

**PENERAPAN ALAT BUKTI DALAM TINDAK
PIDANA INFORMASI DAN TRANSAKSI
ELEKTRONIK DI KEPOLISIAN DAERAH
SUMATERA UTARA**

SKRIPSI

*Diajukan Guna Memenuhi Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Hukum (S.H)
Program Studi Ilmu Hukum*

Oleh:

DANIEL ORTEGA
NPM 1306200315



**FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2018**



Ilmu, Cerdas dan Berprestasi

MAJELIS PENDIDIKAN TINGGI, PENELITIAN & PENGEMBANGAN
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM

Jalan Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474

Website : <http://www.umsu.ac.id> E-mail : rektor@umsu.ac.id

Bankir : Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

BERITA ACARA
UJIAN MEMPERTAHANKAN SKRIPSI SARJANA
BAGI MAHASISWA PROGRAM STRATA I

Panitia Ujian Sarjana Strata I Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dalam sidangnya yang diselenggarakan pada hari Kamis, tanggal 18 Oktober 2018, Jam 08.30 WIB sampai dengan selesai, setelah mendengar, melihat, memperhatikan menimbang:

MENETAPKAN

NAMA : DANIEL ORTEGA
NPM : 1306200315
PRODI/BAGIAN : ILMU HUKUM/HUKUM ACARA
JUDUL SKRIPSI : PENERAPAN ALAT BUKTI DALAM TINDAK PIDANA
INFORMASI DAN TRANSAKSI ELEKTRONIK DI
KEPOLISIAN DAERAH SUMATERA UTARA

Dinyatakan : (A) Lulus Yudisium dengan predikat Istimewa
() Lulus Bersyarat, memperbaiki/Ujian Ulang
() Tidak Lulus

Setelah lulus, dinyatakan berhak dan berwenang mendapatkan gelar Sarjana Hukum (SH) dalam BAGIAN HUKUM ACARA.

PANITIA UJIAN

Ketua

Sekretaris

IDA HANIFAH, S.H., M.H
NIDN: 0003036001

FAISAL, S.H., M.Hum
NIDN: 0122087502

ANGGOTA PENGUJI:

1. M. SYUKRAN YAMIN LUBIS, S.H., CN., M.Kn 1
2. ATIKAH RAHMI, S.H., M.H
3. MUKHLIS IBRAHIM, S.H., M.H
4. AVRIZAL HAMDHY KUSUMA, S.H., M.H

1.

2.

3.

4.



Ilmu, Cerdas dan Berprestasi

MAJELIS PENDIDIKAN TINGGI, PENELITIAN & PENGEMBANGAN
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM

Jalan Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474

Website : <http://www.umsu.ac.id> E-mail : rektor@umsu.ac.id

Bankir : Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

PENDAFTARAN UJIAN SKRIPSI

Pendaftaran Skripsi Sarjana Fakultas Hukum Universitas Muhammadiyah Sumatera Utara Strata I bagi:

NAMA : DANIEL ORTEGA
NPM : 1306200315
PRODI/BAGIAN : ILMU HUKUM/HUKUM ACARA
JUDUL SKRIPSI : PENERAPAN ALAT BUKTI DALAM TINDAK PIDANA
INFORMASI DAN TRANSAKSI ELEKTRONIK DI
KEPOLISIAN DAERAH SUMATERA UTARA

PENDAFTARAN : Tanggal 17 Oktober 2018

Dengan diterimanya Skripsi ini, sesudah lulus dari Ujian Komprehensif, penulis berhak memakai gelar:

SARJANA HUKUM
BAGIAN HUKUM ACARA

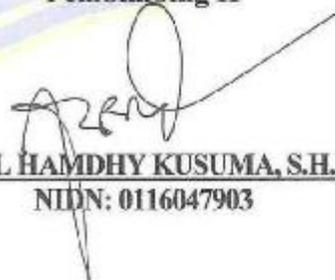
Diketahui
Dekan


IDA HANIYAH, S.H., M.H
NIDN: 0003036001

Pembimbing I


MUKHLIS IBRAHIM, S.H., M.H
NIDN: 0114096201

Pembimbing II


AVRIZAL HAMDHY KUSUMA, S.H., M.H
NIDN: 0116047903



Wajiz, Cerdas dan Berprestasi

MAJELIS PENDIDIKAN TINGGI, PENELITIAN & PENGEMBANGAN
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM

Jalan Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474

Website : <http://www.umsu.ac.id> E-mail : rektor@umsu.ac.id

Bankir : Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

LEMBAR PERSETUJUAN PEMBIMBING

NAMA : DANIEL ORTEGA
NPM : 1306200315
PRODI/BAGIAN : ILMU HUKUM/HUKUM ACARA
JUDUL SKRIPSI : PENERAPAN ALAT BUKTI DALAM TINDAK PIDANA
INFORMASI DAN TRANSAKSI ELEKTRONIK DI
KEPOLISIAN DAERAH SUMATERA UTARA

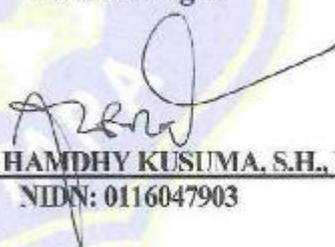
Disetujui Untuk Disampaikan Kepada
Panitia Ujian

Medan, 15 Oktober 2018

Pembimbing I

Pembimbing II


MUKHLIS IBRAHIM, S.H., M.H
NIDN: 0114096201


AVRIZAL. HAMDHY KUSUMA, S.H., M.H
NIDN: 0116047903

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini:

Nama : Daniel Ortega
NPM : 1306200315
Program : Strata – I
Fakultas : Hukum
Program Studi : Ilmu Hukum
Bagian : Hukum Acara
Judul : PENERAPAN ALAT BUKTI DALAM TINDAK PIDANA
INFORMASI DAN TRANSAKSI ELEKTRONIK DI
KEPOLISIAN DAERAH SUMATERA

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis ini secara keseluruhan adalah hasil penelitian/karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya.

Dan apabila ternyata di kemudian hari skripsi ini merupakan hasil plagiat atau merupakan karya orang lain, maka dengan ini saya menyatakan bersedia menerima sanksi akademik dari Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.

Medan, ` Oktober 2018

Saya yang menyatakan



DANIEL ORTEGA



Ilmu, Cerdas dan Terpercaya

MAJELIS PENDIDIKAN TINGGI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM

Jalan Kapten M. H. Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474
Website : <http://www.umsu.ac.id> E-mail : rektor@umsu.ac.id
Bankir : Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut.

KARTU BIMBINGAN
SKRIPSI MAHASISWA

Nama Mahasiswa : DANIEL ORTEGA
NPM : 1306200315
Prodi/Bagian : Ilmu Hukum/Hukum Acara
Judul Skripsi : PENERAPAN ALAT BUKTI DALAM TINDAK PIDANA
INFORMASI DAN TRANSAKSI ELEKTRONIK DI
KEPOLISIAN DAERAH SUMATERA UTARA

Pembimbing I : MUKLIS IBRAHIM, S.H., M.H
Pembimbing II : AVRIZAL HAMDHY KUSUMA, S.H., M.H

TANGGAL	MATERI BIMBINGAN	KONS. LANJUTAN	PARAF
07 Juli 2017	Penelitian tentang Keadilan BABS ditambah dengan teknologi Kendala dan pengutipan sumber metode penelitian		[Signature]
11 Agustus 2017	Metode Penelitian & BABS III		[Signature]
14 September 2017	BABS III + BAB IV dan Abstrak diteliti kegunaan penelitian		[Signature]
24 September 2017	Ace Stagekita ke Paralel I		[Signature]
01-10-2018	di terima Skripsi untuk di kembali		[Signature]
13-10-2018	perbaiki hasil kutipan literatur di-mulai		[Signature]
15-10-2018	mulai di kembalikan dan bimbingan di uph		[Signature]

Diketahui Dekan

Pembimbing I

Pembimbing II

[Signature]
(IDA HANIFAH, S.H., M.H)

[Signature]
(MUKLIS IBRAHIM, S.H., M.H)

[Signature]
(AVRIZAL HAMDHY KUSUMA, S.H., M.H)

ABSTRAK

PENERAPAN ALAT BUKTI DALAM TINDAK PIDANA INFORMASI DAN TRANSAKSI ELEKTRONIK DI KEPOLISIAN DAERAH SUMATERA UTARA

DANIEL ORTEGA
NPM: 1306200315

Aparat penegak hukum dihadapkan pada kesulitan untuk menentukan kualifikasi kejahatan apakah yang dapat dituduhkan pada pelaku *cybercrime* atau tindak pidana informasi dan transaksi elektronik, mengingat sukarnya menemukan serta menerapkan alat bukti. Sementara itu, pesatnya teknologi informasi melalui internet telah mengubah aktivitas-aktivitas kehidupan yang semula perlu dilakukan dengan kontak fisik, kini dengan menggunakan media informasi dan teknologi, aktivitas keseharian dapat dilakukan secara virtual atau maya. Masalah sulit yang dihadapi penegak hukum saat ini adalah bagaimana menjangkit pelaku *cybercrime* yang mengusik rasa keadilan tersebut dikaitkan dengan sistem hukum acara pidana yang berlaku. Tujuan penelitian ini untuk mengetahui Proses penerapan alat bukti dalam tindak pidana ITE di Kepolisian Daerah Sumatera Utara, Kendala yang dihadapi oleh Kepolisian dalam menerapkan alat bukti tindak pidana ITE, serta upaya yang dilakukan untuk mengatasi kendala yang dihadapi dalam menerapkan alat bukti tindak pidana ITE.

Penelitian ini bersifat deskriptif dengan pendekatan yuridis empiris, sumber data yang digunakan untuk mendukung penelitian ini adalah sumber data sekunder yang meliputi bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

Berdasarkan hasil penelitian dan pembahasan dapat diketahui bahwa Proses penerapan alat bukti tindak pidana ITE di Kepolisian Daerah Sumatera Utara diawali dengan proses penyelidikan dan penyidikan. Dimana, pada tahap penyidikan pihak kepolisian akan melakukan penggeledahan dan penyitaan terhadap alat bukti elektronik. Kemudian alat bukti elektronik tersebut akan dilakukan pemeriksaan melalui proses tahapan digital forensik yaitu Pengambilan (*acquisition*), Pemeriksaan dan analisa, Dokumentasi dan presentasi. Selanjutnya, pihak penyidik akan meminta keterangan ahli dan keterangan dari saksi. Kendala yang dihadapi oleh kepolisian dalam menerapkan alat bukti tindak pidana ITE adalah Kurang memadainya peralatan di SUBDIT II/ Unit *CYBER CRIME*, Alat bukti yang terdapat dalam komputer mudah terhapus dan hilang sehingga sulit untuk dilakukan *cloning*. Dan mayoritas Pelaku menggunakan identitas palsu. Upaya untuk mengatasi kendala tersebut adalah mengupayakan penambahan peralatan yang canggih, melakukan kerja sama dengan *proveder* atau kementerian komunikasi dan informatika republik indonesia (KOMINFO).

Kata kunci: Penerapan, Alat Bukti, Tindak Pidana Informasi Dan Transaksi Elektronik..

DAFTAR ISI

LEMBARAN PENDAFTARAN

LEMBARAN BERITA ACARA UJIAN

PERNYATAAN KEASLIAN

KATA PENGANTAR

DAFTAR ISI

ABSTRAK

BAB I : PENDAHULUAN.....	1
A. Latar Belakang.....	1
1. Rumusan Masalah	5
2. Faedah Penelitian	6
B. Tujuan Penelitian	7
C. Metode Penelitian	7
1. Sifat Materi Peneltian.....	7
2. Sumber Data.....	8
3. Alat Pengumpul Data	8
4. Analisis Data.....	9
D. Definisi Operasional	9
BAB II : TINJAUAN PUSTAKA.....	11
A. Alat Bukti	11
B. Tindak Pidana Informasi Dan Transaksi Elektronik.....	25

BAB III: HASIL PENELITIAN DAN PEMBAHASAN.....	32
A. Proses penerapan alat bukti dalam tindak pidana informasi dan transaksi elektronik di Kepolisian Daerah Sumatera Utara	32
B. Kendala yang dihadapi oleh Kepolisian dalam menerapkan alat bukti tindak pidana informasi dan transaksi elektronik	61
C. Upaya yang dilakukan oleh Kepolisian dalam mengatasi kendala yang dihadapi dalam menerapkan alat bukti tindak pidana informasi dan transaksi elektronik.....	65
BAB IV : HASIL KESIMPULAN DAN SARAN	
A. Kesimpulan.....	68
B. Saran.....	70

DAFTAR PUSTAKA

KATA PENGANTAR



Assalamualaikum Wr. Wb.

Syukur Alhamdulillah, karena berkat dan rahmat -Nya, skripsi ini dapat diselesaikan dengan tepat waktu. Skripsi ini disusun dan diajukan untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Hukum di Fakultas Hukum Universitas Muhammadiyah Sumatera Utara Medan. Sehubungan dengan itu, disusun skripsi yang berjudul: **penerapan alat bukti dalam tindak pidana informasi dan transaksi elektronik di kepolisian daerah sumatera utara**

Dengan selesainya skripsi ini, perkenankanlah diucapkan terimakasih yang sebesar-besarnya kepada: Rektor Universitas Muhammadiyah Sumatera Utara Bapak Drs. Agussani, MAP atas kesempatan dan fasilitas yang diberikan untuk mengikuti dan menyelesaikan pendidikan program Sarjana ini. Dekan Fakultas Hukum Universitas Muhammadiyah Sumatera Utara Ibu Hj. Ida Hanifah, SH., M.H atas kesempatan menjadi mahasiswa Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Demikian juga halnya kepada Wakil Dekan I Bapak Faisal, SH., M.Hum. dan Wakil Dekan III Bapak Zainudin SH.,M.H

Terimakasih yang tak terhingga dan penghargaan yang setinggi-tingginya diucapkan kepada Bapak Muklis Ibrahim, SH., M.H selaku Pembimbing I, dan Bapak Avrizal hamdhy kusuma, SH., M.H selaku Pembimbing II, yang dengan penuh perhatian telah memberikan dorongan, bimbingan dan saran sehingga skripsi ini selesai.

Disampaikan juga penghargaan kepada seluruh staf pengajar dan staff biro administrasi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Tak

terlupakan disampaikan kepada seluruh narasumber yang telah memberikan data selama penelitian berlangsung, sehingga atas bantuan dan dorongannya skripsi ini dapat diselesaikan.

Demikian juga kepada temanku Faddel, Imam, Faiz, Cimeng, Ihsan, Ilham, dan yang tidak dapat disebutkan satu persatu namanya yang turut memotivasi dan membantu untuk menyelesaikan skripsi ini.

Akhirnya diharapkan semoga skripsi ini dapat bermanfaat bagi diri sendiri maupun pembaca sekalian.

Wassalamualaikum, Wr. Wb.

Medan, oktober 2018
Hormat saya,

Daniel ortega
1306200315

BAB I

PENDAHULUAN

A. Latar Belakang

Kemajuan teknologi informasi sekarang dan kemungkinannya di masa yang akan datang tidak lepas dari dorongan yang dilakukan oleh perkembangan teknologi komunikasi dan teknologi komputer. Perpaduan teknologi komunikasi dan teknologi komputer melahirkan internet yang menjadi tulang punggung teknologi informasi.

Internet merupakan sebuah dimensi baru dalam kehidupan manusia. Internet adalah sebuah alat penyebaran informasi secara global, sebuah mekanisme penyebaran informasi dan sebuah media untuk berkolaborasi dan berinteraksi antar-individu dengan menggunakan komputer tanpa terhalang batas geografis.

Perkembangan penggunaan Internet yang ditandai oleh pertumbuhan perusahaan-perusahaan penyedia jasa internet dan meningkatnya jumlah pengguna jasa ini, tidak disertai dengan perkembangan hukum di bidang ini. Demikian pula dengan perkembangan zaman, banyak kejahatan konvensional dilakukan dengan modus operandi yang canggih dalam proses beracara diperlukan teknik atau prosedur khusus untuk mengungkap suatu kejahatan.

Perkembangan teknologi pada saat ini memunculkan berbagai media komunikasi yang sangat cepat dalam memberikan berbagai informasi dalam ruang dan waktu yang sangat singkat. Penemuan alat komunikasi berupa komputer memunculkan suatu sistem komunikasi baru yang sering disebut jaringan kerja

(*network*) yang bisa diakses melalui internet dengan menggunakan komputer. Kehadiran teknologi komunikasi memberikan kemudahan dan manfaat yang besar kepada manusia sebagai pengguna yakni untuk membantu menyelesaikan permasalahan terhadap kegiatan-kegiatan yang dilakukan manusia dari tingkat kesulitan yang sederhana hingga yang kompleks, hal ini guna tercapainya efektivitas dan efisiensi dalam setiap kegiatan penyelesaian permasalahan yang dihadapi manusia, khususnya komunikasi.

Seiring dengan semakin pesatnya perkembangan komunikasi melalui internet, memunculkan pula berbagai kejahatan yang dilakukan dengan media internet. Tidak dapat dipungkiri bahwa penggunaan internet yang canggih dan cepat tersebut memunculkan pula kejahatan yang sangat canggih dan sulit untuk diketahui pelakunya. Hal ini disebabkan karena internet merupakan suatu media komunikasi yang tidak terlihat (*maya*), sehingga pelaku kejahatan dapat dengan mudah menghilangkan jejak tanpa dapat diketahui dengan jelas.

Terlepas dari manfaat yang diperoleh dengan kemajuan teknologi di bidang komputer, belakangan muncul persoalan ketika jaringan-jaringan komputer yang dipergunakan oleh berbagai pihak tersebut disalahgunakan oleh pihak-pihak tertentu untuk kepentingan yang berseberangan, atau dikenal dengan kejahatan komputer (*computer crime*). Dalam istilah lain, kejahatan ini lebih dikenal dengan *cyber crime* atau Tindak Pidana Informasi dan Transaksi Elektronik.

Sebelum disahkannya Undang-undang tentang Informasi dan Transaksi Elektronik, salah satu hal yang menjadi kendala dalam penanganan praktik tindak

pidana dunia maya ini adalah bahwa bukti-bukti berupa software, data elektronik, atau data dalam bentuk elektronik (*elektronik evidence*) lainnya yang belum dapat diterima sebagai alat bukti dalam hukum Indonesia. Sebagai cabang ilmu hukum, Hukum Siber termasuk sangat baru. Hukum Siber bertumpu pada disiplin-disiplin ilmu hukum yang telah lebih dulu ada. Beberapa cabang ilmu hukum yang menjadi pilar hukum siber adalah Hak Atas Kekayaan Intelektual, Hukum Perdata Internasional, Hukum Perdata, Hukum Internasional, Hukum Acara dan Pembuktian, Hukum Pidana Internasional, Hukum Telekomunikasi, dan lain-lain.¹

Cyber crime memiliki sifat efisien dan cepat serta sangat menyulitkan bagi pihak penyidik dalam melakukan penyidikan terhadap tindak pidana cyber crime terutama dalam proses pengumpulan alat bukti. Di dalam penyidikan berdasarkan Pasal 1 angka 2 KUHAP, penyidik/polisi mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya.

Alat bukti adalah segala sesuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat-alat bukti tersebut dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan oleh terdakwa. Penyidik harus lebih dulu memperoleh atau mengumpulkan bukti permulaan atau probable cause, baru dapat menjatuhkan dugaan terhadap seseorang. Artinya cukup fakta dan keadaan berdasarkan informasi yang sangat dipercaya bahwa tersangka sebagai pelaku tindak pidana berdasar bukti dan tidak boleh semata-mata berdasar konklusi.

¹<http://repository.usu.ac.id/bitstream/handle/123456789/36008/10E00138.pdf?sequence=1>. Diakses Pada Hari Senin, 13 Maret 2017. Pukul 11:27 WIB

Alat bukti yang sah menurut Pasal 184 KUHAP adalah :

1. Keterangan saksi;
2. Keterangan ahli;
3. Surat;
4. Petunjuk;
5. Keterangan terdakwa.

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai suatu norma hukum khusus terdapat suatu prinsip-prinsip hukum yang juga baru, yang menyimpang dari sistem hukum yang ada sebagaimana diatur dalam KUHP maupun KUHAP. Salah satunya adalah mengenai alat bukti elektronik yang baru diakui sebagai suatu alat bukti yang sah dalam hukum pembuktian di Indonesia. Di mana sebelum Undang-undang tentang Informasi dan Transaksi Elektronik disahkan, dalam hal pembuktian tindak pidana dunia maya ini selalu terbentur pada keterbatasan cakupan alat bukti sementara tindak pidana dunia maya ini semakin hari semakin sering terjadi dan memerlukan pembuktian yang sebenar-benarnya.

Hal lain yang perlu diperhatikan adalah upaya untuk memenuhi persyaratan hukum guna menentukan apakah seseorang yang telah menjadi tersangka itu pantas disangka telah melakukan tindak pidana *cyber crime* berdasarkan alat bukti yang sah dan cukup menurut ketentuan Perundang-undangan.

Aparat penegak hukum dihadapkan pada kesulitan untuk menentukan kualifikasi kejahatan apakah yang dapat dituduhkan pada pelaku *cybercrime* atau tindak pidana informasi dan transaksi elektronik, mengingat sukarnya menemukan serta menerapkan alat bukti. Sementara itu, pesatnya teknologi informasi melalui internet telah mengubah aktivitas-aktivitas kehidupan yang semula perlu

dilakukan dengan kontak fisik, kini dengan menggunakan media informasi dan teknologi, aktivitas keseharian dapat dilakukan secara virtual atau maya. Masalah sulit yang dihadapi penegak hukum saat ini adalah bagaimana menjaring pelaku *cybercrime* yang mengusik rasa keadilan tersebut dikaitkan dengan sistem hukum acara pidana yang berlaku.

Berhadapan dengan kasus *cybercrime*, pembuktian menjadi masalah yang sulit. Seringkali penegak hukum di Indonesia mengalami kesulitan dalam menjerat pelaku *cybercrime* karena masalah pembuktian (*documentary evidence*) yang tidak memenuhi ketentuan hukum acara pidana Indonesia. Sementara upaya penjeratan terhadap pelaku-pelaku *cybercrime* harus tetap dilakukan, upaya perluasan alat bukti serta penerapannya menjadi solusi untuk menegakkan hukum.²

Berdasarkan uraian di atas, maka disusun skripsi ini dengan judul **“Penerapan Alat Bukti Dalam Tindak Pidana Informasi Dan Transaksi Elektronik Di Kepolisian Daerah Sumatra Utara”**.

1. Rumusan Masalah

Berdasarkan uraian di atas dapat ditarik beberapa permasalahan yang akan menjadi batasan pembahasan dari penelitian ini nantinya, antara lain :

- a. Bagaimana proses penerapan alat bukti dalam tindak pidana informasi dan transaksi elektronik di kepolisian daerah sumatera utara ?
- b. Bagaimana kendala yang dihadapi oleh kepolisian dalam menerapkan alat bukti tindak pidana informasi dan transaksi elektronik?

² Dikdik M. Aries Mansur Dan Elisatris. 2005. *Cyber Law. Aspek Hukum Teknologi Informasi*. Bandung:Refika Aditama., halaman 100.

- c. Bagaimana upaya yang dilakukan oleh kepolisian untuk mengatasi kendala yang dihadapi dalam menerapkan alat bukti tindak pidana informasi dan transaksi elektronik?

2. Faedah Penelitian

Faedah penelitian ini diharapkan berguna baik secara teoritis maupun secara praktis, dengan kata lain yang dimaksud dengan faedah teoritis yaitu adalah sebagai sumbangan baik kepada ilmu pengetahuan pada umumnya maupun kepada ilmu hukum khususnya, dari segi praktis penelitian berfaedah bagi kepentingan Negara, Bangsa, masyarakat dan pembangunan.³

a. Faedah Teoritis

Secara teoritis sebagai suatu bentuk penambahan literatur dan sebagai bahan kajian lebih lanjut di bidang hukum acara pidana khususnya dalam hal penerapan alat bukti dalam tindak pidana informasi dan transaksi elektronik.

b. Faedah Praktis

Secara praktis sebagai suatu bentuk sumbangan pemikiran dan masukan serta dapat dijadikan pedoman bagi pihak yang berkepentingan sehingga penerapan alat bukti dalam tindak pidana informasi dan transaksi elektronik dapat berjalan sesuai dengan ketentuan yang berlaku dalam peraturan perundang-undangan di Indonesia.

B. Tujuan Penelitian

Tujuan yang ingin diperoleh dalam penelitian ini adalah sebagai berikut:

³ Fakultas Hukum UMSU. 2014. *Pedoman Penulisan Skripsi*. Medan: Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, Halaman 5

1. Untuk mengetahui proses penerapan alat bukti dalam tindak pidana informasi dan transaksi elektronik di kepolisian daerah Sumatera Utara.
2. Untuk mengetahui kendala yang dihadapi oleh kepolisian dalam menerapkan alat bukti tindak pidana informasi dan transaksi elektronik.
3. Untuk mengetahui upaya yang dilakukan oleh kepolisian untuk mengatasi kendala yang dihadapi dalam menerapkan alat bukti tindak pidana informasi dan transaksi elektronik.

C. Metode Penelitian

Metode yang dipergunakan dalam penelitian ini adalah terdiri dari:

1. Sifat/Materi Penelitian

Penelitian Skripsi ini merupakan penelitian yang menggunakan penelitian deskriptif. Dengan demikian, sifat penelitian dikategorikan penelitian deskriptif dengan analisis yang bersifat kualitatif. Penelitian bersifat deskriptif adalah untuk menggambarkan, menelaah dan menjelaskan serta menganalisa Perundang-undangan yang berlaku.

Jenis penelitian yang diterapkan adalah memakai penelitian dengan pendekatan yuridis empiris, yaitu penelitian yang mengacu kepada norma-norma hukum, yang terdapat dalam peraturan perundang-undangan yang berlaku sebagai pijakan normatif, dipadukan dengan hasil wawancara yang diperoleh langsung dari narasumber. Dimana, setiap data yang diperoleh baik primer maupun sekunder langsung diolah dan dianalisa dengan tujuan untuk memperjelas maksud dari penelitian ini.

2. Sumber Data

Sumber data yang digunakan dalam penelitian dengan metode pendekatan yuridis empiris adalah data primer, dimana data yang diperoleh melalui studi lapangan, wawancara dengan pihak-pihak terkait dan menggunakan data sekunder sebagai rujukan, adapun data sekunder terdiri dari:

- a. Bahan hukum primer, yang terdiri dari Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- b. Bahan hukum sekunder, berupa buku bacaan yang relevan terkait dengan materi yang diteliti.
- c. Bahan hukum tersier, berupa bahan-bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder, berupa kamus hukum dan website di internet.

3. Alat Pengumpul Data

Alat pengumpul data yang dipergunakan dalam penelitian ini adalah :

- a. Wawancara, yaitu suatu alat pengumpulan data penelitian dengan melakukan wawancara langsung dengan narasumber dalam hal ini adalah Ditreskrimsus Polda Sumatera Utara
- b. Studi dokumen, yaitu suatu alat pengumpulan data penelitian dengan melakukan analisa terhadap bahan kepustakaan.

4. Analisis Data

Data yang dikumpulkan dalam penelitian ini dikelompokkan sesuai dengan penelitian dan diteliti serta dievaluasi keabsahannya. Setelah itu diseleksi dan

diolah lalu dianalisa sesuai dengan perundang-undangan yang berlaku untuk melihat kecenderungan yang ada. Analisa data termasuk penarikan kesimpulan dilakukan secara kualitatif, sehingga diharapkan akan memberikan solusi dan jawaban atas permasalahan dalam penelitian ini.

D. Definisi Operasional

Definisi operasional adalah kerangka yang menggambarkan hubungan antara definisi-definisi/konsep-konsep khusus yang akan diteliti.⁴ Sesuai dengan judul penelitian yang diajukan yaitu: “Penerapan Alat Bukti Dalam Tindak Pidana Informasi dan Transaksi Elektronik Di Kepolisian Daerah Sumatera Utara”, maka dapat diterangkan definisi operasional penelitian, yaitu:

1. Penerapan adalah suatu perbuatan mempraktekan suatu teori, metode, dan hal lain untuk mencapai tujuan tertentu dan untuk suatu kepentingan yang diinginkan oleh suatu kelompok atau golongan yang telah terencana dan tersusun sebelumnya.⁵
2. Alat bukti adalah segala sesuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat-alat bukti tersebut, dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan terdakwa.
3. Tindak pidana adalah suatu perbuatan yang dilakukan manusia yang dapat bertanggung jawab yang mana perbuatan tersebut dilarang atau diperintahkan

⁴*Ibid.*,

⁵<http://internetsebagaisumberbelajar.blogspot.co.id/2010/07/pengertian-penerapan.html>,
Diakses Pada Hari Senin, 13 Maret 2017. Pukul 10:47 WIB

atau dibolehkan undang-undang hukum pidana yang yang diberi sanksi berupa sanksi pidana.⁶

4. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *elctronic data interchange (EDI)*, surat elektronik (*elektronik mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode, akses, simbol, atau perpforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahami.⁷
5. Transaksi eletronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan komputer, dan/atau media elektronik lainnya.⁸

⁶ <http://artonang.blogspot.co.id/2014/12/pengertian-tindak-pidana-unsur-unsur.html>.
Diakses Pada Hari Selasa, 03 Oktober 2017. Pukul 23:27 WIB

⁷ <http://repository.usu.ac.id/bitstream/handle/123456789/36008/10E00138.pdf?sequence=1>. ,Diakses Pada Hari Selasa, 03 Oktober 2017. Pukul 23:27 WIB

⁸ *Ibid.*,

BAB II

TINJAUAN PUSTAKA

A. Alat Bukti

Arti dan tujuan kehidupan masyarakat ialah mencari dan mewujudkan ketenteraman atau ketertiban yaitu kehidupan bersama antara sesama anggota masyarakat yang dituntun dan dibina dalam ikatan yang teratur dan layak, sehingga lalu lintas pergaulan masyarakat yang bersangkutan berjalan dengan tertib dan lancar. Agar dapat terwujud tata pergaulan yang tertib dan lancar, satu-satunya cara yang harus ditempuh oleh masyarakat ialah jalan menegakkan ketertiban dan kepastian hukum dalam setiap aspek kehidupan, dengan kaidah-kaidah dan nilai hukum yang telah disepakati.

Secara garis besar fungsi hukum dan aparat penegak hukum, pada umumnya bertujuan :

1. Agar terbina hubungan yang serasi antara negara atau masyarakat dengan warga negara dan warga masyarakat.
2. Hukum yang ditegakkan oleh instansi penegak hukum yang disertai tugas untuk itu, harus menjamin “kepastian hukum” demi tegaknya ketertiban dan keadilan dalam kehidupan masyarakat. Ketidakpastian hukum, akan menimbulkan kekacauan dalam kehidupan masyarakat, dan akan saling berbuat sesuka hati serta bertindak main hakim sendiri. Keadaan seperti ini menjadikan kehidupan berada dalam suatu *social disorganization* atau kekacauan sosial.

3. Untuk membina peningkatan suasana kehidupan masyarakat yang aman dan tertib atau untuk tercipta stabilitas keamanan dan ketertiban kehidupan masyarakat, hukum dan undang-undang harus ditegakkan dengan “tepat”, dan “tegas”

KUHAP sebagai hukum positif akan memberi peluang yang lebih baik dibanding dengan masa sebelumnya. Hal ini didasarkan pada pengamatan, pembuat undang-undang merumuskan ketentuan KUHAP sedemikian rupa sehingga aturan-aturan pada garis besarnya memberi pengertian yang jelas serta memberi pembatasan yang terinci (seperti batas penahanan yang tegas, penjernihan fungsi, diferensiasi fungsi penyidikan dan penuntutan) penjabaran yang lebih jelas hak-hak asasi manusia dan lain sebagainya.

Istilah *criminal justice system* atau sistem peradilan pidana (SPP) menunjukkan mekanisme kerja dalam penanggulangan kejahatan dengan mempergunakan dasar pendekatan sistem. *Criminal justice process* adalah setiap tahap dari suatu putusan yang menghadapkan seorang tersangka ke dalam proses yang membawanya pada penentuan pidana. Sedangkan *Criminal justice system* adalah interkoneksi antar keputusan dari setiap instansi yang terlibat dalam proses peradilan pidana.

Berkenaan dengan hal itu, dalam proses peradilan pidana alat bukti merupakan segala sesuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat-alat bukti tersebut, dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran atas suatu tindak pidana yang telah dilakukan oleh terdakwa.

Alat bukti didefinisikan sebagai hal yang dapat digunakan untuk membuktikan perihal kebenaran suatu peristiwa di pengadilan. Mengenai apa saja yang termasuk alat bukti, masing-masing hukum acara suatu peradilan akan mengaturnya secara rinci. Alat bukti dalam hukum acara pidana berbeda dengan alat bukti dalam hukum acara perdata. Demikian pula alat bukti yang berlaku bagi acara persidangan dalam perkara-perkara tertentu seperti hukum acara Mahkamah Konstitusi, hukum acara dalam persidangan kasus korupsi, hukum acara dalam persidangan kasus terorisme, dan masih banyak lagi.⁹

Alat bukti adalah segala sesuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat-alat bukti tersebut, dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan terdakwa.

1. Alat Bukti Dalam Pemeriksaan Perkara Pidana

Alat bukti yang dapat digunakan dalam pemeriksaan perkara pidana adalah sesuai dengan ketentuan Pasal 184 ayat (1) KUHAP dan secara sah diakui dalam peraturan perundang-undangan.

Berdasarkan Pasal 184 ayat (1) Kitab Undang-Undang Hukum Acara Pidana (KUHAP), bahwa yang termasuk alat bukti yang sah adalah:

a. Keterangan Saksi

Berdasarkan Pasal 1 angka 26 KUHAP dinyatakan, Saksi adalah orang yang dapat memberikan keterangan guna kepentingan penyidikan, penuntutan, dan peradilan tentang perkara pidana yang ia dengar sendiri, ia lihat sendiri, dan ia alami sendiri. Sementara itu, Pasal 1 angka 27 KUHAP menyatakan bahwa keterangan saksi adalah salah satu alat bukti dalam perkara pidana yang berupa keterangan dari saksi mengenai suatu peristiwa pidana yang ia dengar

⁹ Eddy O.S Hiariej. 2012. *Teori dan Hukum Pembuktian*. Jakarta: Penerbit Erlangga, halaman 52.

sendiri, lihat sendiri dan ia alami sendiri dengan menyebut alasan dari pengetahuannya itu.

Konstruksi Pasal 1 angka 26 *juncto* Pasal 1 angka 27 *juncto* Pasal 184 ayat (1) huruf a KUHAP pada intinya mendefinisikan saksi sebagai orang yang dapat memberikan keterangan guna penyidikan, penuntutan, dan peradilan tentang suatu perkara pidana yang ia dengar sendiri, lihat sendiri, dan alami sendiri.

Dalam perkembangannya, definisi saksi sebagaimana dimaksud dalam Pasal 1 angka 26 *juncto* Pasal 1 angka 27 *juncto* Pasal 184 ayat (1) huruf a KUHAP diperluas berdasarkan Putusan Mahkamah Konstitusi Nomor 65/PUU-VIII/2010 tertanggal 8 agustus 2011. Secara eksplisit putusan Mahkamah Konstitusi dalam amarnya menyatakan sebagai berikut :

Pasal 1 angka 26 dan angka 27; Pasal 65; Pasal 116 ayat (3) dan ayat (4); serta Pasal 184 ayat (1) huruf a Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Lembaran Negara Republik Indonesia Tahun 1981 Nomor 76 dan Tambahan Lembaran Negara Republik Indonesia Nomor 3209) adalah bertentangan dengan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 sepanjang pengertian saksi dalam Pasal 1 angka 26 dan angka 27; Pasal 65; Pasal 116 ayat (3) dan ayat (4); serta Pasal 184 ayat (1) huruf a Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Lembaran Negara Republik Indonesia Tahun 1981 Nomor 76 dan Tambahan Lembaran Negara Republik Indonesia Nomor 3209), tidak dimaknai termasuk pula “orang yang dapat memberikan keterangan dalam rangka penyidikan, penuntutan, dan peradilan suatu tindak pidana yang tidak selalu ia dengar sendiri, ia lihat sendiri, dan ia alami sendiri”. Pasal 1 angka 26 dan angka 27; Pasal 65; Pasal 116 ayat (3) dan ayat (4); serta Pasal 184 ayat (1) huruf a Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Lembaran Negara Republik Indonesia Tahun 1981 Nomor 76 dan Tambahan Lembaran Negara Republik Indonesia Nomor 3209) tidak mempunyai kekuatan hukum mengikat sepanjang pengertian saksi dalam Pasal 1 angka 26 dan angka 27; Pasal 65; Pasal 116 ayat (3) dan ayat (4); serta Pasal 184 ayat (1) huruf a Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Lembaran Negara Republik Indonesia Tahun 1981 Nomor 76 dan Tambahan Lembaran Negara Republik Indonesia Nomor 3209), tidak dimaknai termasuk pula “orang yang dapat memberikan keterangan

dalam rangka penyidikan, penuntutan, dan peradilan suatu tindak pidana yang tidak selalu ia dengar sendiri, ia lihat sendiri, dan ia alami sendiri”.¹⁰

Dengan demikian, berdasarkan putusan Mahkamah Konstitusi, definisi keterangan saksi sebagai alat bukti adalah keterangan dari saksi mengenai suatu peristiwa pidana yang ia dengar sendiri, ia lihat sendiri, dan ia alami sendiri dengan menyebut alasan pengetahuannya itu, termasuk pula keterangan dalam rangka penyidikan, penuntutan, dan peradilan suatu tindak pidana yang tidak selalu ia dengar sendiri, ia lihat sendiri, dan ia alami sendiri.

Berdasarkan KUHAP, keterangan saksi sebagai bukti yang sah, selain keterangan tersebut mengenai apa yang ia lihat sendiri, ia dengar atau ia alami sendiri, termasuk pula perluasan sebagaimana yang diputuskan Mahkamah Konstitusi, juga harus disampaikan di depan sidang pengadilan dan di bawah sumpah. Pada hakikatnya, keterangan saksi sebagai alat bukti yang sah, yaitu keterangan yang diberikan di depan sidang pengadilan ditujukan dengan maksud keterangan tersebut dapat dikonfirmasi oleh hakim, jaksa penuntut umum, dan advokat.

Pada umumnya semua orang atau siapa saja dapat didengar keterangan atau menajadi saksi, kecuali sebagaimana dimaksud menurut Pasal 168 KUHAP, bahwa yang tidak dapat didengar keterangannya dan dapat mengundurkan diri sebagai saksi, adalah:

- 1) Keluarga sedarah atau semenda dalam garis lurus ke atas atau ke bawah sampai derajat ketiga dari terdakwa atau yang bersama-sama sebagai terdakwa;

¹⁰ Eddy O.S Hiariej. Op. Cit., halaman 102.

- 2) Saudara dari terdakwa atau yang bersama-sama sebagai terdakwa, saudara ibu atau saudara bapak, juga mereka yang mempunyai hubungan karena perkawinan dan anak-anak saudara terdakwa sampai derajat ketiga;
- 3) Suami atau istri terdakwa maupun sudah bercerai atau yang bersama-sama sebagai terdakwa.¹¹

Orang-orang tersebut berdasarkan Pasal 168 KUHAP, ialah mempunyai hak untuk mengundurkan diri dari kesaksian, namun dapat memberikan kesaksian apabila menurut Pasal 169 ayat (1) KUHAP, apabila saksi itu menghendaknya sendiri dan penuntut umum dan terdakwa secara tegas menyetujuinya, maka dapat memberikan keterangan dengan sumpah, tetapi sebaliknya apabila penuntut umum dan terdakwa tidak menyetujuinya, maka menurut Pasal 169 ayat (2) KUHAP tetap diperbolehkan memberikan keterangan tanpa sumpah.

Selain itu, orang yang sama sekali tidak dapat didengar atau memberikan keterangannya atau sebagai saksi atau dapat mengundurkan diri dalam suatu perkara pidana menurut Pasal 170 ayat (1) KUHAP, yaitu Mereka yang karena pekerjaan, harkat martabat atau jabatannya diwajibkan menyimpan rahasia, dapat minta dibebaskan dari kewajiban menyimpan rahasia, dapat minta dibebaskan dari kewajiban untuk memberi keterangan sebagai saksi, yaitu tentang hal yang dipercayakan kepada mereka. Demikian pula terdapat saksi-saksi yang dapat

¹¹ <http://digilib.unila.ac.id/8153/6/5.%20Bab%20II%20ok.pdf>. Diakses Pada Hari Selasa, 03 Oktober 2017. Pukul 23:27 WIB

memberikan keterangan tapi tidak disumpah sebagaimana menurut Pasal 171 huruf a dan b KUHAP, yaitu:

- a) Anak yang umurnya belum cukup lima belas tahun dan belum pernah kawin;
- b) Orang sakit ingatan atau sakit jiwa meskipun kadang-kadang ingatannya baik kembali.

Saksi menurut sifatnya dapat dibagi atas dua bagian, yaitu:

1. *Saksi A Charge* (saksi yang memberatkan terdakwa)

Saksi ini adalah saksi yang telah dipilih dan diajukan oleh penuntut umum, dengan keterangan atau kesaksian akan memberatkan terdakwa.

2. *Saksi A De Charge* (saksi yang meringankan/menguntungkan terdakwa)

Saksi ini dipilih atau diajukan oleh penuntut umum atau terdakwa atau penasihat hukum, yang mana keterangan atau kesaksian yang diberikan akan meringankan atau menguntungkan terdakwa

Alat bukti keterangan saksi merupakan alat bukti yang paling utama dalam perkara pidana. Boleh dikatakan, tidak ada perkara pidana yang luput dari pembuktian alat bukti keterangan saksi. Hampir semua pembuktian perkara pidana, selalu bersandar kepada pemeriksaan keterangan saksi. Sekurang-kurangnya di samping pembuktian dengan alat bukti lain, masih diperlukan pembuktian dengan alat bukti saksi.

b. Keterangan Ahli

Penyebutan alat bukti “keterangan ahli” sering disebut “saksi ahli”. Penyebutan demikian tidak dapat dibenarkan merujuk kepada ketentuan hukum

KUHAP yang dalam pasal-pasal nya menggunakan kata keterangan ahli. Disamping tidak dibenarkan secara yuridis, dalam pengertian saksi tidak ada didalamnya kategori saksi ahli dan lebih jelas lagi apabila didasarkan kepada perbedaan makna antara keterangan saksi dengan makna keterangan ahli.

Pasal 1 angka 28 KUHAP menyebutkan bahwa “keterangan ahli adalah keterangan yang diberikan oleh seorang yang memiliki keahlian khusus tentang hal yang diperlukan untuk membuat terang suatu perkara pidana guna kepentingan pemeriksaan”.

Ketentuan tentang keterangan ahli adalah keterangan yang dinyatakan di sidang pengadilan. Perlu diperhatikan, karena keterangan ahli dapat juga didapat diluar sidang pengadilan, pada tahap penyidikan demikian pula hendaknya dibedakan keterangan ahli yang dilakukan dengan sumpah atau janji dan keterangan ahli tanpa sumpah atau janji.

Perbedaan-perbedaan tersebut berpengaruh terhadap klasifikasi alat bukti. Keterangan ahli yang dinyatakan dalam sidang pengadilan merupakan alat bukti sebagaimana dimaksud dalam Pasal 184 KUHAP. Sedangkan keterangan ahli yang diberikan diluar sidang pengadilan, yang berbentuk tulisan atau yang dikenal “*Visum Et Repertum (VER)*” berkualifikasi sebagai alat bukti surat. Keterangan ahli yang diberikan tanpas sumpah atau janji, keterangannya hanya merupakan keterangan yang dapat menguatkan keyakinan hakim.¹²

¹² Hendar Soetarna. 2011. *Hukum Pembuktian dalam Acara Pidana*. Bandung: Alumni., halaman 69.

Timbul kemungkinan terjadinya perbedaan pengertian, antara pengertian keterangan ahli, dengan keterangan saksi. Sepintas pengertiannya seperti sama, sedangkan antara keduanya memiliki perbedaan yang nyata.

Keterangan seorang ahli adalah penilaian sesuatu yang sudah nyata ada, serta pengambilan kesimpulan mengenai sesuatu yang nyata itu. Keterangan saksi mengemukakan “peristiwa”nya, sedangkan keterangan ahli, menilai peristiwa itu dan mengambil keputusan atas peristiwa itu.¹³

Keterangan ahli terutama dibutuhkan untuk memberi penjelasan terkait *physical evidence* (bukti fisik) atau *real evidence* (bukti nyata) yang telah dihadirkan di depan sidang pengadilan. Demikian pula keterangan ahli dibutuhkan untuk menerangkan hal-hal diluar pengetahuan h hukum. Akan tetapi, dapat saja keterangan ahli juga menyangkut masalah hukum terkait dengan dasar hukum atau alasan yang menjadi pokok perkara termasuk pula didalamnya adalah analisis atau pengertian elemen-elemen suatu tindak pidana yang didakwakan.¹⁴

Keterangan ahli biasanya bersifat umum berupa pendapat atas pokok perkara pidana yang sedang disidangkan atau yang berkaitan dengan pokok perkara tersebut. Ahli tidak diperkenankan memberikan penilaian terhadap kasus konkret yang sedang disidangkan. Oleh karena itu, pertanyaan terhadap ahli biasanya bersifat hipotesis atau pertanyaan yang bersifat umum. Ahli pun tidak dibolehkan memberikan penilaian terhadap salah atau tidaknya terdakwa berdasarkan fakta persidangan yang dinyatakan kepadanya.¹⁵

c. Surat

Alat bukti tertulis atau surat adalah “segala sesuatu yang memuat tanda-tanda bacaan yang dimaksudkan untuk mencurahkan isi hati atau untuk menyampaikan buah pikiran seseorang dan dipergunakan sebagai pembuktian”.¹⁶

¹³ *Ibid.*, halaman 70

¹⁴ Eddy O.S. Hiariej. *Op. Cit.*, halaman 107

¹⁵ *Ibid.*,

¹⁶ Hendar Soetarna. *Op. Cit.*, halaman 73.

Demikian pula menurut Pasal 187 KUHAP, bahwa yang dimaksud dengan Surat sebagaimana tersebut pada Pasal 184 ayat (1) huruf c, di buat atas sumpah jabatan atau dikuatkan dengan sumpah, adalah:

1. Berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat di hadapannya, yang memuat keterangan tentang kejadian atau keadaan yang didengar, dilihat atau yang dialaminya sendiri, disertai dengan alasan yang jelas dan tegas tentang keterangannya itu;
2. Surat yang dibuat menurut ketentuan peraturan perundang-undangan atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukkan bagi pembuktian sesuatu hal atau sesuatu keadaan;
3. Surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai suatu hal atau sesuatu keadaan yang diminta secara resmi kepadanya;
4. Surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.

Contoh-contoh dari alat bukti surat itu adalah berita acara pemeriksaan (BAP) yang dibuat oleh polisi (penyelidik/penyidik), BAP pengadilan, berita acara penyitaan (BAP), surat perintah penangkapan (SPP), surat izin penggeledahan (SIP), surat izin penyitaan (SIP), dan lain sebagainya.¹⁷

¹⁷ Andi Sofyan dan Abdul asis, 2014. *Hukum Acara Pidana*. Jakarta: Prenadamedia Group, halaman 264.

d. Petunjuk

Menurut Pasal 188 KUHP, bahwa yang dimaksud dengan alat bukti petunjuk adalah:

1. Petunjuk adalah perbuatan, kejadian atau keadaan, yang karena persesuaiannya, baik antara yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya.
2. Petunjuk sebagaimana dimaksud dalam ayat (1) hanya dapat diperoleh dari:
 - a) Keterangan saksi
 - b) Surat
 - c) Keterangan terdakwa.
3. Penilaian atas kekuatan pembuktian dari suatu petunjuk dalam setiap keadaan tertentu dilakukan oleh hakim dengan arif lagi bijaksana setelah ia mengadakan pemeriksaan dengan penuh kecermatan berdasarkan hati nuraninya.¹⁸

e. Keterangan Terdakwa

Dalam Pasal 184 ayat (1) KUHP tentang alat-alat bukti, Keterangan terdakwa ditempatkan di urutan terakhir. Penempatan tersebut dimaksudkan agar terdakwa terlebih dahulu mendengar, melihat alat bukti yang lain. Melalui sistem yang demikian, diharapkan terdakwa benar-benar dapat merenungi, menyadari apa yang didakwakan, meskipun bukan berarti terdakwa harus membenarkan atau mengiyakan setiap alat bukti yang dikemukakan dalam sidang.

Pasal 189 ayat (4) KUHP menyatakan bahwa keterangan terdakwa saja tidak cukup untuk membuktikan bahwa ia bersalah melakukan perbuatan yang didakwakan kepadanya, melainkan harus disertai dengan alat bukti yang lain.

Pasal tersebut disamping merujuk ke pasal lain, pasal 183 KUHP juga merupakan upaya jangan sampai ada keterangan terdakwa yang direayasa. Terdakwa bukanlah pelaku tindak pidana, tetapi demi keuntungan finansial

¹⁸*Ibid.*, halaman 264.

ataupun pertimbangan kelayakan untuk menjalani pidana penjara, terdakwa mengakui dan tidak mengingkari apa yang didakwakan, sedangkan pelaku sebenarnya adalah orang lain.

Ketentuan lainnya sehubungan alat bukti keterangan terdakwa bahwa keterangan terdakwa ialah apa yang terdakwa nyatakan disidang tentang perbuatan yang ia lakukan atau yang ia ketahui sendiri atau alami sendiri. Sedangkan keterangan terdakwa yang diberikan di luar sidang dapat digunakan untuk membantu menemukan bukti di sidang, asalkan keterangan itu didukung oleh suatu alat bukti yang sah sepanjang mengenai hal yang didakwakan kepadanya sebagaimana diatur dalam Pasal 189 ayat (1) dan ayat (2) KUHAP.¹⁹

2. Alat Bukti Dalam Pemeriksaan Tindak Pidana Informasi dan Transaksi Elektronik

Perkembangan teknologi tidak mengurangi perkembangan tindak pidana. Justru dengan adanya teknologi setiap tindak pidana dapat dilakukan hampir disetiap kesempatan. Pengaturan regulasi hukum terkait tindak pidana bidang elektronik atau yang disebut dengan *cyber crime*, masih dirasa sangat minim. Bahkan interpretasi dilakukan dengan mengaitkan beberapa aturan hukum yang lama.

Alat bukti dalam Undang Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terdapat dalam Pasal 5 yang berbunyi sebagai berikut:

- 1) Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
- 2) Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat 1 merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.²⁰

¹⁹*Ibid.*, halaman 80.

²⁰ Josua Sitompul. 2012. *CyberSpace, CyberCrimes, CyberLaws*. Jakarta:Tatanusa., halaman 279.

Ketentuan ini menegaskan bahwa alat bukti elektronik telah diterima dalam sistem hukum pembuktian di Indonesia di berbagai peradilan, pidana, perdata, agama, militer, tata usaha negara, mahkamah konstitusi, termasuk arbitrase. Akan tetapi, penekanan dari bagian ini adalah pengaturan alat bukti elektronik dalam hukum acara pidana di indonesia, dan tidak membahas topik ini terkait hukum acara lainnya.

UU ITE tidak menjelaskan apa yang dimaksud dengan perluasan dari alat bukti yang sah. Akan tetapi, Pasal 5 ayat (2) UU ITE memberikan petunjuk penting mengenai perluasan ini, yaitu bahwa perluasan tersebut harus sesuai dengan Hukum Acara yang berlaku di Indonesia. Mengacu kepada pembahasan sebelumnya, perluasan tersebut mengandung makna:

- a. Memperluas cakupan atau ruang lingkup alat bukti yang diatur dalam Pasal 184 KUHAP; dan
- b. Mengatur sebagai alat bukti lain, yaitu menambah jumlah alat bukti yang diatur dalam Pasal 184 KUHAP.²¹

Mengacu kepada ketentuan-ketentuan mengenai pembuktian yang diatur dalam KUHAP maka sesuai dengan Hukum Acara yang berlaku di Indonesia. maksudnya ialah bahwa harus ada alat penguji terhadap alat bukti elektronik agar alat bukti tersebut dapat dinyatakan sah di persidangan sama seperti terhadap alat bukti lainnya, yaitu persyaratan formil dan persyaratan materiel. Persyaratan tersebut ditentukan berdasarkan jenis alat bukti elektronik yang dimaksud (dalam bentuk original atau hasil cetaknya).

²¹*Ibid.*, halaman 279.

1) Alat bukti elektronik memperluas cakupan atau ruang lingkup alat bukti

Alat bukti dalam KUHAP yang diperluas ialah alat bukti surat. Esensi dari surat ialah kumpulan dari tanda baca dalam bahasa tertentu yang memiliki makna. Esensi ini sama dengan hasil cetak dari Informasi atau Dokumen elektronik. Hasil cetak dari Informasi atau Dokumen Elektronik dikategorikan sebagai surat lain sebagaimana dimaksud dalam Pasal 187 huruf d KUHAP dan hanya dapat dijadikan alat bukti apabila hasil cetak tersebut memiliki hubungan dengan isi dari alat pembuktian yang lain. Hasil cetak Informasi atau Dokumen Elektronik belum dapat dikategorikan sebagai akta otentik mengingat pembatasan yang diberikan oleh Pasal 5 ayat (4) UU ITE.

2) Alat bukti elektronik sebagai alat bukti lain

Hal alat bukti elektronik sebagai alat bukti lain dipertegas dalam Pasal 44 UU ITE yang mengatur bahwa Informasi atau Dokumen Elektronik adalah alat bukti lain. Penegasan bahwa informasi atau dokumen elektronik dalam bentuk originalnya merupakan alat bukti selain yang telah diatur dalam KUHAP ialah pengaturan yang sangat penting mengingat informasi atau dokumen elektronik dalam bentuk originalnya dapat mengandung informasi yang tidak dapat diperoleh apabila Informasi atau Dokumen Elektronik tersebut dicetak.

3) Alat bukti elektronik sebagai sumber petunjuk

Pasal 188 ayat (2) KUHAP menentukan secara limitatif sumber petunjuk, yaitu: keterangan saksi, surat, dan keterangan terdakwa. Akan tetapi, berdasarkan uraian diatas, alat bukti elektronik juga dapat dijadikan sumber petunjuk, yaitu hasil cetak Informasi atau Dokumen Elektronik

dapat dikategorikan sebagai surat. Surat yang dimaksud ialah “surat lain” sepanjang surat itu memiliki hubungan dengan isi dari alat pembuktian yang lain sebagaimana dimaksud dalam Pasal 187 huruf d.²²

B. Tindak Pidana Informasi dan Transaksi Elektronik

Berbicara masalah *cyber crime* tidak lepas dari permasalahan keamanan jaringan komputer atau keamanan informasi berbasis internet dalam era global ini, apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggannya. Untuk mencapai tingkat kehandalan tentunya informasi itu sendiri harus selalau dimutakhirkan sehingga informasi yang disajikan tidak ketinggalan zaman. Kejahatan dunia maya (*cybercrime*) ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat.

Berdasarkan beberapa literatur serta praktiknya, *cybercrime* memiliki beberapa karakteristik, yaitu :

1. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber/*cyber (cyberspace)*, sehingga tidak dapat dipastikan yurisdiksi Negara mana yang berlaku terhadapnya.
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian materiil maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya
5. Perbuatan tersebut sering dilakukan secara transnasional/melintasi batas negara.²³

²²*Ibid.*, halaman 280.

²³ Budi Suhariyanto. 2013. *Tindak Pidana Teknologi Informasi (cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: Rajawali Pers., halaman 13.

Perbuatan melawan hukum dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, kejahatan dalam teknologi informasi disebut dengan *Cyber Crime*. *Cyber Crime* adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi dan komunikasi tanpa batas, serta memiliki sebuah karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan tingkat keamanan yang tinggi, dari sebuah informasi yang disampaikan dan diakses oleh pengguna internet.

1. Jenis Tindak Pidana Informasi dan Transaksi Elektronik

Jenis Tindak Pidana Informasi dan Transaksi Elektronik tidak dijelaskan secara rinci didalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Tindak-tindak pidana yang diatur dalam UU ITE diatur dalam BAB VII tentang perbuatan yang dilarang; perbuatan-perbuatan tersebut dapat dikategorikan menjadi beberapa kelompok sebagai berikut.

a. Tindak Pidana yang berhubungan dengan aktivitas illegal, yaitu:

- 1) Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal, yang terdiri dari:
 - a) Kesusilaan
 - b) Perjudian
 - c) Pennghinaan atau pencemaran nama baik;
 - d) Pemerasan atau pengancaman;
 - e) Berita bohong yang menyesatkan dan merugikan konsumen;
 - f) Menimbulkan rasa kebencian berdasarkan SARA;

- g) Mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi;
- 2) Dengan cara apapun melakukan akses ilegal;
- 3) Intersepsi ilegal terhadap informasi atau dokumen elektronik dan sistem Elektronik;
- b. Tindak pidana yang berhubungan dengan gangguan (*Interferensi*), yaitu:
 - 1) Gangguan terhadap Informasi atau Dokumen Elektronik (*data interference*);
 - 2) Gangguan terhadap Sistem Elektronik (*system interference*);
- c. Tindak pidana memfasilitasi perbuatan yang dilarang
- d. Tindak pidana pemalsuan informasi atau dokumen elektronik
- e. Tindak pidana tambahan (*accessoir*); dan
- f. Perberatan-perberatan terhadap ancaman pidana.²⁴

2. Bentuk Tindak Pidana Informasi dan Transaksi Elektronik

Bentuk tindak pidana Informasi dan Transaksi Elektronik ini biasanya dikenal dengan istilah *Cyber Crime* (Kejahatan Mayantara) istilah tersebut kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/carding, *confidence fraud*, penipuan identitas, dan pornografi anak.

Walaupun kejahatan dunia maya atau *cybercrime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional di mana

²⁴ Josua Sitompul. *Op. Cit.*, halaman 147.

komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.²⁵

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi dalam beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk, antara lain:

- a. *Unauthorized access to computer system and service*, yaitu kejahatan yang dilakukan ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.
- b. *Illegal contents*, yaitu kejahatan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah:
 - 1) Pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain.
 - 2) Pemuatan hal-hal yang berhubungan dengan pornografi.
 - 3) Pemuatan suatu informasi yang merupakan rahasia negara, agitasi, dan propaganda untuk melawan pemerintah yang sah, dan sebagainya.
- c. *Data forgery*, yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen

²⁵<http://mkhiabanifakhri.ilearning.me/2013/12/16/definisi-dan-jenis-jenis-kejahatan-internet>. Diakses Pada Hari Sabtu, 25 Maret 2017. Pukul 14:51 WIB.

ecommerce dengan membuat seolah-olah terjadi “salah ketik” yang pada akhirnya akan menguntungkan pelaku.

- d. *Cyber espionage*, yaitu 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 komputerisasi.
- e. *Cyber sabotage and extortion*, yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet. Biasanya 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 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, tentunya dengan bayaran tertentu.
- f. *Offence against intellectual property*, yaitu kekayaan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang diinternet. Sebagai contoh adalah peniruan tampilan *web page* suatu situs milik

orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

- g. *Infringements of privacy*, yaitu kejahatan yang 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 komputersasi, yang apabila diketahui oleh orang lain, maka dapat merugikan orang secara materiel maupun immateriel, seperti kartu kredit, nomor PIN ATM, keterangan tentang cacat atau penyakit tersembunyi, dan sebagainya.²⁶

Merujuk pada bentuk *cybercrime* sebagaimana dijelaskan diatas, maka penting kiranya untuk melakukan evaluasi tentang kerangka kerja tindak kejahatan *cyber*. Tidak semua kejahatan yang dilakukan dengan komputer merupakan kejahatan komputer (*cybercrimes*). Misalnya, apabila seseorang mencuri suatu kode akses tertentu seperti nomor kartu untuk sambungan telepon jarak jauh dan menggunakannya untuk melakukan telepon jarak jauh, nomor tersebut diperiksa oleh komputer sebelum sambungan telepon itu diproses. Meskipun dalam hal ini tetap juga menggunakan media komputer, akan tetapi tindak kejahatan seperti ini tidak dikategorikan kejahatan komputer melainkan lebih kepada “penipuan bea”.²⁷

²⁶Maskun. 2013. *Kejahatan Siber , Cyber Crime*. Jakarta: Kencana. halaman 51.

²⁷*Ibid.*, halaman 55.

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Proses Penerapan Alat Bukti Dalam Tindak Pidana Informasi Dan Transaksi Elektronik Di Kepolisian Daerah Sumatera Utara

Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global. Di samping itu, perkembangan teknologi informasi telah menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum. Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai (*user*) atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer.

UU ITE dipersepsikan sebagai *cyberlaw* di Indonesia, yang diharapkan bisa mengatur segala urusan dunia Internet (*siber*), termasuk didalamnya memberi punishment terhadap pelaku *cybercrime*. *Cybercrime* dideteksi dari dua sudut pandang:

1. Kejahatan yang Menggunakan Teknologi Informasi Sebagai Fasilitas:
Pembajakan, Pornografi, Pemalsuan/Pencurian Kartu Kredit, Penipuan Lewat Email (*Fraud*), Email Spam, Perjudian Online, Pencurian Account Internet, Terorisme, Isu Sara, Situs Yang Menyesatkan, dsb.

2. Kejahatan yang Menjadikan Sistem Teknologi Informasi Sebagai Sasaran: Pencurian Data Pribadi, Pembuatan/Penyebaran Virus Komputer, Pembobolan/Pembajakan Situs, *Cyberwar*, *Denial of Service* (DOS), Kejahatan Berhubungan Dengan Nama Domain, dsb.

Cybercrime menjadi isu yang menarik dan kadang menyulitkan karena:

- a. Kegiatan dunia *cyber* tidak dibatasi oleh teritorial negara
- b. Kegiatan dunia *cyber* relatif tidak berwujud
- c. Sulitnya pembuktian karena data elektronik relatif mudah untuk diubah, disadap, dipalsukan dan dikirimkan ke seluruh belahan dunia dalam hitungan detik
- d. Pelanggaran hak cipta dimungkinkan secara teknologi
- e. Sudah tidak memungkinkan lagi menggunakan hukum konvensional.

Analogi masalahnya adalah mirip dengan kekagetan hukum konvensional dan aparat ketika awal mula terjadi pencurian listrik. Barang bukti yang dicuri pun tidak memungkinkan dibawa ke ruang sidang. Secara umum, dapat disimpulkan bahwa UU ITE boleh disebut sebuah *cyberlaw* karena muatan dan cakupannya luas membahas pengaturan di dunia maya, meskipun di beberapa sisi ada yang belum terlalu lugas dan juga ada yang sedikit terlewat. Muatan UU ITE kalau dirangkumkan sebagai berikut:

- 1) Tanda tangan elektronik memiliki kekuatan hukum yang sama dengan tanda tangan konvensional (tinta basah dan bermaterai). Sesuai dengan *e-ASEAN Framework Guidelines* (pengakuan tanda tangan digital lintas batas)
- 2) Alat bukti elektronik diakui seperti alat bukti lainnya yang diatur dalam KUHAP

- 3) UU ITE berlaku untuk setiap orang yang melakukan perbuatan hukum, baik yang berada di wilayah Indonesia maupun di luar Indonesia yang memiliki akibat hukum di Indonesia
- 4) Pengaturan Nama domain dan Hak Kekayaan Intelektual
- 5) Perbuatan yang dilarang (*cybercrime*) dijelaskan pada Bab VII (pasal 27-37), yakni sebagai berikut:
 - a) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
 - b) Setiap Orang dengan sengaja dan tanpajak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
 - c) Setiap Orang dengan sengaja dan tanpajak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
 - d) Setiap Orang dengan sengaja dan tanpajak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.
 - e) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
 - f) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).
 - g) Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi. Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
 - h) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum Mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun engan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
 - i) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.
 - j) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik

- dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
- k) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan. Kecuali intersepsi-intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang. Ketentuan lebih lanjut mengenai tata cara intersepsi diatur dengan Peraturan Pemerintah.
- l) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
- m) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
- n) Terhadap perbuatan yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.
- o) 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.
- p) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
1. Perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
 2. Sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33. Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

- q) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.
- r) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.
- s) Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.²⁸

Penerapan Teknologi Informasi dan Transaksi Elektronik akan menimbulkan berbagai perubahan sosial. Oleh karena itu, perlu untuk diperhatikan bagaimana upaya melakukan transformasi teknologi dan industri dalam mengembangkan struktur sosial yang kondusif. Apabila partisipasi masyarakat dan peranan hukum tidak berjalan dengan maksimal, maka upaya pengembangan teknologi tidak saja kehilangan dimensi kemanusiaan tetapi juga menumpulkan tujuan yang akan dicapai.

Peranan hukum diharapkan dapat menjamin bahwa pelaksanaan perubahan itu akan berjalan dengan cara yang teratur, tertib dan lancar. Perubahan yang tidak direncanakan dengan sebuah kebijakan hukum acap kali akan menimbulkan berbagai persoalan baru dalam masyarakat. Di sinilah hukum akan berfungsi dalam menghadapi perubahan masyarakat. Fungsi hukum dalam masyarakat ada dua, yaitu:

- a. Produk hukum harus mampu mengangkat peristiwa-peristiwa (gejala hukum) dalam masyarakat ke dalam hukum sebagai sarana pengaturan masyarakat di masa akan datang. Fungsi pengaturan diwujudkan dengan dibentuknya norma-norma yang merupakan alat pengawas masyarakat (*social control*). Fungsi ini

²⁸<http://repository.usu.ac.id/bitstream/handle/123456789/37052/Chapter%20II.pdf?sequence=4>. Diakses Pada Hari Selasa, 03 Oktober 2017. Pukul 23:27 WIB

- bertujuan agar orang-orang bertingkah laku sesuai dengan harapan masyarakat umum yang telah diwujudkan dalam norma hukum yang dibentuk bersama
- b. Fungsi kedua dimaksudkan untuk menjamin kelangsungan hidup masyarakat dalam suasana perubahan masyarakat yang terus menerus terjadi. Ini dimaksudkan agar setiap perubahan masyarakat sesuai dengan tujuan-tujuan yang telah direncanakan atau dikehendaki.²⁹

Dampak tersebut tidak selalu berlangsung demikian, karena di pihak lain timbul itikad tidak baik untuk mencari keuntungan dengan melawan hukum, yang berarti melakukan kejahatan. Pemanfaatan teknologi informasi dan transaksi elektronik, sering disalahgunakan oleh sebagian kalangan untuk memperoleh keuntungan pribadi maupun kelompok, yang pada akhirnya perbuatan itu merupakan perbuatan yang tergolong dalam tindak pidana.

Hukum acara pidana atau hukum pidana formil merupakan aturan-aturan untuk melaksanakan hukum pidana materil dalam proses peradilan pidana, mulai dari tahap penyidikan, penuntutan, persidangan, sampai pada pelaksanaan putusan pengadilan. Hukum acara pidana mengatur prosedur yang harus dilakukan oleh aparat penegak hukum dalam menjalankan kewenangannya dan mengatur tahap-tahap proses peradilan pidana. Hukum acara pidana menegaskan hak dan kewajiban para saksi, tersangka dan terdakwa dalam setiap tahap dalam proses peradilan pidana. Dengan adanya aturan yang dimaksud, diharapkan kebenaran materil dapat terungkap, keadilan dapat ditegakkan, ketertiban dapat dijaga, hak asasi manusia dapat dilindungi, dan penyalahgunaan wewenang dapat dihindari.

Payung hukum pidana formil yang berlaku di Indonesia adalah Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana yang disebut juga Kitab Undang-Undang Hukum Acara Pidana (KUHAP). KUHAP merupakan hukum acara untuk melaksanakan hukum pidana materil yang utamanya diatur

²⁹<http://repository.usu.ac.id/bitstream/handle/123456789/36008/10E00138.pdf?sequence=1>. Diakses Pada Hari Selasa, 03 Oktober 2017. Pukul 23:27 WIB

dalam Kitab Undang-Undang Hukum Pidana (KUHP). Dalam perkembangannya, terdapat begitu banyak undang-undang yang lahir kemudian yang memuat pengaturan dan sanksi pidana yang tidak diatur dalam KUHP.³⁰

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan undang-undang yang secara khusus mengatur mengenai transaksi elektronik dan didalamnya juga diatur perbuatan-perbuatan yang dikategorikan sebagai tindak pidana siber serta sanksi pidananya.

Alat bukti dalam Undang-undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terdapat dalam Pasal 5 yang berbunyi sebagai berikut:

1. Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
2. Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat 1 merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.³¹

Penerapan alat bukti sangat erat kaitannya dengan pembuktian. Pembuktian sebenarnya telah dimulai pada tahap penyidikan. Pembuktian bukan dimulai pada tahap penuntutan maupun persidangan. Dalam penyidikan, penyidik akan mencari pemenuhan unsur pidana berdasarkan alat-alat bukti yang diatur dalam perundang-undangan. Pada tahap penuntutan dan persidangan kesesuaian dan hubungan antara alat-alat bukti dan pemenuhan unsur pidana akan diuji. Dalam rangka penegakan hukum sesuai Sistem Peradilan Pidana, Polri bertugas melakukan penyidikan tindak pidana yang dilaksanakan oleh penyidik/penyidik pembantu pada Fungsi Reserse Kriminal Polri maupun fungsi operasional Polri lainnya yang diberi wewenang untuk melakukan penyidikan serta

³⁰Josua Sitompul. *Op. Cit.*, halaman 307.

³¹*Ibid.*, halaman 279.

mengkoordinasikan dan melakukan pengawasan terhadap Penyidik Pegawai Negeri Sipil (PPNS). Peranan penyidik Polri dalam sistem Peradilan Pidana berada pada bagian terdepan dan merupakan tahap awal mekanisme proses peradilan pidana yaitu pemeriksaan pendahuluan.

Penyidikan itu sendiri merupakan kegiatan penyidik dalam mencari dan mengumpulkan bukti agar membuat terang tindak pidana yang terjadi dan untuk menemukan tersangkanya. Suatu peristiwa atau tindak pidana dapat diketahui melalui laporan, pengaduan, tertangkap tangan dan diketahui sendiri oleh petugas Polri. Penyidikan tindak pidana pada hakekatnya merupakan wujud penegakan hukum yang di atur dalam perundang-undangan mengingat tugas-tugas penyidikan tindak pidana banyak berkaitan dengan hal-hal yang menyangkut Hak Asasi Manusia (HAM). Salah satu tugas dari penyidik kepolisian adalah melakukan pemeriksaan terhadap tersangka tindak pidana. Pemeriksaan yang dilakukan oleh Penyidik dalam rangka penyidikan merupakan kegiatan untuk mendapatkan keterangan, kejelasan dan keidentikan tersangka dan atau saksi dan atau alat bukti maupun tentang unsur-unsur tindak pidana yang telah terjadi sehingga kedudukan atau peranan seseorang maupun alat bukti di dalam tindak pidana tersebut menjadi jelas dan dituangkan dalam Berita Acara Pemeriksaan (BAP).

Pada dasarnya seluruh kegiatan dalam proses hukum penyelesaian perkara pidana, sejak penyidikan sampai putusan akhir diucapkan di muka persidangan oleh majelis hakim adalah berupa kegiatan yang berhubungan dengan pembuktian atau kegiatan untuk membuktikan. Walaupun hukum pembuktian perkara pidana

terfokus pada proses kegiatan pembuktian di sidang pengadilan, tetapi sesungguhnya proses membuktikan sudah ada dan dimulai pada saat penyidikan. Bahkan, pada saat penyelidikan, suatu pekerjaan awal dalam menjalankan proses perkara pidana oleh negara. Yang dimaksud dengan mencari bukti sesungguhnya adalah mencari alat bukti, karena bukti tersebut hanya terdapat atau dapat diperoleh dari alat bukti dan termasuk barang bukti. Bukti yang terdapat pada alat bukti itu kemudian dinilai oleh pejabat penyidik untuk menarik kesimpulan, apakah bukti yang ada itu menggambarkan suatu peristiwa yang diduga tindak pidana atau tidak. Bagi penyidik, bukti yang terdapat dari alat bukti itu dinilai untuk menarik kesimpulan, apakah dari bukti yang ada itu sudah cukup untuk membuat terang tindak pidana yang terjadi dan sudah cukup dapat digunakan untuk menemukan tersangkanya.

Sejak adanya laporan mengenai terjadinya tindak pidana, penyidik telah mendapatkan satu bagian dari keseluruhan bagian teka-teki gambar, dan setelah menemukan bagian pertama itu, penyidik harus mencari bagian-bagian lain dari gambar untuk disusun sehingga ia memperoleh gambar yang utuh mengenai suatu tindak pidana dan pelakunya. Akan tetapi, mengingat gambar yang utuh itu terdiri dari begitu banyak bagian dan bagian-bagian itu tersebar di banyak tempat dalam berbagai bentuk, dalam banyak kasus penyidik menemukan banyak kesulitan. Untuk mencari bagian-bagian lain itu, penyidik harus bergerak ke masa lalu. Dalam usaha menemukan kebenaran materil dimasa lalu itu, penyidik menemukan kenyataan bahwa semakin lama mereka bergerak semakin kecil kemungkinannya untuk berhasil menemukan keseluruhan gambar. Jejak dapat hilang, saksi dapat

lupa, dan barang bukti dapat rusak. Oleh karena itu dibutuhkan penyidik yang ahli dibidangnya dan bergerak dengan secepat mungkin berdasarkan bukti yang ditemukan.

Proses penegakan hukum Oleh Kepolisian diawali dengan proses penyelidikan. Dimana, Penyelidikan berdasarkan ketentuan Pasal 1 angka 5 KUHAP adalah serangkaian tindakan penyidik untuk mencari dan menemukansuatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam undang-undang ini. Sedangkan penyidik berdasarkan ketentuan Pasal 1 Angka 4 KUHAP adalah pejabat polisi negara Republik Indonesia yang diberi wewenang oleh undang-undang ini untuk melakukan penyelidikan. Setelah penyelidikan selesai makan ditingkatkan ke tahap penyidikan.³²

Berdasarkan Pasal 1 angka 2 KUHAP, Penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang untuk mencari serta mengumpulkan bukti yang terjadi guna menemukan tersangkanya. Sedangkan penyidik diatur dalam Pasal 1 angka 1 KUHAP yang mengatur bahwa penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang untuk melakukan penyidikan.³³

Pasal 42 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur bahwa penyidikan terhadap tindak pidana Informasi Dan Transaksi Elektronik dilakukan berdasarkan ketentuan dalam hukum acara pidana dan ketentuan dalam UU ITE. Maksudnya, semua aturan yang ada dalam KUHAP tetap berlaku sebagai ketentuan umum (*lex*

³²Andi Sofyan dan Abdul asis. *Op. Cit.*, halaman 84.

³³*Ibid.*,

generalis) kecuali yang disimpangi oleh UU ITE sebagai ketentuan yang khusus (*lex specialis*). Dengan kata lain, ketentuan-ketentuan mengenai penyidikan yang tidak diatur dalam UU ITE tetap diberlakukan sebagaimana diatur dalam KUHAP. Pengaturan ini juga selaras dengan ketentuan dalam Pasal 284 ayat (2) KUHAP yaitu bahwa terhadap semua perkara diberlakukan ketentuan KUHAP, dengan pengecualian untuk sementara mengenai ketentuan khusus acara pidana sebagaimana tersebut pada undang-undang tertentu, sampai ada perubahan dan atau dinyatakan tidak berlaku lagi. UU ITE ialah salah satu contoh dari ketentuan khusus acara pidana sebagaimana tersebut pada undang-undang tertentu dan ketentuan khusus acara pidana ini tetap berlaku sebelum ditinjau kembali, diubah atau dicabut.³⁴

Penyidik yang diberikan kewenangan untuk melakukan penyidikan tindak pidana Informasi dan Transaksi Elektronik ialah penyidik polisi negara Republik Indonesia (penyidik Polri) dan penyidik pegawai negeri sipil tertentu di lingkungan pemerintah yang lingkup tugas dan tanggung jawabnya di bidang teknologi informasi dan transaksi elektronik. Penegasan ini selaras dengan pengaturan dalam KUHAP yang mendefinisikan penyidik sebagai pejabat polisi negara republik indonesia atau pejabat pegawai negeri tertentu yang diberi wewenang khusus oleh undang-undang untuk melakukan penyidikan.

Pemberian kewenangan kepada polri dan pejabat pegawai negeri tertentu untuk melakukan penyidikan tindak pidana yang tidak diatur dalam KUHAP, seperti yang diatur dalam UU ITE merupakan pengaturan yang umum ditemui dalam perundang-undangan Indonesia. Pada prinsipnya, kepolisian negara republik indonesia merupakan alat negara utama yang berperan dalam penegakan hukum dalam penyidikan untuk semua tindak pidana. Sedangkan pejabat pegawai negeri sipil yang mengemban fungsi kepolisian, diberikan kewenangan sebagai penyidik berdasarkan undang-undang yang menjadi kewenangannya untuk

³⁴Josua Sitompul. *Op. Cit.*, halaman 309.

melakukan penyidikan terhadap tindak-tindak pidana tertentu. Penyidik Polri memiliki kapasitas dan kapabilitas untuk melakukan semua penyidikan. Akan tetapi, PPNS diberikan wewenang tertentu untuk melakukan penyidikan karena mereka yang dinilai ahli atau memiliki kompetensi untuk memahami tindak-tindak pidana tertentu disektornya masing-masing.

Berdasarkan Pasal 7 ayat (1) KUHAP, bahwa penyidik karena kewajiban mempunyai wewenang, yaitu :

- a) Menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana
- b) Melakukan tindakan pertama pada saat di tempat kejadian
- c) Menyuruh berhenti seseorang tersangka dan memeriksa tanda pengenal diri tersangka
- d) Melakukan penangkapan, penahanan, penggeledahan, dan penyitaan
- e) Melakukan pemeriksaan dan penyitaan surat
- f) Mengambil sidik jari dan memotret seorang
- g) Memanggil orang untuk didengar dan diperiksa sebagai tersangka atau saksi
- h) Mendatangkan orang ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara
- i) Mengadakan penghentian penyidikan
- j) Mengadakan tindakan lain menurut hukum yang bertanggung jawab.³⁵

Hal ini juga sebagaimana diatur dalam Pasal 43 ayat (5) UU ITE, Penyidik berwenang untuk :

- 1) Menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana teknologi informasi dan transaksi elektronik.
- 2) Memanggil setiap orang atau pihak lainnya untuk didengar dan/atau diperiksa sebagai tersangka atau saksi.
- 3) Melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana teknologi informasi dan transaksi elektronik.
- 4) Melakukan pemeriksaan terhadap orang dan/atau badan usaha yang patut diduga melakukan tindak pidana teknologi informasi dan transaksi elektronik.

³⁵ Andi Sofyan dan Abdul asis. *Op. Cit.*, halaman 88.

- 5) Melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan teknologi informasi yang diduga digunakan untuk melakukan tindak pidana teknologi informasi dan transaksi elektronik.
- 6) Melakukan penggeledahan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana teknologi informasi dan transaksi elektronik.
- 7) Melakukan penyegelan dan penyitaan terhadap alat dan atau sarana kegiatan teknologi informasi yang diduga digunakan secara menyimpang dari ketentuan Peraturan Perundang-undangan.
- 8) Meminta bantuan ahli yang diperlukan dalam penyidikan
- 9) Mengadakan penghentian penyidikan tindak pidana sesuai dengan ketentuan hukum acara pidana yang berlaku.³⁶

Berkaitan dengan penerapan alat bukti tindak pidana informasi dan transaksi elektronik, UU ITE telah mengatur bahwa upaya paksa yang dapat digunakan oleh aparat penegak hukum untuk memperoleh alat bukti elektronik ialah melalui penggeledahan dan penyitaan sistem elektronik atau melalui intersepsi atau penyadapan. Aparat penegak hukum menggunakan cara penggeledahan dan penyitaan apabila penyidik sudah mengetahui secara jelas sumber alat bukti elektronik tersebut (lokasi komputer, laptop, USB, server milik tersangka, korban, atau saksi). Sedangkan berdasarkan batasan-batasan yang diatur dalam perundang-undangan, intersepsi atau penyadapan dapat digunakan oleh aparat penegak hukum sebagai cara mengumpulkan informasi dan keterangan terkait dengan suatu tindak pidana (tersangka, tindak pidana yang dipersangkakan, saksi, lokasi tindak pidana). Informasi tersebut dapat dijadikan alat bukti.

Berdasarkan sistem pembuktian di Indonesia, kesalahan terdakwa ditentukan oleh minimal dua alat bukti yang sah dan keyakinan hakim. Keabsahan alat bukti didasarkan pada pemenuhan syarat dan ketentuan baik segi formil maupun materil. Prinsip ini juga berlaku terhadap pengumpulan dan penyajian alat bukti

³⁶*Ibid.*, halaman 312.

elektronik baik yang dalam bentuk original maupun hasil cetaknya, yang diperoleh baik melalui penggeledahan dan penyitaan maupun intersepsi.

Pasal 43 ayat (6) Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, menyatakan bahwa: “Dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.”³⁷

Keharusan izin dari ketua pengadilan setempat adalah dalam rangka *check and balance* antara aparat penegak hukum dari eksekutif dengan peradilan dari yustisi. Dengan demikian kemungkinann penyalahgunaan wewenang dapat dicegah. Ketentuan izin dalam UU ITE harus selaras dengan KUHAP, oleh karena itu penggeledahan dan penyitaan sistem elektronik harus dilakukan dengan:

- a. Disaksikan minimal dua orang saksi.
- b. Dibuat acara penggeledahan dan /atau penyitaan (Pasal 34 ayat (1) KUHAP).³⁸

Selain itu, penyidik harus memperhatikan Pasal 43 ayat (2) UU ITE yaitu harus dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan public, integritas data, atau keutuhan data sesuai dengan ketentuan peraturan perundang-undangan.

KUHAP telah memberikan pengaturan yang jelas mengenai upaya paksa penggeledahan dan penyitaan secara umum, tetapi belum terhadap sistem elektronik. Akan tetapi, KUHAP belum mengatur mengenai intersepsi atau

³⁷http://eprints.ums.ac.id/30305/7/NASKAH_PUBLIKASI.pdf. Di Akses Pada Hari Senin, 10 April 2017. Pukul 21.15 WIB

³⁸*Ibid.*,

penyadapan, hal ini diatur di dalam berbagai undang-undang yang lebih spesifik. Oleh karena itu, ketentuan tentang persyaratan formil dan materil mengenai alat bukti elektronik harus mengacu pada KUHAP, UU ITE, dan undang-undang lain yang mengatur secara spesifik mengenai alat bukti elektronik tersebut.

Alat bukti elektronik adalah Informasi Elektronik dan/atau Dokumen Elektronik yang memenuhi persyaratan formil dan persyaratan materil yang diatur dalam Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Barang bukti dapat dikatakan alat bukti digital karena berbentuk Informasi Elektronik dan/atau Dokumen Elektronik yang sesuai dengan kriteria Pada Pasal 1 angka 1 dan angka 4 Undang-Undang No. 11 tahun 2008 yang meliputi tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya dan bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya, yang dalam putusan diatas merupakan alat bukti yang mempunyai kedudukan untuk menjelaskan suatu tindak cyber crime yang

mungkin dilakukan oleh tersangka, sehingga alat bukti digital ini memperjelas fakta yang terjadi dengan didukung alat bukti lainnya.³⁹

Persyaratan materil ialah ketentuan dan persyaratan yang dimaksudkan untuk menjamin keutuhan data (*integrity*), ketersediaan (*availability*), keamanan (*security*), keotentikan (*authennticity*), dan keteraksesan (*accessibility*) informasi atau dokumen elektronik dalam proses pengumpulan dan penyimpanan dalam proses penyidikan dan penuntutan, serta penyampaianya di sidang pengadilan.

Persyaratan materil alat bukti elektronik diatur dalam Pasal 5 ayat (3) UU ITE, yaitu informasi atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam UU ITE. Lebih lanjut, sistem elektronik diatur dalam Pasal 15 sampai dengan Pasal 16 UU ITE dan dari kedua pasal ini, dapat diperoleh persyaratan yang lebih rinci, yaitu bahwa sistem elektronik :

- 1) Andal, aman, dan bertanggung jawab.
- 2) Dapat menampilkan kembali informasi atau dokumen elektronik secara utuh
- 3) Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik.
- 4) Dilengkapi dengan prosedur atau petunjuk dan dapat beroperasi sesuai prosedur atau petunjuk yang telah ditetapkan tersebut.⁴⁰

Persyaratan formil alat bukti elektronik diatur dalam Pasal 5 ayat (4) dan Pasal 43 UU ITE, yaitu :

- a) Informasi atau dokumen elektronik tersebut bukanlah ;
 - 1) Surat yang menurut undang-undang harus dibuat dalam bentuk tertulis
 - 2) Surat beserta dokumennya yang menurut undang-undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta tanah.
- b) Penggeledahan atau penyitaan terhadap sistem elektronik harus dilakukan atas izin ketua pengadilan negeri setempat

³⁹*Ibid.*,

⁴⁰Josua Sitompul. *Op. Cit.*, halaman 284.

- c) Penggeledahan atau penyitaan tetap menjaga terpeliharanya kepentingan pelayanan umum.⁴¹

Pasal 6 UU ITE juga memberikan persyaratan materil mengenai keabsahan alat bukti elektronik, yaitu bahwa informasi atau dokumen elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Alat bukti elektronik harus memenuhi persyaratan baik secara formil dan materil sehingga alat bukti tersebut dapat dinyatakan sah dan dapat dipergunakan di persidangan. Ketentuan dan persyaratan tersebut adalah untuk menjamin kepastian hukum dan berfungsi sebagai alat penguji dalam menentukan keabsahan alat bukti sehingga hakim yakin dengan fakta-fakta hukum yang dihadirkan melalui alat bukti elektronik.

UU ITE secara komprehensif telah mengakui alat bukti elektronik sebagai perluasan alat bukti yang ada dalam hukum acara baik pidana maupun perdata, dan sebagai perluasan alat bukti dalam hukum acara yang ada pada saat ini. Untuk dapat dipercaya sebagai alat bukti, maka dapat dilakukan dengan cara menggunakan peralatan komputer untuk menyimpan dan memproduksi print-out, proses data seperti pada umumnya dengan memasukkan inisial dalam sistem pengelolaan arsip yang dikomputerisasikan dan menguji data dalam waktu yang tepat setelah data dituliskan oleh seseorang yang mengetahui peristiwa hukum nya.⁴²

Pada dasarnya seluruh kegiatan dalam proses hukum penyelesaian perkara pidana, sejak penyidikan sampai putusan adalah berupa kegiatan yang berhubungan dengan pembuktian atau kegiatan untuk membuktikan. Mencari bukti sesungguhnya adalah mencari alat bukti. Bukti yang terdapat pada alat bukti

⁴¹*Ibid.*, halaman 285.

⁴²Petrus Reinhard Golose. 2008. *Seputar Kejahatan Hacking. Teori Dan Studi Kasus*. Jakarta:Yayasan Pengembangan Kajian Ilmu Kepolisian., halaman 72.

itu kemudian dinilai oleh pejabat penyelidik untuk menarik kesimpulan, apakah bukti yang ada itu menggambarkan suatu peristiwa yang diduga tindak pidana ataukah tidak. Pembuktian sendiri ialah perbuatan membuktikan, membuktikan berarti memberi atau memperlihatkan bukti, melakukan sesuatu sebagai kebenaran, melaksanakan, menandakan, menyaksikan, dan meyakinkan.

Alat bukti elektronik memiliki cakupan yang luas dan jenis yang beragam. Tiap jenis alat bukti elektronik tersebut memiliki karakteristik secara teknis yang memerlukan penanganan tersendiri dalam menentukan keabsahannya secara hukum. Oleh karena itu, perlu adanya kesepahaman diantara kalangan aparat penegak hukum mengenai prinsip-prinsip pengumpulan, penganalisaan, serta penyajian alat bukti elektronik yang beragam itu. Dalam hal diperlukan, dapat ditetapkan peraturan dan putusan yang lebih spesifik yang dijadikan pedoman dalam memeriksa alat bukti elektronik baik ditingkat penyidikan, penuntutan, maupun di persidangan.

Berdasarkan penjelasan di atas, bahwa salah satu syarat materil alat bukti elektronik dapat diterima di pengadilan ialah bahwa informasi dan dokumen elektronik harus dapat dijamin ketersediaan, keutuhan, keotentikan, dan keteraksesannya. Dengan dipenuhinya persyaratan materil dan juga persyaratan formil maka alat bukti elektronik memiliki nilai yang sama. Untuk menjamin terpenuhinya persyaratan tersebut diperlukan suatu metode ilmiah yang didukung teknologi khusus untuk memeriksa alat bukti elektronik.

Informasi elektronik atau dokumen elektronik, bila tidak ditangani dengan benar, dapat berubah, rusak atau hilang. Jika informasi tersebut hilang dan tidak

dapat ditemukan kembali maka aparat penegak hukum tidak dapat memperoleh alat bukti elektronik. Jika informasi tersebut berubah atau rusak maka informasi yang dimaksud tidak dapat dijadikan alat bukti dipersidangan. Oleh karena itu, aparat penegak hukum dalam hal ini penyidik harus mencari, mengumpulkan, dan menganalisa informasi dengan cepat dan tepat.

Hal lain yang perlu diperhatikan dalam pengumpulan barang bukti yang menyimpan alat bukti elektronik ialah bahwa ada begitu banyak jenis alat dan media yang menyimpan informasi. Tidak hanya komputer, laptop, handphone, atau USB, tetapi juga router, modem, kamera digital, hardisk eksternal, CD atau DVD, serta PDA. Mengingat ada begitu banyak jenis media penyimpanan informasi dan teknologi, penanganannya memiliki karakteristik masing-masing.

Tahapan pengumpulan alat bukti elektronik, penyidik akan menemukan berbagai informasi, baik yang relevan dengan tindak pidana, maupun yang tidak relevan. Terkait dengan hal ini, penyidik harus menjaga kerahasiaan informasi, khususnya informasi yang terkait privasi seseorang yang tidak relevan dengan tindak pidana. Semua informasi yang tidak relevan tidak boleh diungkap di pengadilan. Dalam pengumpulan dan pemeriksaan alat bukti elektronik, banyak kasus di Indonesia, penyidik memerlukan kerjasama dengan penyelenggara telekomunikasi.

Berdasarkan informasi yang ia peroleh, penyidik harus menghubungi penyelenggara telekomunikasi yang dimaksud untuk memperoleh rekaman transaksi elektronik (*log file*) dari modem yang digunakan. Selain itu, penyelenggara juga dapat memberikan informasi mengenai identitas yang

diberikan oleh pengguna layanan telekomunikasi pada waktu mendaftar *SIM Card* untuk pertama kalinya.

Alat bukti elektronik, sebagai alat bukti yang sah dalam pembuktian perkara pidana, tentu berbeda dengan alat-alat bukti lainnya, semisal surat ataupun saksi, yang dapat dengan mudah dilihat, dibaca dan dinilai kekuatannya pembuktian secara langsung. Bukti elektronik, sebagaimana perkembangan teknologi informasi dengan berbagai karakteristiknya, tidak saja dari segi formalitasnya (cara memperoleh) maupun dari segi materiilnya (melihat nilai pembuktiannya) agar mempunyai kekuatan pembuktian di persidangan, *reability* (dapat dipertanggungjawabkan keabsahannya), *necessity* (diperlukan untuk pembuktian) dan *relevance* (relevan dengan pembuktian). Sebagai salah satu alat bukti yang sah, karakteristik dari bukti elektronik memerlukan penanganan yang khusus pula.

UU ITE tidak mengatur perihal cara atau metode yang digunakan untuk mengumpulkan atau mengamankan, menampilkan, atau menjamin keutuhan informasi alat bukti elektronik karena pada dasarnya, UU ITE menganut sas netral teknologi. Maksudnya, cara atau metode pengumpulan dan pengamanan alat bukti elektronik dapat menggunakan teknologi yang tersedia sepanjang dapat memenuhi persyaratan keabsahan alat bukti elektronik.

Digital forensik yang juga dikenal dengan nama Computer Forensik adalah salah satu subdivisi dari ilmu forensik yang melakukan pemeriksaan dan menganalisa bukti legal yang ditemui pada computer dan menyimpan media

digital, misalnya flashdisk, hardisk, CDROM, pesan email, gambar, atau bahkan, sederetan paket atau informasi yang berpindah dalam suatu jaringan computer.⁴³

Dalam menangani bukti elektronik sehingga dapat diterima di persidangan adalah terpenuhinya prinsip-prinsip dasar sebagaimana yang telah dikeluarkan oleh *Association of Chief Police Officers* (ACPO) yang memberikan empat prinsip dalam penanganan alat bukti elektronik, yaitu :

1. Semua penanganan terhadap alat bukti elektronik (yaitu data yang diperoleh dari komputer atau media penyimpanan, atau alat dan perangkat elektronik lain) yang dilakukan oleh aparat penegak hukum tidak boleh mengakibatkan adanya perubahan atau kerusakan terhadap data agar dapat diterima dipengadilan. Dengan demikian, data yang diperoleh pada waktu penyidikan sama dengan data yang dihadirkan di persidangan. Penanganan yang tidak tepat terhadap data dapat merusak, menghilangkan, mengubah data.
2. Dalam keadaan-keadaan dimana seseorang harus mengakses data original yang terdapat dalam komputer atau media penyimpanan, orang yang dimaksud harus memiliki kompetensi untuk melakukannya, dan harus mampu memberikan penjelasan mengenai relevansi tindakannya terhadap data dan akibat perbuatannya itu.
3. Harus ada prosedur dan proses yang jelas yang diterapkan untuk mengumpulkan dan menganalisa alat bukti elektronik. Prosedur yang dimaksud memuat penanganan alat bukti elektronik mulai dari penemuan barang bukti (komputer, telepon genggam, USB, router, atau laptop) yang mengandung alat bukti elektronik, pembungkusan barang bukti,

⁴³ <https://www.google.co.id/amp/s/aprilinaputri19.wordpress.com/2013/09/30/mengenal-lebih-tau-tentang-forensik-it-cyber-crime/amp>. Diakses Pada Hari Rabu, 11 Oktober 2017. Pukul 13.00 WIB.

pemeriksaan, analisa dan pelaporan. Dengan demikian, setiap pihak yang berkepentingan dapat memeriksa proses dan prosedur yang dimaksud dan memperoleh hasil yang sama. Terakhir, harus ada pihak atau pejabat yang bertanggung jawab untuk memastikan pelaksanaan kegiatan agar sesuai dengan peraturan perundang-undangan serta keseluruhan proses dan prosedur yang dimaksud.⁴⁴

Prinsip-prinsip dasar di atas, dalam implementasinya diterapkan melalui tahapan digital forensik yang harus dilakukan dalam menyajikan bukti elektronik. Tahapan ini pula yang dapat ditanyakan kepada ahli di persidangan dalam menilai kekuatan bukti elektronik dalam pembuktian perkara. Secara umum, digital forensik dapat dibagi menjadi :

- a. Komputer forensik, yaitu forensik yang dilakukan terhadap komputer, laptop, atau hardisk dan media penyimpanan sejenis.
- b. Mobile forensik, yaitu forensik yang dilakukan terhadap telepon genggam.
- c. Audio forensik, yaitu forensik yang dilakukan terhadap suara.
- d. Image forensik, yaitu forensik yang dilakukan terhadap gambar.
- e. Video forensik, yaitu forensik yang dilakukan terhadap video dan CCTV.⁴⁵

Komponen pada digital forensik pada umumnya hampir sama dengan bidang yang lain. Komponen ini mencakup manusia (*people*), perangkat/peralatan (*equipment*) dan aturan (*protocol*) yang dirangkai, dikelola dan diberdayakan sedemikian rupa dalam upaya mencapai tujuan akhir dengan segala kelayakan dan kualitas.

Manusia yang diperlukan dalam komputer forensik merupakan pelaku yang tentunya mempunyai kualifikasi tertentu untuk mencapai kualitas yang diinginkan. Belajar forensik tidak sama dengan menjadi ahli dalam bidang forensik. Dibutuhkan lebih dari sekedar pengetahuan umum tentang komputer, tetapi juga pengalaman (*experience*) disamping berbagai pelatihan (*training*) pada materi-

⁴⁴Josua Sitompul. *Op. Cit.*, halaman 289.

⁴⁵*Ibid.*, halaman 291.

materi digital forensik yang telah ditempuh dan dibuktikan dengan sertifikat-sertifikat pendukung. Ada tiga kelompok sebagai pelaku digital forensik :

- 1) *Collection Specialist*, yang bertugas mengumpulkan barang bukti berupa *digital evidence*.
- 2) *Examiner*, tingkatan ini hanya memiliki kemampuan sebagai penguji terhadap media dan mengekstrak data.
- 3) *Investigator*, tingkatan ini sudah masuk kedalam tingkatan ahli atau sebagai penyidik.⁴⁶

Berdasarkan prinsip ACPO yang telah dijelaskan di atas, prosedur digital forensik terbagi tiga tahap besar, yaitu :

a) Pengambilan (*acquisition*)

Mengingat sifatnya yang dapat diubah, dirusak, atau dihilangkan apabila tidak ditangani dengan tepat, pengambilan informasi atau dokumen elektronik harus dilakukan dengan menjaga dan melindungi keutuhan atau integritasnya. Tahap ini dimaksudkan untuk mengambil dan mengamankan alat bukti elektronik asli (*original*). Cara atau prosedur pengambilan alat bukti elektronik original dapat didasarkan pada kondisi awal ditemukannya alat bukti elektronik atau alat/perangkat yang menyimpan alat bukti elektronik tersebut.

b) Pemeriksaan dan analisa

Pemeriksaan terhadap alat bukti elektronik *original* umumnya menggunakan perangkat keras dan perangkat lunak yang khusus dibuat

⁴⁶<http://e-dokumen.kemenag.go.id/files/VQ2Hv7uT1339506324.pdf>. Di Akses Pada Hari Selasa, 11 April 2017. Pukul 23.45 WIB

untuk kepentingan digital forensik. Pada tahap ini, pemeriksa melakukan ekstraksi, yaitu mengambil seluruh data dari media dimana data tersebut tersimpan, termasuk data yang telah terhapus sebelumnya. Pemeriksa juga menggunakan *write blocker*, yaitu alat yang digunakan untuk mencegah penulisan terhadap data original. Selain itu, dalam melakukan pengambilan data, pemeriksa juga perlu menentukan nilai dari keseluruhan data yang diambil (*hash*). Nilai (*hash*) dari data original akan sama dengan nilai dari hasil ekstraksi. Sehingga apabila diperlukan pemeriksaan oleh pemeriksa yang berbeda, nilai dari alat bukti elektronik tersebut akan sama. Setelah alat bukti elektronik original diperoleh, pemeriksaan terhadap alat bukti elektronik harus dilakukan dengan membuat salinan (*copy*) dari informasi atau dokumen elektronik yang asli (*original*). Setelah pengambilan informasi atau dokumen elektronik dilakukan, tahap selanjutnya ialah pemeriksaan dan analisa terhadap alat bukti elektronik. Pemeriksaan dilakukan terhadap salinan dari alat bukti elektronik yang asli. Pemeriksa juga dapat membuat salinan dari salinan alat bukti elektronik sebagai bahan kerja. Pada tahap ini, pemeriksa juga melakukan analisa, yaitu menginterpretasikan informasi yang telah diekstraksi dan menentukan informasi atau data yang relevan dengan tindak pidana.

c) Dokumentasi dan presentasi

Setiap tindakan yang dilakukan dalam pengumpulan dan pemeriksaan alat bukti elektronik harus didokumentasikan secara akurat dan menyeluruh. Tidak hanya tindakan dalam melakukan digital forensik, tetapi juga tindakan yang terkait dengannya. Laporan dapat memuat proses dan tahapan yang dilakukan dalam pemeriksaan, termasuk alat dan perangkat yang digunakan. Selain itu, laporan juga perlu memuat informasi

mengenai keseluruhan data yang diperoleh serta data yang relevan dengan tindak pidana.⁴⁷

Melalui prinsip-prinsip dan tahapan dalam digital forensik, maka bukti elektronik akan sangat berperan dalam proses pembuktian dalam perkara pidana, dimana yang hendak dicari adalah kebenaran materiil. Beberapa hal yang dapat diungkap dan dibuktikan dengan bukti elektronik, adalah dapat mengidentifikasi obyek (bukti elektronik), menentukan keterkaitan bukti elektronik dengan pelaku yang diduga melakukan tindak pidana, merekonstruksi masa lalu, melindungi yang tidak salah dan untuk menyiapkan ahli di persidangan.

Hal ini tidak lepas dari pengertian digital forensik sebagai salah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang ditemui pada komputer dan media penyimpanan digital. Menjabarkan keadaan ini dari suatu artefak digital yang dapat mencakup sebuah sistem komputer, media penyimpanan (seperti flash disk, hardisk, atau CD-ROM), sebuah dokumen elektronik (misalnya sebuah pesan email atau gambar JPEG), atau bahkan sederetan paket yang berpindah dalam jaringan komputer. Sehingga isi dari bukti elektronik yang diperoleh dari proses bukti elektronik tidak sekedar ada informasi apa dalam bukti elektronik akan tetapi dapat pula merinci urutan peristiwa yang menyebabkan terjadinya situasi terkini.

Prinsip-prinsip dan tahapan melalui digital forensik dalam menggali alat bukti berupa bukti elektronik sehingga dapat digunakan dalam pembuktian perkara pidana, ternyata tidak mudah karena karakteristik yang melekat padanya. Setelah

⁴⁷Josua Sitompul. *Op. Cit.*, halaman 291.

prinsip dan tahapan terpenuhi (dapat dikatakan sebagai syarat formal) maka selanjutnya adalah syarat materiil, yaitu keterkaitan antara isi bukti elektronik dengan pembuktian perkara. Sebagaimana alat-alat bukti lainnya dalam pembuktian perkara pidana yang bersifat bebas, dalam arti akan kembali kepada hakim dalam menilai persesuaian dengan alat-alat bukti lainnya di persidangan dalam rangka untuk memenuhi minimum pembuktian untuk dapat menimbulkan keyakinan pada hakim.

Kepolisian Daerah Sumatera Utara dalam menangani tindak pidana Informasi dan Transaksi Elektronik bertugas untuk melakukan penyelidikan dan penyidikan. Kasus yang telah ditangani oleh Kepolisian Daerah Sumatera Utara dari tahun 2015 ada 92 kasus, tahun 2016 ada 120 kasus, dan tahun 2017 18 kasus. Dimana, Pasal yang paling banyak dilanggar pengguna medsos adalah Pasal 27 dan Pasal 28 UU ITE.⁴⁸

Proses penerapan alat bukti dalam tindak pidana informasi dan transaksi elektronik di Kepolisian Daerah Sumatera Utara dimulai dari proses penyelidikan dan penyidikan. Penyelidikan maupun penyidikan tindak pidana *cybercrime* dilakukan setelah adanya laporan maupun pengaduan masyarakat terlebih dahulu kalau tindak pidana tersebut delik aduan contohnya pencemaran nama baik. Akan tetapi, kalau ia pidana umum tanpa adanya laporan aduan Kepolisian bisa saja melakukan tindakan.⁴⁹

Tahapan awal yang akan dilakukan dalam menangani tindak pidana Informasi dan Transaksi Elektronik adalah penyelidikan. Tujuan penyelidikan adalah untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan. Setelah penyelidikan selesai, maka tahap selanjutnya adalah melakukan penyidikan. Penyidikan dilakukan untuk mencari serta mengumpulkan bukti yang terjadi guna menemukan tersangkanya. Pada tahap penyidikan, pihak penyidik akan

⁴⁸ Hasil Wawancara Dengan Bapak Kompol Jumanto. Kanit 3 Subdit II. Ditreskrimsus Polda Sumut. Pada Hari Rabu, 01 Maret 2017.

⁴⁹ Hasil Wawancara Dengan Bapak Kompol Jumanto. Kanit 3 Subdit II. Ditreskrimsus Polda Sumut. Pada Hari Rabu, 01 Maret 2017.

melakukan penggeledahan dan penyitaan terhadap benda yang digunakan sebagai alat atau yang berhubungan dengan tindak pidana dan diduga mengandung alat bukti elektronik contohnya handphone, komputer, laptop, maupun alat komunikasi lain yang digunakan saat melakukan tindak pidana. Penggeledahan dan penyitaan tersebut dilakukan setelah meminta persetujuan penetapan sita dari pengadilan setempat dimana barang tersebut disita.

Setelah dilakukannya penggeledahan dan penyitaan terhadap seluruh alat/perangkat yang berkaitan dengan tindak pidana informasi dan transaksi elektronik, maka penerapan alat bukti tindak pidana informasi dan transaksi elektronik oleh kepolisian daerah sumatera utara dilakukan melalui tahapan digital forensik di laboratorium forensik kepolisian daerah sumatera utara.

Adapun tahapan digital forensik yang dilakukan oleh kepolisian daerah sumatera utara dapat diketahui sebagai berikut :

a. Pengambilan (*acquisition*)

Tahapan pertama ini bertujuan untuk mengambil dan mengamankan alat bukti elektronik asli (*original*). Pada tahap ini, pengambilan dan pengamanan alat bukti elektronik asli (*original*) dilakukan terhadap alat/perangkat yang telah diperoleh sebelumnya pada saat penggeledahan dan penyitaan. Baik itu handphone, komputer, laptop maupun alat komunikasi lain yang digunakan oleh pelaku untuk melakukan tindak pidana *cybercrime*.

b. Pemeriksaan dan analisa

Alat bukti elektronik asli (*original*) yang telah diambil dan diamankan tersebut selanjutnya akan dilakukan penelitian oleh ahli digital forensik yang telah bersertifikasi melalui alat khusus yang ada di laboratorium digital forensik polda sumut. Dimana seluruh alat bukti asli (*original*) yang telah diperoleh tersebut akan dilakukan proses *clauining/copy* untuk dipisahkan dengan yang asli atau originalnya. Hal ini dilakukan karena alat bukti elektronik tersebut sangat mudah terhapus. Hasil dari *clauining/copy* tersebut selanjutnya akan dilakukan pemeriksaan dan dianalisa untuk menemukan informasi yang berhubungan dengan tindak pidana informasi dan transaksi elektronik.

c. Dokumentasi dan presentasi

Pada tahap ini, seluruh alat bukti yang telah diambil dan diamankan serta telah dilakukan pemeriksaan dan analisa akan dilakukan proses dokumentasi. Dimana seluruh berkas perkara akan dilakukan proses pengumpulan dan dibuat berita acara dan mengadakan pelaporan mengenai proses dan tahapan yang dilakukan dalam proses pemeriksaan dan analisa, termasuk alat dan perangkat yang digunakan.⁵⁰

Alat bukti yang telah diperoleh tersebut, setelah dilakukan pengeledahan dan penyitaan, serta dilakukan pemeriksaan melalui proses digital forensik di laboratorium forensik Kepolisian Daerah Sumatera Utara, selanjutnya pihak penyidik akan meminta keterangan ahli. Pihak penyidik akan meminta Keterangan ahli tentang alat bukti elektronik yang telah diperoleh sebelumnya apakah

⁵⁰ Hasil Wawancara Dengan Bapak Kompol Jumanto. Kanit 3 Subdit II. Ditreskrimsus Polda Sumut. Pada Hari Rabu, 01 Maret 2017.

memiliki keterkaitan dengan tindak pidana informasi dan elektronik yang telah terjadi. Setelah memperoleh keterangan ahli, penyidik juga akan meminta keterangan dari saksi yang melihat, mendengar ataupun mengalami langsung peristiwa yang diduga sebagai tindak pidana informasi dan transaksi elektronik tersebut.⁵¹

Ketika penyidik telah selesai melakukan penyidikan, penyidik wajib segera menyerahkan berkas perkara tersebut kepada Penuntut Umum. Hasil dari digital forensik tersebut yang selanjutnya akan dilimpahkan penyidik kepada Kejaksaan untuk dibawa ke Pengadilan. Apabila pada saat penyidik menyerahkan hasil penyidikan, dalam waktu 14 hari penuntut umum tidak mengembalikan berkas tersebut, maka penyidikan dianggap selesai.

B. Kendala Yang Dihadapi oleh Kepolisian dalam mengumpulkan alat bukti tindak pidana Informasi Dan Transaksi Elektronik

Pada perkara *cyber crime* atau tindak pidana Informasi dan Transaksi Elektronik, alat bukti yang sah dan dapat diungkapkan dalam proses pembuktian ditentukan berdasarkan Pasal 5 Ayat (1) dan (2) UU ITE, yang menegaskan bahwa informasi dan atau dokumen elektronik dapat dianggap sebagai alat bukti yang sah secara hukum dalam proses pembuktian, khususnya pada perkara *cybercrime*. Alat-alat bukti tersebut merupakan perluasan dari alat-alat bukti sebagaimana diatur dan berlaku dalam hukum acara, khususnya hukum acara pidana, yakni sesuai ketentuan Pasal 184 KUHAP. Melihat ketentuan di atas, pada

⁵¹ Hasil Wawancara Dengan Bapak Kompol Jumanto. Kani 3 Subdit II. Ditreskrimsus Polda Sumut. Pada Hari Rabu, 01 Maret 2017.

perkara *cybercrime* ini alat bukti yang digunakan adalah alat bukti yang dihasilkan dan mengandung unsur teknologi informasi.⁵²

Informasi dan atau dokumen elektronik dapat dianggap sebagai alat bukti elektronik sebagaimana ditentukan sebagai perluasan alat bukti pada hukum acara pidana yang berlaku berdasarkan Pasal 5 Ayat (2) UU ITE tentang Informasi dan Transaksi Elektronik, juga terhadap alat-alat bukti tersebut dapat dilakukan penafsiran secara ekstensif/diperluas, sehingga informasi dan atau dokumen elektronik termaksud kekuatan hukum yang sama dengan alat bukti pada perkara pidana biasa sebagaimana diatur dalam Pasal 184 KUHAP.

Berdasarkan analisis di atas, maka alat-alat bukti yang ditentukan dalam Pasal 184 KUHAP dapat diterapkan pada perkara *cybercrime* melalui berbagai instrumen elektronik seperti informasi elektronik dan atau dokumen elektronik. Alat-alat bukti termaksud merupakan alat bukti yang sah secara hukum dan dapat digunakan pada proses pembuktian dalam perkara-perkara *cyber crime*, sesuai ketentuan Pasal 5 Ayat (1) dan (2) UU ITE, sehingga tidak terjadi kekosongan hukum serta diharapkan dapat mencapai kepastian hukum dan rasa keadilan.

Pembuktian alat bukti elektronik dalam perkara pidana sering ditemui kendala ketika memasukkan alat bukti elektronik ke dalam ketentuan alat bukti KUHAP dan cara untuk mengakui data elektronik sebagai alat bukti yang sah di dalam pengadilan. Namun kendala yang sangat nyata di alami oleh aparat penegak hukum, mulai dari penyidik, jaksa dan hakim adalah sumber daya manusia yang masih kurang tentang elektronik, sehingga di Indonesia masih jarang kita

⁵² www.jurnal.unsyiah.ac.id/MIH/article/download/4564/3937. Di Akses Pada Hari Selasa, 11 April 2017. Pukul 23.45 WIB.

dapatkan polisi *cyber*, jaksa *cyber* dan hakim, yang seharusnya para aparat hukum *cyber* ini harus merata diseluruh wilayah hukum indonesia untuk memutuskan kasus *cyber* yang adil dan sah. Kendala lain yang dialami aparat penegak hukum adalah belum memadainya fasilitas pelengkap untuk memudahkan alat elektronik dijadikan barang bukti dalam persidangan.

Pembuktian dalam hukum pidana merupakan sesuatu yang sangat vital perannya, mengingat dalam KUHAP (Kitab Undang-Undang Acara Pidana) peran suatu bukti sangat berpengaruh kepada pertimbangan hakim. Setiap kendala yang muncul membuat penegak hukum menjadi bingung untuk menyimpulkan suatu perkara dalam bidang Teknologi Informasi, yang mana bentuk barang bukti berbentuk digital.

Secara umum, kendala yang dihadapi oleh aparat penegak hukum dalam menerapkan alat bukti tindak pidana Informasi dan Transaksi Elektronik

1. Kelemahan lain ada pada perangkat digital forensik (lab komputer forensik Mabes POLRI) yang belum dimiliki secara menyeluruh oleh POLRI di setiap daerah, mengingat penting keberadaannya dalam mencegah, maupun menangani kasus-kasus yang berkaitan dalam Cyber Crime
2. Kejahatan dunia maya ini sering melibatkan antar negara (transnasional) dan tidak mengenal batas wilayah (*borderless*), dan diluar yuridiksi hukum Indonesia, dalam hal ini Polisi atau interpol kesulitan dalam melakukan penindakan dan pemeriksaan terhadap pelaku/operator yang sangat cerdas dalam menjalankan setiap modus kejahatannya.

3. Masih kurangnya sumber daya manusia dalam hal pengetahuannya tentang teknologi digital, kode-kode digital ditingkat POLRI, jaksa, hakim, sehingga dalam menangani tindak pidana dunia maya mengalami hambatan dalam pembuktian.
4. Masih lemahnya peraturan Undang-undang yang mengatur tindak pidana dunia maya, dan faktor ini yang dapat dimanfaatkan oleh para pelaku tindak pidana dunia maya untuk mencari celah-celah hukum agar lolos dari jerat hukum.⁵³

Adapun kendala yang dihadapi oleh penyidik di Kepolisian Sumatera Utara dalam menerapkan alat bukti tindak pidana Informasi dan Transaksi Elektronik adalah :

- a. Kendala Internal, yaitu Kurang memadainya peralatan di SUBDIT II/ Unit *CYBER CRIME*
- b. Kendala Eksternal, yaitu :
 - 1) Alat bukti yang terdapat dalam komputer mudah terhapus dan hilang sehingga sulit untuk dilakukan *clauining*

Hal ini menjadi salah satu kendala yang dialami oleh pihak kepolisian dalam mengumpulkan alat bukti tindak pidana informasi dan transaksi elektronik disebabkan karena Dokumen yang telah dihapus oleh pemilik akun tidak bisa di munculkan kembali kecuali pemilik akun itu sendiri.
 - 2) Pelaku menggunakan identitas palsu

⁵³<http://e-journal.uajy.ac.id/5962/2/HK110266.pdf>. Di Akses Pada Hari Selasa, 11 April 2017. Pukul 23.45 WIB

Kendala lain yang dialami oleh pihak kepolisian dalam mengumpulkan alat bukti dalam tindak pidana informasi dan transaksi elektronik yaitu mayoritas pelaku menggunakan identitas palsu. Dimana, sebelum melakukan tindak pidana informasi dan transaksi elektronik, pelaku akan membuat akun dengan menggunakan identitas palsu. Hal ini menyebabkan pihak kepolisian mengalami kesulitan dalam melacak dan mengetahui dimana keberadaan pelaku berada.⁵⁴

C. Upaya Yang Dilakukan Oleh Kepolisian Untuk Mengatasi Kendala Yang Dihadapi Dalam Menerapkan Alat Bukti Tindak Pidana Informasi Dan Transaksi Elektronik

Penyalahgunaan teknologi informasi menjadi salah satu agenda dari kejahatan di tingkat global. Kejahatan di tingkat global ini menjadi ujian berat bagi masing-masing negara untuk memeranginya. Alat yang digunakan oleh negara untuk memeranginya adalah Hukum. Hukum difungsikan, salah satunya untuk mencegah terjadinya dan menyebarnya *cybercrime*, serta menindak jika *cybercrime* terbukti telah menyerang atau merugikan masyarakat dan negara.⁵⁵

Negara hukum menentukan alat-alat perlengkapannya yang bertindak menurut dan terikat kepada peraturan-peraturan yang ditentukan terlebih dahulu oleh alat-alat perlengkapan yang dikuasakan untuk mengadakan peraturan-peraturan itu. Tindakan yang dilakukan aparat inilah yang dikategorikan sebagai implementasi hukum.

⁵⁴ Hasil Wawancara Dengan Bapak Kopol Jumento. Kani 3 Subdit II. Ditreskrimsus Polda Sumut. Pada Hari Rabu, 01 Maret 2017.

⁵⁵ Abdul Wahid Dan Mohammad Labib. 2005. *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama., halaman 142.

Alat negara itu yang bertanggung jawab untuk menggunakan hukum sebagai senjata guna melawan berbagai bentuk kejahatan yang akan, sedang atau telah mengancam bangsa Indonesia. Alat negara (penegak hukum) dituntut bekerja keras seiring dengan perkembangan *cybercrime* yang semakin mengkhawatirkan. Alat negara ini menjadi subjek utama yang berperan melawan *cybercrime*.⁵⁶

Alat bukti elektronik memiliki karakter yang unik, yaitu bentuknya yang elektronik, dapat digandakan dengan mudah, dan sifatnya yang mudah untuk dirubah. Atas dasar itu penanganannya pun harus hati-hati, karena penanganan yang tidak hati-hati menyebabkan bukti elektronik tersebut menyebabkan bukti itu menjadi benalu sendiri bagi aparat penegak hukum. Artinya malah membuat pelaku menjadi tidak terbukti karena kesalahan prosedur dalam penanganan.

Penanganan dan penyitaan alat bukti elektronik pada intinya adalah bagaimana bukti elektronik itu dapat dihadirkan ke muka persidangan secara autentik dan dapat direpresentasikan atau tidak rusak. Namun hal itu akan sulit terwujud apabila terjadinya kendala-kendala dalam penerapan alat bukti itu sendiri. Oleh karena itu, kendala-kendala tersebut harus segera diatasi sedini mungkin, sehingga penerapan alat bukti dapat berjalan dengan efektif dan efisien.

Adapun upaya yang dilakukan oleh Kepolisian Daerah Sumatera Utara, dalam mengatasi kendala-kendala sebagaimana yang telah dijelaskan sebelumnya adalah :

1. Upaya untuk mengatasi kendala Internal

⁵⁶*Ibid.*,

Melakukan usulan kepada pemerintah melalui Kepala Kepolisian Republik Indonesia untuk melakukan penambahan peralatan di SUBDIT II/ Unit *CYBER CRIME* sehingga proses penerapan alat bukti dalam tindak pidana informasi dan transaksi Elektronik di Kepolisian Daerah Sumatera Utara dapat berjalan lebih efektif dan efisien.

2. Upaya untuk mengatasi kendala Eksternal

Melakukan kerja sama dengan *provider* atau kementerian komunikasi dan informatika republik indonesia (KOMINFO) karena dua instansi tersebut mempunyai alat yang lebih lengkap sehingga mudah untuk melakukan pengungkapan terhadap kasus tindak pidana *cyber crime*.⁵⁷

⁵⁷ Hasil Wawancara Dengan Bapak Kopol Jumanto. Kanit 3 Subdit II. Ditreskrimsus Polda Sumut. Pada Hari Rabu, 01 Maret 2017.

BAB IV

KESIMPULAN DAN SARAN

A. Kesimpulan

1. Proses penerapan alat bukti tindak pidana ITE di Kepolisian Daerah Sumatera Utara diawali dengan proses penyelidikan dan penyidikan. Dimana, pada tahap penyidikan pihak kepolisian akan melakukan penggeledahan dan penyitaan terhadap alat bukti elektronik. Kemudian alat bukti elektronik tersebut akan dilakukan pemeriksaan melalui proses tahapan digital forensik, yaitu :

- a. Pengambilan (*acquisition*)
- b. Pemeriksaan dan analisa
- c. Dokumentasi dan presentasi

Alat bukti yang telah diperoleh tersebut, setelah dilakukan penggeledahan dan penyitaan, serta dilakukan pemeriksaan melalui proses digital forensik di laboratorium forensik Kepolisian Daerah Sumatera Utara, selanjutnya pihak penyidik akan meminta keterangan ahli. Pihak penyidik akan meminta Keterangan ahli tentang alat bukti elektronik yang telah diperoleh sebelumnya apakah memiliki keterkaitan dengan tindak pidana informasi dan elektronik yang telah terjadi. Setelah memperoleh keterangan ahli, penyidik juga akan meminta keterangan dari saksi yang melihat, mendengar ataupun mengalami langsung peristiwa yang diduga sebagai tindak pidana informasi dan transaksi elektronik tersebut.

2. Kendala yang dihadapi oleh penyidik di Kepolisian Sumatera Utara dalam menerapkan alat bukti tindak pidana Informasi dan Transaksi Elektronik adalah:
 - a. Kendala Internal, yaitu Kurang memadainya peralatan di SUBDIT II/ Unit *CYBER CRIME*
 - b. Kendala Eksternal, yaitu :
 - 1) Alat bukti yang terdapat dalam komputer mudah terhapus dan hilang sehingga sulit untuk dilakukan *clauining*
 - 2) Pelaku menggunakan identitas palsu.
3. Upaya yang dilakukan oleh Kepolisian Daerah Sumatera Utara, dalam mengatasi kendala-kendala tersebut adalah :
 - a. Upaya untuk mengatasi kendala Internal

Melakukan usulan kepada pemerintah melalui Kepala Kepolisian Republik Indonesia untuk melakukan penambahan peralatan di SUBDIT II/ Unit *CYBER CRIME* sehingga proses penerapan alat bukti dalam tindak pidana Informasi dan Transaksi Elektronik di Kepolisian Daerah Sumatera Utara dapat berjalan lebih efektif dan efisien.
 - b. Upaya untuk mengatasi kendala Eksternal

melakukan kerja sama dengan *proveder* atau kementerian komunikasi dan informatika republik indonesia (KOMINFO) karena dua instansi tersebut mempunyai alat yang lebih lengkap sehingga mudah untuk melakukan pengungkapan terhadap kasus tindak pidana cyber crime.

B. Saran

1. Diharapkan Kepada Kepolisian Daerah Sumatera Utara dapat mengoptimalkan kinerja dalam penerapan alat bukti tindak pidana Informasi dan Transaksi Elektronik, tentunya harus sesuai dengan prosedur yang telah ditetapkan, karena berdasarkan alat bukti tersebut sangat menentukan terbitnya suatu putusan berkeadilan, asal saja alat bukti tersebut relevan dengan pokok perkara yang disidangkan.
2. Kepolisian Daerah Sumatera Utara diharapkan harus segera mengatasi segala kendala yang timbul dalam penerapan alat bukti dalam tindak pidana Informasi Dan Transaksi Elektronik. Sehingga, penerapan alat bukti dalam tindak pidana Informasi Dan Transaksi Elektronik dapat berjalan dengan efektif dan efisien.
3. Perlu ditingkatkan kinerja kepolisian dalam menerapkan alat bukti tindak pidana ITE dengan melakukan penambahan peralatan di SUBDIT II/ Unit *CYBER CRIME* serta Perlu menjaga keharmonisan antara instansi yang terkait dengan kasus *Cybercrime* khususnya dalam kasus tindak pidana Informasi dan Transaksi Elektronik sehingga dapat mempermudah kinerja polisi dalam menerapkan alat bukti tindak pidana Informasi Dan Transaksi Elektronik.

DAFTAR PUSTAKA

A. Buku

- Abdul Wahid Dan Mohammad Labib. 2005. *Kejahatan Mayantara (Cyber Crime)*. Bandung:Refika Aditama
- Andi Sofyan & Abdul Asis. 2014. *Hukum Acara Pidana Suatu Pengantar*. Jakarta: Prenadamedia Group
- Budi Suhariyanto. 2013. *Tindak Pidana Teknologi Informasi (cybercrime):Urgensi Pengaturan dan Celah Hukumnya*. Jakarta:Rajawali Pers
- Dikdik M. Aries Mansur Dan Elisatris. 2005. *Cyber Law. Aspek Hukum Teknologi Informasi*. Bandung:Refika Aditama
- Eddy O.S Hiariej. 2012. *Teori dan Hukum Pembuktian*. Jakarta: Penerbit Erlangga
- Fakultas Hukum UMSU. 2014. *Pedoman Penulisan Skripsi*. Medan: Fakultas Hukum Universitas Muhammadiyah Sumatera Utara
- Hendar Soetarna. 2011. *Hukum Pembuktian dalam Acara Pidana*. Bandung: Alumni
- Josua Sitompul. 2012. *CyberSpace, CyberCrimes, CyberLaws*. Jakarta:Tatanusa
- Maskun. 2013. *Kejahatan Siber , Cyber Crime*. Jakarta: Kencana
- Petrus Reinhard Golose. 2008. *Seputar kejahatan Hacking. Teori Dan Studi Kasus*. Jakarta:Yayasan Pengembangan Kajian Ilmu Kepolisian

B. Perundang-Undangan

- Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana,
- Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

C. Internet

<http://repository.usu.ac.id/bitstream/handle/123456789/36008/10E00138.pdf?sequence=1>.

<http://digilib.unila.ac.id/8153/6/5.%20Bab%20II%20ok.pdf>.

<http://mkhiabanifakhri.ilearning.me/2013/12/16/definisi-dan-jenis-jenis-kejahatan-internet>.

<http://repository.usu.ac.id/bitstream/handle/123456789/37052/Chapter%20II.pdf?sequence=4>

http://eprints.ums.ac.id/30305/7/NASKAH_PUBLIKASI.pdf.

www.jurnal.unsyiah.ac.id/MIH/article/download/4564/3937