atau melawan hukum

Pengertian "*tanpa hak atau melawan hukum*" dapat diartikan sebagai suatu perbuatan yang dilakukan oleh seseorang yang tidak memiliki hak untuk melakukan perbuatan itu, melawan hukum adalah perbuatan yang bertentangan dengan aturan hukum yang berlaku. Unsur tanpa hak atau melawan hukum dalam tindakan *DDoS* dimaksudkan dalam tindakan penyerangan dan pererusakan website serta tindakan penerobosan system keamanan website.

- d) Mengakses komputer dan/atau Sistem Elektronik milik orang lain

Pengertian "*mengakses computer dan/atau system elektronik milik orang lain*" diartikan sebagai suatu tindakan yang dilakukan oleh orang yang tidak memiliki hak untuk mengakses computer atau system elektronik milik orang lain. orang lain dalam hal ini adalah orang yang memiliki hak akses computer atau system elektronik.

- e) Dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan

Pengertian "*dengan cara apapun dengan melanggar, menerobos, melampaui, atau*

menjebol sistem pengamanan” diartikan sebagai suatu tindakan yang dilakukan tidak memiliki batas kepada suatu cara atau metode tertentu dan tindakan tersebut bertujuan melanggar, menerobos, melampaui atau menjebol system pengamanan terhadap system elektronik dalam hal ini dapat berupa *firewall* atau system pengamanan tertentu yang digunakan untuk melakukan pengamanan terhadap system elektronik.

Pasal 33 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang menyebutkan bahwa:

“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”

Pasal 33 memiliki unsur-unsur sebagai berikut:

a) Setiap orang

Pengertian “*setiap orang*” dalam Pasal ini dapat diartikan sebagai manusia laki-laki atau perempuan yang merupakan subjek hukum

baik individu atau kelompok yang diduga ataupun terdakwa melakukan perbuatan pidana. Dalam hal serangan *DDoS* walaupun serangannya dilakukan menggunakan bot atau program tertentu tetapi serangan tersebut sejatinya dilakukan oleh manusia.

b) Dengan sengaja

Pengertian "*dengan sengaja*" adalah perbuatan yang dilakukan atas kehendaknya dan dilakukan secara sadar oleh diduga atau terdakwa dalam melakukan perbuatan. Pelaku *DDoS* melakukan serangan ini dengan sengaja hal ini melihat motif-motif serangan yang dilakukan oleh pelaku *DDoS* diantaranya ketidaksukaan kepada pemilik *website*, menunjukkan eksistensi sebagai *cracker*, ketidaksetujuan terhadap kebijakan pemerintah, dan melakukan serangan dengan imbalan uang.

c) Tanpa hak atau melawan hukum

Pengertian "*tanpa hak atau melawan hukum*" dapat diartikan sebagai suatu perbuatan yang dilakukan oleh seseorang yang tidak memiliki hak untuk melakukan perbuatan itu, melawan hukum adalah perbuatan yang bertentangan dengan aturan hukum yang berlaku. Unsur tanpa hak atau melawan hukum dalam tindakan *DDoS* dimaksudkan dalam tindakan

penyerangan dan pengerusakan website serta tindakan penerobosan system keamanan website.

d) Melakukan tindakan apa pun

Pengertian “*melakukan tindakan apapun*” dapat diartikan sebagai segala tindakan yang dilakukan untuk tujuan penyerangan dan tidak terbatas pada salah satu jenis serangan saja melainkan bersifat universal. Dalam hal serangan *DDoS* terhadap website jenis serangan yang digunakan untuk melumpuhkan website sangat beragam dan berkembang seiring dengan perkembangan keamanan website.

e) Terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.

Pengertian “*terganggunya sistem elektronik atau mengakibatkan sistem elektronik menjadi tidak bekerja dengan semestinya*” dapat diartikan sebagai suatu perbuatan yang dilakukan yang berakibat terhadap sistem elektronik mengalami gangguan, gangguan tersebut disebabkan atau dipicu karena adanya perbuatan seseorang yang melakukan serangan. Tidak bekerja sebagaimana mestinya adalah kondisi dimana sistem elektronik tidak berjalan sesuai dengan

keadaan normal system elektronik. Dalam hal serangan DDoS unsur terganggunya system elektronik adalah pada saat website mengalami gangguan sehingga mengakibatkan *website* tersebut tidak dapat diakses dan bekerja sebagaimana mestinya.

Berdasarkan unsur-unsur yang termuat dalam Pasal 30 ayat (3) maka Pasal ini dapat digunakan untuk jenis serangan *DDoS* yang terlebih dahulu melanggar, menerobos, melampaui, atau menjebol system pengamanan yang terdapat dalam system jaringan komputer. Adapun serangan *DDoS* yang sesuai dengan Pasal 30 ayat (3) adalah sebagai berikut:

- 1) *Memchached Amplification Attack*
- 2) *Syn flood*
- 3) *DNS flood*
- 4) *Amplified DNS flood*
- 5) *RST/FIN flood*
- 6) *SSDP Reflected Amplification Attack*
- 7) *IoT Botnet Attack*
- 8) *LDAP Amplification Attack*
- 9) *CLDAP Reflection Attack*
- 10) *Chargen Reflective Flood*
- 11) *SNMP Reflected Amplification Attack*

Sedangkan Pasal 33 dapat digunakan untuk serangan yang ditujukan langsung kepada *webserver* sebuah website

tanpa ada tindakan melanggar, menerobos, melampaui, atau menjebol system pengamanan jaringan computer. Adapun serangan *DDoS* yang termasuk dalam cakupan Pasal 33 adalah sebagai berikut:

- 1) *UDP flood*
- 2) *Http flood*
- 3) *TOS flood*
- 4) *NTP amplification*
- 5) *UDP fragmentation*
- 6) *Ping flood*
- 7) *Tsunami Syn Flood*
- 8) *ACK flood*

Adapun mengenai sanksi serangan siber dengan metode *DDoS attack* diatur dalam Pasal 46 ayat (3) dan Pasal 49 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Pasal 46 ayat (3) menyebutkan bahwa:

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)

Kemudian Pasal 49 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11

Tahun 2008 Tentang Informasi dan Transaksi Elektronik menyebutkan bahwa:

Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000,00 (sepuluh miliar rupiah)

Berdasarkan Pasal 406 KUHP, Pasal 46 ayat (3) dan Pasal 49 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik pelaku *DDoS attack* dapat dikenai sanksi pidana berdasarkan jenis serangan *DDoS* yang digunakan. Dengan demikian, telah jelas bahwa aturan hukum terhadap sanksi pidana tindakan *DDoS attack* terhadap website termuat dalam hukum positif (*ius constitutum*). Berdasarkan Pasal-Pasal tersebut para penegak hukum dapat menjatuhkan pidana kepada pelaku *DDoS attack* terhadap *website* sesuai kadar perbuatan dan kategori jenis serangan *DDoS* yang dilakukan.

B. Analisis Fiqih Jinayah Tentang Sanksi Pidana Kejahatan Siber Dengan Metode *DDoS Attack* Terhadap *Website*

Fiqih Jinayah yang juga dikenal sebagai Hukum Pidana Islam adalah suatu keilmuan yang mengatur tentang perbuatan yang diberi peringatan dan dilarang oleh syara' karena mendatangkan kemudharatan bagi agama, jiwa, akal, harta, dan keturunan yang didalamnya memuat tentang pembahasan semua jenis pelanggaran atau kejahatan manusia beserta sanksi atas perbuatan yang dilakukan.⁸⁴ Serangan siber dengan metode *DDoS* adalah perbuatan yang dikategorikan sebagai perbuatan yang mendatangkan kemudharatan terhadap harta, hal ini dapat diketahui berdasarkan dampak yang dihasilkan oleh serangan siber dengan metode tersebut yaitu merugikan pemilik *website* baik itu perorangan ataupun korporasi yang diakibatkan tidak dapat diaksesnya *website* karena *webserver website* mengalami gangguan atau kerusakan.⁸⁵

Tolak ukur penentuan dapat diberikan hukuman atau tidak terhadap suatu perbuatan dalam hukum pidana islam juga menggunakan asas legalitas. Asas legalitas dalam Islam bukan berdasarkan pada akal manusia, tetapi dari ketentuan Tuhan. Sedangkan asas legalitas secara

⁸⁴ *Op Cit*, Muhammad Nur. *Pengantar dan Asas-asas hukum pidana Islam*.

⁸⁵ *Op Cit*, Hermawan. *Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial Of Service Attack*.

jelas dianut dalam hukum Islam. Terbukti adanya beberapa ayat yang menunjukkan asas legalitas tersebut. Allah tidak akan menjatuhkan hukuman pada manusia dan tidak akan meminta pertanggungjawaban manusia sebelum adanya penjelasan dan pemberitahuan dari Rasul-Nya. Demikian juga kewajiban yang harus diemban oleh umat manusia adalah kewajiban yang sesuai dengan kemampuan yang dimiliki, yaitu taklif yang sanggup di kerjakan.⁸⁶

Dasar hukum asas legalitas dalam Islam antara lain:

Al-Qur'an surat Al-Isra': 15

مَنْ اهْتَدَىٰ فَإِنَّمَا يَهْتَدِي لِنَفْسِهِ ۗ وَمَنْ ضَلَّ
فَأِنَّمَا يَضِلُّ عَلَيْهَا ۗ وَلَا تَزِرُ وَازِرَةٌ وِزْرَ أُخْرَىٰ ۗ وَمَا
كُنَّا مُعَذِّبِينَ حَتَّىٰ نَبْعَثَ رَسُولًا

“Barangsiapa yang berbuat sesuai dengan hidayah (Allah), Maka Sesungguhnya Dia berbuat itu untuk (keselamatan) dirinya sendiri; dan Barangsiapa yang sesat Maka Sesungguhnya Dia tersesat bag(kerugian) dirinya sendiri. dan seorang yang berdosa tidak dapat memikul dosa orang lain, dan Kami tidak akan meng'azab sebelum Kami mengutus seorang Rasul”

⁸⁶ *Op Cit*, Muhammad Nur.

Al-Qur'an surat Al-Qashash: 59

وَمَا كَانَ رَبُّكَ مُهْلِكَ الْقُرَىٰ حَتَّىٰ يَبْعَثَ فِي
أُمِّهَا رَسُولًا يَتْلُو عَلَيْهِم آيَاتِنَا ۗ وَمَا كُنَّا مُهْلِكِي
الْقُرَىٰ إِلَّا وَأَهْلُهَا ظَالِمُونَ

“Dan tidak adalah Tuhanmu membinasakan kota-kota, sebelum Dia mengutus di ibukota itu seorang Rasul yang membacakan ayat-ayat Kami kepada mereka; dan tidak pernah (pula) Kami membinasakan kota-kota; kecuali penduduknya dalam Keadaan melakukan kezaliman”

Kebebasan menggunakan komputer dan mengakses internet adalah hak bagi setiap individu maupun kolektif, namun penggunaan computer dan akses internet tidak boleh digunakan untuk melakukan tindakan yang merugikan orang lain sehingga dapat menimbulkan kemudharatan. Dalam hukum islam dikenal asas Amar Makruf Nahi Mungkar asas ini merupakan rambu bagi umat islam dalam melakukan sesuatu. Dalam filsafat hukum Islam amar makruf dikenal sebagai *fungsi social engineering*, sedang nahi munkar sebagai *social control* dalam kehidupan penegakan hukum. Berdasarkan prinsip inilah di dalam hukum Islam dikenal adanya istilah

perintah dan larangan. Islam memberikan kebebasan bagi setiap penganutnya baik kebebasan individu maupun kolektif, kebebasan berpikir, kebebasan berserikat, kebebasan menyampaikan pendapat, kebebasan beragama, kebebasan berpolitik, dan lain sebagainya.

Serangan siber dengan metode *Distibuted Denial of Service attack* dalam hukum islam termasuk kedalam tindakan yang menimbulkan kemudharatan karena tindakan tersebut dilakukan untuk merusak barang milik orang lain dalam hal ini *website*. Tindakan ini merupakan jenis kejahatan baru yang lahir karena adanya perkembangan teknologi sehingga tidak ada aturan hukum yang termuat didalam Al Qur'an maupun Hadits walaupun demikian tindakan ini dapat dikenakan sanksi pidana berdasarkan aturan hukum yang lahir melalui Ijma dan Qiyas sebagaimana sumber hukum dalam islam yaitu Al Qur'an, Hadits, Ijma dan Qiyas.

Adapun aturan hukum terhadap tindakan serangan siber dengan metode *DDoS attack* terdapat dalam kaidah fiqih (*Qawaid fiqhiyah*) yang bersumber dari kitab *Al-Qawâ'id wal-Ushûl al -Jûmi'ah wal-Furûq wat-Taqâsîm al-Badî'ah an-Nâfi'ah*, karya Syaikh 'Abdur-Rahmân as-Sa'di, tahqiq: Dr.Khalid bin 'Ali bin Muhammad al-Musyaiqih, Darul wathan, cetakan II. Kaidah fikih didefinisikan sebagai ketentuan umum (dominan) yang dapat diterapkan terhadap kasus-kasus yang menjadi cakupannya agar kasus tersebut dapat

diketahui status hukumnya.⁸⁷ Kaidah fikih menghimpun persoalan-persoalan fikih dalam satu naungan berupa rumus dan ketentuan umum. Kaidah fiqih yang dimaksud adalah kaidah fiqih ke-13 (tiga belas) yang menyatakan bahwa:

الإِثْلَافُ يَسْتَوِي فِيهِ الْمُتَعَمِّدُ وَالْجَاهِلُ وَالنَّاسِي

Artinya:

“Perbuatan merusakkan barang orang lain hukumnya sama, apakah terjadi karena kesengajaan, ketidaktahuan, atau karena lupa”.

Kaidah ini memberikan patokan dalam perbuatan seseorang yang melakukan perusakan, baik kepada jiwa ataupun harta orang lain. Kaidah ini juga menjelaskan bahwa barangsiapa yang merusakkan barang orang lain tanpa alasan yang benar, maka ia wajib mengganti barang yang ia rusakkan tersebut atau membayar ganti rugi kepada pemilik harta. Sama saja, apakah kerusakan tersebut terjadi karena kesengajaan olehnya, atau karena tidak tahu atau karena lupa.⁸⁸ Kaidah tersebut di atas dapat digunakan sebagai landasan hukum terhadap tindakan *DDoS attack*

⁸⁷ Pusdatin Staimtarate, “Mengenal Ushul Fikih, Fikih, dan Kaidah Fikih,” 27 February, 2020, hal. 1 <<http://www.staimtarate.ac.id/berita/mengenal-ushul-fikih-fikih-dan-kaidah-fikih>> [diakses 25 September 2021].

⁸⁸ *Op Cit*, Manhaj.

karena pada dasarnya serangan ini tujuannya adalah untuk merusak website yang merupakan barang orang lain dengan cara membanjiri *traffic* jaringan pada *webserver* sehingga menyebabkan *webserver* mengalami kerusakan.

Berdasarkan unsur-unsur yang terdapat dalam hukum islam tindakan serangan siber dengan metode *DDoS attack* terhadap website dapat dikenakan *Jarimah* karena telah memenuhi unsur-unsur sebagai berikut:

a) *Ar-rukn asy-syar'i*

Tindakan ini telah memenuhi unsur *Ar-rukn asy-syar'i* karena tindakan ini telah jelas dilarang berdasarkan kaidah fiqih ke-13 (tiga belas) yang menyatakan bahwa perbuatan merusakkan barang orang lain hukumnya sama, apakah terjadi karena kesengajaan, ketidaktahuan, atau karena lupa.

b) *Ar-rukn al-maddi* (unsur materil)

Terpenuhinya *Ar-rukn al-maddi* hal ini dikarenakan tindakan ini secara jelas nyata adanya hal ini didasarkan atas data-data serangan siber yang terjadi dan tindakan ini dapat dilakukan oleh siapa saja yang mempunyai keahlian dalam bidang komputer atau system elektronik sehingga rukun maddi (unsur material) terpenuhi.

c) *Ar-rukun al-adabi* (unsur moril)

Terpenuhinya *Ar-rukun al-adabi* dikarenakan tindakan ini hanya dapat dilakukan oleh orang yang memiliki keahlian dalam bidang Komputer atau system elektronik, yang mana keahlian tersebut hanya dimiliki oleh orang dewasa, bukan orang dalam gangguan jiwa (ODGJ), dan tindakan ini dilakukan dengan tidak terpaksa.

Islam sebagai Agama *rahmatanlil'alamin* tentu memiliki syarat-syarat tertentu yang menjadi ukuran dalam menerapkan jarimah kepada pelaku tindak pidana. Adapun pelaku serangan siber dengan metode *DDoS attack* ini telah memenuhi syarat-syarat penerapan jarimah sehingga dapat diterapkannya jarimah. Syarat-syarat yang telah terpenuhi tersebut adalah sebagai berikut:

1) *Mukallaf*

Mukallaf adalah orang yang telah mempunyai kewajiban menjalankan syari'at atau hukum Islam. Serangan siber dengan metode *DDoS attack* pada umumnya adalah orang yang telah balig dan berakal hal ini dikarenakan dalam memahami ilmu computer dan jaringan dibutuhkan kemampuan berfikir yang mampu memahami metode serangan, pelacakan alamat IP (*internet protocol*) target dan pemahaman membaca istilah bahasa pemrograman. Dalam mempelajari itu semua diperlukan waktu yang

tidak sedikit setidaknya diperlukan waktu beberapa tahun untuk dapat mahir dalam melakukan serangan *DDoS*. Berdasarkan hal tersebut pelaku serangan siber dengan metode *DDoS attack* dapat diidentifikasi sebagai orang yang *mukallaf*.

- 2) Mempunyai kebebasan atau kemauan sendiri (tidak ada unsur keterpaksaan)

Pelaku serangan siber dengan metode *DDoS attack* jika dilihat dari motif tindakannya maka dapat diketahui bahwa pelaku tersebut tidak ada unsur keterpaksaan dalam kata lain atas kemauan sendiri dan mempunyai kebebasan. Motif tersebut diantaranya adalah karena motif ketidaksukaan kepada pemilik website, untuk menunjukkan eksistensi sebagai *cracker* (perusak) dalam komunitasnya, tidak setuju dengan kebijakan pemerintah, dan motif imbalan uang.

- 3) Dikenai aturan hukum syara' (*multazim*).

Multazim adalah pelaku harus orang yang telah dikenai hukum syara' atau disebut *multazim li al-ahkam*. *Multazim* berbeda dengan *Mukallaf* dikarenakan *Multazim* tidak terbatas kepada orang muslim saja namun juga dapat juga non muslim.

- 4) Adanya unsur kesengajaan atau niat melakukan pidana

Unsur kesengajaan atau niat melakukan pidana dalam tindakan serangan siber dengan metode *DDoS* dapat dilihat ketika pelaku telah melakukan serangan dibuktikan dengan adanya rekam jejak serangan dan aplikasi atau program yang digunakan untuk melakukan serangan *DDoS*.

Adanya landasan hukum yang terdapat dalam kaidah fiqih dan terpenuhinya unsur serta syarat penerapan jarimah di atas memberikan penegasan bahwa serangan siber dengan metode *DDoS attack* terhadap *website* dapat dikenai sanksi jarimah sehingga dapat dihukum sebagaimana mestinya. Hukuman yang dapat diberikan terhadap pelaku *DDoS attack* terhadap *website* ini adalah jenis hukuman *ta'zir*, hukuman *ta'zir* ini diberikan karena landasan hukum yang digunakan sebagai dasar aturan larangan serangan siber dengan metode *DDoS attack* terhadap *website* adalah kaidah fiqih.

Jarimah ta'zir menurut 'Audah adalah *jarimah* yang diancam dengan hukuman *ta'zir*. Dan di dalam ketentuan syari'ah, jika tidak ada batasan hukumanya, maka masuk kategori *jarimah ta'zir*, yaitu semua *jarimah* yang belum/tidak ditentukan kadar hukumannya.⁸⁹ Adapun menurut al-Mawardi *jarimah ta'zir* adalah hukuman pendidikan atas perbuatan dosa (tindak pidana)

⁸⁹ *Op Cit*, Rokhmadi. h. 193

yang belum ditentukan hukuman di dalamnya sebagaimana hukuman *hudud*.⁹⁰ Menurut 'Audah *ta'zir* dibagi menjadi tiga macam yaitu:

- 1) *Ta'zir* karena melakukan perbuatan maksiat. Yang dimaksud maksiat adalah semua perbuatan yang tidak boleh dilakukan atau wajib untuk tidak melakukannya. Para ulama' telah sepakat bahwa *ta'zir* adalah setiap perbuatan maksiat yang tidak dijatuhi hukuman (*had*) maupun *kaffarat*, baik maksiat yang menyinggung hak Allah maupun hak adami. *Ta'zir* yang menyinggung hak Allah adalah semua perbuatan yang berkaitan dengan kepentingan dan kemaslahatan umum. Sedangkan *ta'zir* yang menyinggung hak adami adalah setiap perbuatan yang mengakibatkan kerugian kepada orang tertentu, bukan orang banyak.
- 2) *Ta'zir* untuk kepentingan umum. Sedangkan lingkup *ta'zir* untuk memelihara kepentingan umum adalah semua perbuatan yang dapat merugikan atau membahayakan kepentingan umum meskipun perbuatannya bukan maksiat. Perbuatan-perbuatan yang masuk kategori ini tidak dapat ditentukan, karena perbuatan tersebut tidak diharamkan karena zatnya, melainkan karena sifatnya. Jika sifat tersebut ada, maka perbuatannya diharamkan, dan jika sifat tersebut

⁹⁰ *Ibid*, Rokhmadi.

tidak ada, maka perbuatannya tergolong *mubah*. Sifat yang menjadi alasan dikenakannya hukuman atas perbuatan tersebut adalah membahayakan atau merugikan kepentingan umum. Jika dalam suatu perbuatan terdapat unsur merugikan kepentingan umum, maka perbuatan tersebut dianggap tindak pidana dan pelakunya dikenakan hukuman. Akan tetapi, jika dalam perbuatan tersebut tidak terdapat unsur merugikan kepentingan umum, maka perbuatan tersebut bukan tindak pidana dan pelakunya tidak dapat dikenakan hukuman.

3) *Ta'zir* karena pelanggaran.

Ta'zir karena melakukan pelanggaran adalah melakukan perbuatan yang diharamkan dan meninggalkan perbuatan yang diwajibkan.⁹¹

Hukuman *ta'zir* pada dasarnya terbagi kedalam beberapa jenis hukuman, macam-macam hukuman *ta'zir* adalah sebagai berikut:

a) Hukuman Mati

Dalam jarimah *ta'zir* hukuman mati ini diterapkan oleh para fuqaha secara beragam, sebagian *fuqaha* safi'iyah membolehkan hukuman mati sebagai *ta'zir* dalam kasus penyebaran aliran-aliran sesat yang menyimpang dari ajaran al-Quran dan as-

⁹¹ *ibid*, Rokhmadi.

Sunnah. Hukuman mati untuk jarimah ta'zir hanya dilaksanakan dalam jarimah-jarimah yang sangat berat dan berbahaya, sengan syarat-syarat sebagai berikut:

- 1) Bila pelaku adalah residivis yang tidak mempan oleh hukuman-hukuman hudud selain hukuman mati.
 - 2) Harus dipertimbangkan betul-betul dampak kemaslahatan terhadap masyarakat dan pencegahan terhadap kerusakan yang menyebar dibumi.
- b) Hukuman *Jilid*

Hukuman *jilid* (cambuk) merupakan hukuman pokok dalam syariat islam untuk *jarimah hudud*, namun hanya ada beberapa jarimah yang dikenakan hukuman *jilid*, seperti *zina*, *qadzaf*, dan minum *khamar*. Hukuman *jilid* untuk *ta'zir* ini tidak boleh melebihi hukuman *jilid* dalam *hudud*. Namun mengenai batas maksimalnya tidak ada kesepakatan di kalangan *fuqaha*. Hal ini dikarenakan hukuman *had* dalam jarimah *hudud* itu berbeda-beda antara satu *jarimah* dengan *jarimah* yang lainnya. Zina hukuman jilidnya serratus kali, *Qadzaf* delapan puluh kali, sedangkan *syurbul khamar* ada yang mengatakan empat puluh kali dan ada yang delapan puluh kali.

c) Hukuman Penjara

Pemenjaraan secara *syar'i* adalah menghalangi atau melarang seseorang untuk mengatur dirinya sendiri. Baik itu dilakukan di dalam negeri, rumah, masjid, di dalam penjara, atau di tempat-tempat lain. Hukuman penjara dalam syariat islam dibagi dalam dua bagian yaitu:

- 1) Hukuman penjara yang dibatasi waktunya
- 2) Hukuman penjara yang tidak dibatasi waktunya.

d) Hukuman Pengasingan

Hukuman pengasingan merupakan salah satu jenis hukuman ta'zir. untuk jarimah-jarimah selain zina hukuman ini diterapkan apabila perbuatan pelaku dapat menjalar atau merugikan orang lain.

e) Hukuman Pemboikotan

Pemboikotan yang dimaksud dalam hal ini yaitu seorang penguasa menginstruksikan masyarakat untuk tidak berbicara dengan seseorang dengan batas waktu tertentu. Hal ini dilakukan berdasarkan dalil pada peristiwa yang menimpa tiga orang sahabat yang tidak ikut berperang. Ketika mengetahui hal itu, Rasulullah saw melarang kaum muslim untuk berbicara dengan mereka.

f) Hukuman *Salib*

Hukuman *salib* ini berlaku dalam satu kondisi, yaitu jika sanksi bagi pelaku kejahatan adalah

hukuman mati. Terhadapnya boleh dijatuhi hukuman salib. Masa penyaliban ini tidak boleh lebih dari tiga hari dan ia (terhukum) tidak dilarang untuk makan, minum, wudu, dan salat dengan isyarat.

g) Hukuman Denda (*Ghuramah*)

Hukuman denda (غرامة) bisa merupakan hukuman pokok yang berdiri sendiri dan dapat pula digabungkan dengan hukuman pokok lainnya. Penjatuhan hukuman denda Bersama-sama dengan hukuman lain bukan merupakan hal yang dilarang bagi seorang hakim yang mengadili perkara *jarimah ta'zir*, karena hakim diberi kebebasan yang penuh dalam masalah ini. Dalam hal ini hakim dapat mempertimbangkan berbagai aspek, baik yang berkaitan dengan jarimah, pelaku, situasi, maupun kondisi tempat dan waktunya. Syariat islam tidak menetapkan batas terendah atau tertinggi dari hukuman denda. Hal ini sepenuhnya diserahkan kepada hakim dengan mempertimbangkan berat ringannya jarimah yang dilakukan pelaku. Apabila seorang hakim telah menetapkan sanksi tertentu, maka ia tidak boleh membatalkan ketetapanya. Dalam kondisi terpidana tidak mampu membayar *ghuramah* (ganti rugi), maka ditunggu sampai terpidana memiliki harta, baru kemudian *ghuramah* (ganti rugi) tersebut diserahkan kepada negara.

h) Hukuman Lainnya

Disamping hukuman-hukuman yang telah disebutkan, terdapat hukuman-hukuman *ta'zir* yang lain, hukuman-hukuman tersebut adalah sebagai berikut:

- 1) Peringatan keras.
- 2) Dihadirkan di hadapan sidang.
- 3) Nasihat.
- 4) Celaan.
- 5) Pengucilan.
- 6) Pemecatan.
- 7) Pengumuman kesalahan secara terbuka.⁹²

Berdasarkan jenis *ta'zir* yang dikemukakan oleh 'Audah serangan siber dengan metode *DDoS attack* terhadap *website* termasuk kedalam kategori *ta'zir* karena perbuatan maksiat, hal ini dikarenakan tindakan merusak barang milik orang lain adalah perbuatan yang dilarang dan termasuk kedalam perbuatan maksiat kemudian jika dilihat dari dampak yang ditimbulkan oleh tindakan *DDoS attack* maka tindakan ini mengakibatkan kerugian kepada orang tertentu dalam hal ini adalah pemilik *website*. Adapun rumusan hukuman yang dapat dijatuhkan kepada pelaku *DDoS attack* sesuai dengan kaidah fiqh ke 13 (tiga belas) yang termaktub dalam kitab *Al-Qawâ'id wal-Ushûl*

⁹² *Op Cit*, Marsaid. *Al Fiqh Al Jinayah*.

al -Jûmi'ah wal-Furûq wat-Taqâsîm al-Badî'ah an-Nâfi'ah, karya Syaikh 'Abdur-Rahmân as-Sa'di, maka jenis hukumannya dapat berupa hukuman denda (*Ghurramah*).

Hukuman denda (*Ghuramah*) ini dapat dijadikan hukuman pokok ataupun hukuman tambahan bagi pelaku *DDoS attack* karena hakim memiliki kebebasan dalam menjatuhkan hukuman. Jika hukuman denda dirasa kurang memberikan efek jera maka hakim dapat memberikan hukuman pokok berupa penjara dan hukuman tambahan berupa denda (*Ghuramah*). Adapun mengenai masa hukuman penjara dan jumlah denda yang dikenakan kepada pelaku *DDoS* tergantung kepada penguasa atau hakim, karena Ciri khas dari *jarimah ta'zir* adalah hukumannya tidak tertentu dan tidak terbatas. Artinya hukuman tersebut belum ditentukan oleh syara' dan ada batas minimal dan ada batas maksimal dan penentuan hukuman *ta'zir* tersebut adalah hak penguasa.

Mengingat tindakan *DDoS attack* terhadap *website* dapat dilakukan dari berbagai lintas negara maka perlu adanya penjelasan terkait dengan yurisdiksi penjatuhan hukuman terhadap pelaku *DDoS attack* tersebut. Adapun yurisdiksi terkait dengan penjatuhan hukuman pidana terhadap pelaku *DDoS attack* menurut konsepsi asas teritorial menjelaskan bahwa dalam hukum islam memberikan aturan bahwa hukum pidana islam hanya berlaku di wilayah dimana hukum islam diberlakukan. Abu Hanifah berpendapat bahwa Hukum

Islam diterapkan atas jarimah (tindak pidana) yang dilakukan di *dar as-salam*, yaitu tempat-tempat yang masuk dalam kekuasaan pemerintahan Islam tanpa melihat jenis *jarimah* maupun pelaku, muslim maupun non-muslim. Aturan-aturan pidana Islam ini hanya berlaku secara penuh untuk wilayah-wilayah negeri muslim.⁹³

Sanksi pidana *Distributed Denial of Service Attack (DDoS Attack)* terhadap *website* memiliki persamaan dan perbedaan antara Hukum Positif dan Fiqih Jinayah. Hal yang melatarbelakangi persamaan dan perbedaan tersebut berasal dari unsur-unsur tindak pidana, aturan hukum, dan rumusan sanksi yang terdapat dalam Hukum Positif maupun Fiqih Jinayah. Adapun persamaan sanksi pidana *Distributed Denial of Service Attack (DDoS Attack)* terhadap *website* menurut hukum positif dan fiqih jinayah adalah sebagai berikut:

- a) Persamaan dari segi unsur-unsur tindakan *DDoS attack* yang terdapat dalam hukum positif dan fiqih jinayah, keduanya sama-sama mengategorikan bahwa tindakan *DDoS attack* merupakan suatu tindak kejahatan, yakni dengan membanjiri *traffic* lalu lintas jaringan *webserver* sehingga *website* mengalami kerusakan.
- b) Persamaan dari segi jenis hukuman atau sanksi pidana yang diterapkan, hukum positif memberikan rumusan hukuman penjara dan denda

⁹³ *Ibid*, Muhammad Nur. h 38.

bagi pelaku *DDoS attack* karena perbuatannya yang melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya, begitupun dengan fiqih jinayah yang memberikan rumusan hukuman denda (*ghuramah*) dan penjara dalam fiqih jinayah tindakan *DDoS attack* dikategorikan sebagai perbuatan maksiat karena bertujuan untuk merusak barang orang lain dengan sengaja.

Adapun perbedaan sanksi pidana *Distributed Denial of Service Attack (DDoS Attack)* terhadap *website* menurut hukum positif dan fiqih jinayah yaitu perbedaan dari segi penentuan berat ringannya sanksi pidana yang dijatuhkan, dalam hukum positif beratnya ringannya hukuman telah tertulis jelas dalam Pasal 406 KUHP dan Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yaitu dalam Pasal 46 ayat (3) dan 49. Hal ini berbeda dengan sanksi *DDoS attack* yang terdapat dalam fiqih jinayah yang mana berat ringannya hukuman *ta'zir* yang diberikan tergantung kepada penguasa atau hakim.

BAB V

PENUTUP

A. Simpulan

Hukum Positif dan Fiqih Jinayah merumuskan sanksi pidana kejahatan siber dengan metode *DDoS attack* terhadap *Website* sebagai berikut:

- 1) Menurut Hukum Positif Pasal 406 ayat (1) KUHP yang terdapat dalam Bab XXVII Tentang Pengerusakan Barang dengan ancaman pidana penjara 2 (dua) tahun 8 (delapan) bulan atau denda paling banyak Rp.300.00,- (tiga ratus rupiah). Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 30 ayat (3) Jo Pasal 46 ayat (3) dengan ancaman pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah) dan Pasal 33 Jo Pasal 49 dengan ancaman pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000,00 (sepuluh miliar rupiah).
- 2) Menurut Fiqih Jinayah sanksi pidana yang dapat dijatuhkan kepada pelaku *DDoS attack* terhadap *website* adalah *jarimah ta'zir* berupa hukuman denda (غرامة), apabila hukuman denda tersebut

belum memberikan efek jera maka hakim dapat memberikan hukuman tambahan berupa hukuman penjara. Adapun mengenai ketentuan batas terendah ataupun tertinggi hukuman denda dalam lingkup *jarimah ta'zir* sepenuhnya diserahkan kepada hakim dengan ketentuan Apabila seorang hakim telah menetapkan sanksi tertentu, maka ia tidak boleh membatalkan ketetapanannya. Dalam kondisi terpidana tidak mampu membayar *ghuramah* (ganti rugi), maka ditunggu sampai terpidana memiliki harta, baru kemudian *ghuramah* (ganti rugi) tersebut diserahkan kepada negara.

B. Saran

Berdasarkan hasil penelitian dan pembahasan tentang permasalahan yang diangkat dalam skripsi ini, maka rekomendasi penulis adalah sebagai berikut:

1. Kepada Pemerintah dan Masyarakat yang memiliki website agar meningkatkan sistem keamanan jaringan untuk menekan serangan siber dengan metode *DDoS attack* terhadap *website*.
2. Kepada para penegak hukum khususnya kepolisian agar meningkatkan penegakan hukum dalam bidang siber khususnya terkait dengan kasus serangan *DDoS attack* terhadap *website* di Indonesia.

3. Kepada perumus Undang-undang agar mengklasifikasikan serangan *DDoS attack* berdasarkan metode serangan agar penjatuhan sanksi pidana kepada pelaku *DDoS* dapat tepat dan adil.
4. Dalam bidang hukum islam khususnya fiqh jinayah, perlu dikembangkan lagi penggalian hukum-hukum terkait dengan kejahatan siber agar Fiqh jinayah mampu menjawab permasalahan hukum baru dalam bidang Teknologi Informasi dikemudian hari.
5. Penelitian ini diharapkan dapat menjadi referensi bagi para penegak hukum, akademisi dan masyarakat dalam upaya menegakkan hukum dan keadilan dan melengkapi penelitian terdahulu.

DAFTAR PUSTAKA

- Allot Communications, *DDoS Attack Handbook* (Allot Communications, 2018)
- Cisco.com, “Cisco Annual Internet Report (2018-2-23) White Paper,” *09 March*, 2020, hal. 1 <<https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html?dtid=ossdc000283>> [diakses 7 Januari 2022]
- Community, W3C, “The History Of The Web,” *4 March*, 2012, hal. 1 <w3.org/community/webed/wiki/The_history_of_the_Web> [diakses 20 Agustus 2021]
- Fadillah, Abdul Azmi, “Aktivitas Komunikasi Lingkar Ganja Nusantara Bandung Melalui Cyberspace,” *Program Studi Ilmu Komunikasi, Fakultas Sosial Politik, Universitas Komputer Indonesia*
- FOCUS, NS, *2020 DDOS ATTACK LANDSCAPE*, 2020 <<https://nsfocusglobal.com/company-overview/resources/2020-ddos-attack-landscape-report/>>
- Geges, Septian, dan Waskitho Wibisono, “Pengembangan Pencegahan Serangan Distributed Denial of Service (Ddos) Pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis Dan Client Puzzle,” *JUTI: Jurnal Ilmiah Teknologi Informasi*, 13.1 (2015), 53 <<https://doi.org/10.12962/j24068535.v13i1.a388>>
- Gutnikov, Alexander, Oleg Kupreev, dan Yaroslav Shemeley, “DDoS Attack In Q3 2021,” *scurelist.com*, 2021, hal. 1 <<https://scurelist.com/ddos-attacks-in-q3-2021/104796/>> [diakses 5 Januari 2022]
- Hakim, Lukman, *Asas-Asas Hukum Pidana*, 1 ed. (Jakarta: deepublish publisher, 2020)
- Harminingtyas, Rudika, “Analisis Layanan Website Sebagai Media Promosi, Media Transaksi Dan Media Informasi Dan Pengaruhnya Terhadap Brand Image Perusahaan Pada Hotel Ciputra Di Kota Semarang,” *Jurnal STIE SEMARANG*, 6.3

(2014), 37–57

- Hermawan, Rudi, “Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos),” *Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos)*, 5.1 (2013), 1–14
- Intern, Dicoding, “Apa Itu Web Server dan Fungsinya,” 27 Januari, 2021, hal. 1 <<https://www.dicoding.com/blog/apa-itu-web-server-dan-fungsinya/>> [diakses 11 Januari 2022]
- Jamil, Peresensi M, “Resensi : “ Cyber Crime (Akar Masalah , Solusi , Dan Penanggulangannya),” April 2010, 2017, 1–14
- Kemendikbud, Spada, “Definisi Cyber Crime,” 24 March, 2021 <<https://lmsspada.kemdikbud.go.id/mod/page/view.php?id=57347&forceview=1>> [diakses 20 Agustus 2021]
- Manhaj, Al, “Kaidah Ke. 13 : Perbuatan Merusakkan Barang Orang Lain Hukumnya Sama,” *Al-Qawâ'id wal-Ushûl al-Jûmi'ah wal-Furûq wat-Taqâsîm al-Badi'ah an-Nâfi'ah, karya Syaikh 'Abdur-Rahmân as-Sa'di, Tahqîq: Dr. Khâlid bin 'Ali bin Muhammad al-Musyâiqih, Dârul-Wathan, Cetakan II, Tahun 1422 H – 2001 M*, hal. 1 <<https://almanhaj.or.id/2512-kaidah-ke-13-perbuatan-merusakkan-barang-orang-lain-hukumnya-sama.html>> [diakses 18 September 2021]
- Marsaid, *Al-Fiqh Al-Jinayah (Hukum Pidana Islam)*, ed. oleh Jauhari, 1 ed. (Palembang: RAFFAH Press, 2020)
- Mathilda, Fiorida, “Cyber Crime Dalam Sistem Hukum Indonesia Cyber Crime in Indonesia Law System,” *SIGMA-Mu - Jurnal Publikasi Hasil Penelitian dan Gagasan Ilmiah Multidisiplin*, 2.2 (2012), 34–45 <<https://jurnal.polban.ac.id/index.php/sigmamu/article/view/870>>
- Moeljatno, *Kitab Undang-Undang Hukum Pidana* (Jakarta: PT. Bumi Aksara, 2014)
- Muhammad Nur, *Pengantar dan Asas-asas Hukum Pidana Islam*, 2020
- Multatuli, Project, *Kami mohon maaf. Situs kami tak bisa diakses penuh lantaran serangan DDoS sejak semalam, usai*

- menerbitkan artikel “Tiga Anak Saya Diperkosa,” 06 Oktober, 2021 <https://twitter.com/projectm_org> [diakses 20 Oktober 2021]
- Nasution, Endah Octaviana, dan Achmad Basuki, “Implementasi Algoritme C5 . 0 Untuk Klasifikasi Serangan DDoS,” 5.1 (2021), 389–95
- Naufal, M., dan M. Sofwan Jannah, “Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif Dan Hukum Islam,” *Al-Mawarid Journal of Islamic Law*, 12.1 (2012), 69–84
- Polri, Siber, “Data Statistik Laporan Masyarakat Melalui Portal Patroli Siber,” 20 Oktober, 2021, hal. 1 <<https://patrolisiber.id/statistic>> [diakses 20 Oktober 2021]
- Rokhmadi, *Hukum Pidana Islam*, 1 ed. (Semarang: CV. Karya Abadi Jaya, 2015)
- Sofyan, Andi, dan Nur Azisa, *Buku Ajar Hukum Pidana*, 1 ed. (Makasar: Pustaka Pena Press, 2020) <<https://doi.org/10.21070/2020/978-623-6833-81-0>>
- Southern District of California, Department of Justice U.S. Attorney’s Office, “Utah Man Sentenced for Computer Hacking Crime,” 2 July, 2019, hal. 1 <<https://www.justice.gov/usao-sdca/pr/utah-man-sentenced-computer-hacking-crime>> [diakses 21 Oktober 2021]
- Staimtarate, Pusdatin, “Mengenal Ushul Fikih, Fikih, dan Kaidah Fikih,” 27 February, 2020, hal. 1 <<http://www.staimtarate.ac.id/berita/mengenal-ushul-fikih-fikih-dan-kaidah-fikih>> [diakses 25 September 2021]
- Subagyo, Joko, *Metode Penelitian dalam Teori dan Praktek* (Jakarta: PT. Rineka Cipta, 2006)
- Suteki, dan Galang Taufani, *Metodologi Penelitian Hukum (Filsafat, Teori, dan Praktik)*, 3 ed. (Depok: Raja Grafindo Persada, 2020)
- Suyanto, *Pengantar Hukum Pidana*, 1 ed. (Yogyakarta: deepublish, 2018)
- Syahid, Bilal, “Pengertian Website – Sejarah, Jenis, Manfaat, Unsur, Tahapan, Fungsi, Para Ahli,” 07 November, 2021, hal. 1 <<https://www.gurupendidikan.co.id/pengertian-website/>>

[diakses 20 Agustus 2021]

Takdir, *Mengenal Hukum Pidana*, ed. oleh Tahmid Nur, 1 ed. (Sulawesi selatan: Penerbit Laskar Perubahan, 2013)

Unsurya, Puskominfo, “Definisi Dan Perbedaan Internet, Intranet Dan Extranet,” 25 February, 2014, hal. 1 <<https://universitassuryadarma.ac.id/definisi-dan-perbedaan-internet-intranet-dan-extranet/>> [diakses 20 Agustus 2021]

Wardi Muslich, Ahmad, *Hukum Pidana Islam*, cetakan ke (Jakarta: Sinar Grafika Offset, 2016)

Widagdo, Setiawan, *Kamus Hukum*, ed. oleh Umi Athelia Kurniati, 1 ed. (Jakarta: PT. Prestasi Pustaka Raya, 2012)

Zainuddin, *Pengantar Hukum Pidana Islam* (Yogyakarta: CV. Budi Utama, 2019)

DAFTAR RIWAYAT HIDUP

A. DATA PRIBADI

Nama : Eko Wahyu Ramadani
Tempat, tanggal lahir : Marga mulia, 22 Desember 1999
Jenis kelamin : Laki-laki
Agama : Islam
Status : Belum kawin
Alamat rumah : Ds. Marga mulia RT 02/RW 01
Kec. Rambang Kab. Muara
Enim Prov. Sumatera Selatan
Alamat Kos : jl. Kliwonan Baru 2 RT 07/ RW
07 Kel. Tambak aji Kec. Ngaliyan
Kota Semarang Jawa Tengah
No. Telepon : 081548718028
Motto : Dan janganlah kamu berbuat
kerusakan di bumi setelah
(diciptakan) dengan baik

DATA PENDIDIKAN

1. Pendidikan Formal
 - a. Tahun 2006-2012 SDN 12 Rambang
 - b. Tahun 2012-2015 SMPN 1 Tanjung sari Lampung Selatan
 - c. Tahun 2015-2018 MA Baitul Kirom Lampung Selatan

2. Pendidikan Non formal
 - a. Pon-pes Baitul Kirom Lampung Selatan

B. PENGALAMAN ORGANISASI

1. PMII Rayon Syariah
2. HMJ HPI
3. Lembaga Riset dan Debat

C. HOBBY

1. Menulis

Demikian daftar riwayat hidup ini saya buat dengan sebenar-benarnya dan dapat dipertanggungjawabkan

Semarang, 23 Maret 2022



Eko Wahyu Ramadani

1802026009