BAB III

INFORMASI LOWONGAN KERJA YANG MENYESATKAN PADA INTERNET

A. Para Pihak yang Terkait dalam Informasi Lowongan Kerja yang Menyesatkan

Kemajuan teknologi telah merubah pandangan dan sikap manusia dalam melakukan kegiatannya yang selama ini di dominasi dengan kegiatan yang bersifat fisik. Lahirnya internet mengubah jarak dan waktu menjadi tidak terbatas, setiap orang dapat berkomunikasi dengan orang lain yang berjarak ribuan kilometer dari tempat ia berada hanya dengan menggunakan fasilitas komputer yaitu internet.

Kecanggihan teknologi komputer telah memberikan kemudahan-kemudahan, terutama dalam membantu pekerjaan manusia. Perkembangan teknologi komputer menyebabkan munculnya jenis kejahatan-kejahatan baru, yaitu dengan memanfaatkan komputer sebagai modus operandi. Penyalahgunaan komputer dalam perkembangannya menimbulkan permasalahan yang sangat rumit, diantaranya proses pembuktian atas suatu tindak pidana (faktor yuridis). Terlebih lagi penggunaan komputer untuk tindak pidana ini memiliki karakter tersendiri atau berbeda dengan tindak pidana yang dilakukan tanpa menggunakan komputer. Perbuatan atau tindakan, pelaku, alat bukti dalam tindak pidana biasa dapat dengan mudah di identifikasi namun tidak demikian halnya untuk kejahatan yang dilakukan dengan menggunakan komputer[26].

[26] Ahmad M Ramli, *Cyber Law Dan Haki Dalam Sistem Hukum Indonesia*, Refika Aditama, Bandung, 2006, Hlm 19.

Komputer dapat mempermudah suatu bentuk kejahatan yang konvensional seperti penipuan atau perbuatan curang tanpa harus bertatap muka langsung dengan korban yaitu dengan cara melakukan sabotase *situs* atau *web* melalui jaringan internet yang dipermudah dengan adanya *sofware*. Penipuan atau perbuatan curang tersebut dilakukan dengan cara-cara baru sehingga tidak mudah untuk dilakukan penyelidikan ataupun penyidikan seperti dalam tindak pidana biasa karena di dalam dunia maya (*cyberspace*) sulit untuk diketahui secara pasti, siapa yang melakukan atau bagaimana tindak pidana itu dilakukan. Kendala-kendala tersebut tidak menyebabkan pelaku tindak pidana itu lolos begitu saja dari jeratan hukum dikarenakan perkembangan terjadi bukan hanya dalam kejahatan namun perkembangan terjadi juga pada majunya penegak hukum dengan membentuk *cyber police* sebagai reformasi hukum dalam tugasnya untuk penindak para pelaku kejahatan *cyber*.

Banyaknya penyedia internet dan semakin terjangkaunya biaya akses internet membuat semakin banyak orang mulai mengenal internet dan menggunakannya. Hal tersebut membuat para penipu melakukan aksi *scam* dengan memanfaatkan kesadaran masyarakat yang masih kurang mengerti akan dampak negatif dari internet serta ketidaksempurnaan kebijakan-kebijakan pemerintah dalam hal tersebut. *Scam* adalah berita elektronik dalam Internet yang membohongi dan bersifat menipu, sehingga pengirimnya akan mendapat manfaat dan keuntungan tertentu. Contoh *scam* yang sering di jumpai adalah surat berantai, pengumuman lotere, dan lain lain. Akibat *scam* ini bagi penerimanya akan lebih serius, jika dibandingkan dengan *spam*. Secara etomologis *scam* dalam bahasa Inggris dapat diartikan sebagai *confidence trick or confidence game* (cara untuk di percaya atau permainan

kepercayaan), sehingga pada awalnya penerima berita merasa yakin dan tidak mencurigai bahwa hal ini merupakan bentuk penipuan[27].

Aksi *scam* ini marak terjadi dan jumlah penipuan bermodus *scam* selama bulan Maret 2009 melonjak 68% dari bulan sebelumnya. Berdasarkan hasil peninjauan oleh badan Milis IT-Center, tercatat ada lebih dari 12.567 *e-mail* baru dan unik serta 2.560 *situs* palsu yang digunakan sebagai sarana *scam* [28]. Serangan *scam* pertama yang tercatat adalah pada *Kaskus* dan Iklan lotre pada 2 September 1996, namun Istilah *scam* telah populer sebelum kejadian itu melalui majalah *Carding* 2007[29].

1. Kasus Informasi Lowongan Kerja yang Menyesatkan

Teknik umum yang sering digunakan oleh para penipu adalah penggunaan alamat *e-mail* dan *situs web* palsu untuk menyesatkan pengguna internet sehingga pengguna internet terpancing menerima keabsahan *e-mail* atau *web sites*. Pelaku juga seringkali memanfaatkan logo atau merk dagang milik lembaga resmi, seperti nama perusahaan atau *web* yang populer, hal itu dimaksudkan agar tampak meyakinkan tidak seperti penipu. Pemalsuan ini dilakukan untuk memancing korban untuk menginvestasikan uangnya kepada pelaku dan kemudian pelaku membuat *situs* palsu yang sama persis dengan *situs* resmi, atau pelaku *scam* mengirimkan *e-mail* yang berisikan *link* ke situs palsu tersebut, dan terakhir membuat *hyperlink* ke *web-site* palsu atau menyediakan *form* isian yang ditempelkan pada *e-mail* yang dikirim[30].

---

[27] Rachmansyah, *Kejahatan Scam*, http: //blogspot.com// Rachmansyah// *Scam*, Diakses Pada Tanggal 13 Mei 2010, Pukul 21:55 WIB

[28] Priadi, *Changing The World One Person At a Time,* http: //blogspot.com// priadi//*About Scam*, Diakses Pada Tanggal 06 April 2010, Pukul 15:55 WIB

[29] Rachmansyah, *Loc Cit*

[30] *Ibid*.

Target *scam* adalah kecerobohan dan ketidaktelitian para pengguna jasa *situs-situs* iklan dan jejaring sosial, *online shopping* dan sejenisnya yang melibatkan transaksi secara *on-line* melalui situs internet. *Scam* dapat dilakukan secara aktif maupun pasif. *Scamer* mengirimkan ribuan *email* atau iklan (*spotlight*) ke target sasaran dengan menipu sebagai *e-mail* resmi suatu perusahaan atau instansi resmi. *E-mail* tersebut terlihat seperti dikirim dari pihak resmi, sehingga pelanggan target seringkali tidak menyadari kalau target sedang ditipu.

Pada *e-mail* atau iklan tersebut *scamer* mencantumkan beberapa tawaran yang mungkin menggiurkan bagi para pengguna internet (*netter*). Berikut adalah contoh *e-mail scam* yang menggunakan nama perusahaan[31] :

RECEPTIONIST

Requirements :

Age 20 year old above
Min. Education SMU/SMK
Good Personality
Good Communication Skill
High Motivation

Basic Salary Rp. 1.500.000,- above

Qualified and interested applicants send resume, Cv and latest photograph to :

hrd_run14@yahoo.com

(Gambar 1)

Scamer mengaku pihak resmi perusahaan terpercaya, sehingga *scamer* dapat meyakinkan korbannya sampai 10% dari penerima *e-mail* untuk mengikuti perintahnya. Hal ini dikarenakan tipuan *scamer* sulit

[31] Priadi, *Op Cit*.

dibandingkan, oleh pengguna internet yang kebanyakan hasilnya mirip dengan aslinya dan apabila akan dibuktikan keabsahanya maka akan memakan waktu dan juga pengeluaran yang banyak.

Berdasarkan gambar di atas dapat dijelaskan sebagai berikut :

a. Dikirim dari *email* yang mengandung kata hrd atau *recruitment* dengan domain yahoo.com.
b. Tidak mencantumkan alamat atau nomor telepon.
c. Selalu mencantumkan besaran gaji, dan angkanya biasanya bulat, misalnya 2 juta atau 3 juta.
d. Dikirim dari alamat IP 202.72.209.226.
e. Dari profil akun Yahoo yang bersangkutan diketahui bahwa hampir semua akun Yahoo tersebut terakhir dimodifikasi (atau dibuat) pada tanggal 19 Maret 2006.

Kasus *scam* menimpa masyarakat pencari kerja sejak bulan April 2006 lalu, *netter* menerima *e-mail* dari PT. Maxgain (www.maxgain.co.id) dalam perekrutan karyawan baru. Modus serangannya terlihat dari isi surat elektronik tersebut yang mengharuskan penerima atau pelamar meng*klik link* alamat tertentu. Berikut dapat di lihat isi surat elektronik yang tercantum di kolom gambar nomor 1 yang dikirim oleh *scamer*[32].

Pelaku *scam* dapat memanfaatkan data pribadi penerima atau pelamar dengan melakukan pengisian menu login di situs *hrd_run14@yahoo.com* palsu tersebut. Pada kenyataannya para pelamar tidak mendapat gaji tetap dan terkesan perusahaan tersebut bukan ingin mencari karyawan, tetapi mencari koneksi ke orang-orang yang memiliki

[32] *Ibid.*

banyak uang untuk di investasikan. Bahkan ada beberapa pelamar yang kehilangan uang setelah melamar pekerjaan ke perusahaan tersebut.

Alamat *situs* palsu berakhiran *yahoo.com* tersebut menunjukkan bahwa pelaku kejahatan memiliki *web server* di *yahoo*. Hal tersebut bisa menjadi pelaku juga melibatkan orang-orang dari dalam perusahaan, karena surat elektronik tersebut ditulis dalam format yang cukup tersusun rapi, setidak-tidaknya pelaku *scam* itu melibatkan orang dalam.

Pelaku *Scam* mengambil daftar alamat *situs* perusahaan ternama PT Maxgain dari hasil *surfing* melalui *goggle*. Sasarannya dilakukan secara acak dari *netter* yang bergabung dalam komunitas *mailing list* dimulai sejak Januari 2007. Media *mailing list* tersebut bukan merupakan *maillist* internal perusahaan resmi, melainkan *mailing list* eksternal yang dikuti para *netter*, hampir dari kebanyakan *situs* atau *web* yang mengiklankan informasi lowongan kerja berasal dari Disnakertrans yang berperan sebagai penyebar luas informasi kerja yang bekerja sama dengan perusahaan terkait dalam pempublikasian informasi tersebut dengan melalui sarana publik seperti majalah, koran, iklan dan sekarang dengan media elektronik yaitu internet yang di pakai pihak Dinas Tenaga Kerja dan Transmigrasi (Disnakertrans) dalam rangka mengikuti perkembangan zaman / *era globalisasi* [33].

Pelaku *Scam* mempergunakan fasilitas yang diberikan pemerintah dalam mengembangkan teknologi informasi tersebut dengan tujuan lain yang menimbulkan rusaknya lalulintas mayatara (*cyberspace*) demi terwujudnya suatu pencapaian tujuan antara lain keuntungan pelaku

[33] Hasil wawancara dengan Asep Ujang Sugiarmanto, *Hasil Tinjauan Aksi Scam Pada Salah Satu Perusahaan Ternama*, Bagian Multimedia, BAPESITELDA, Bandung, Pada Hari Selasa 16 Februari 2010, Pukul 13.45. WIB

dengan merugikan orang lain disampinya yang membuat, menyebarkan atau pun menerima informasi tersebut.

Contoh kasus *Scam* di Indonesia lainnya dialami oleh perusahaan PT Maxgain dan pengguna *situs* loker di internet. Pada tahun 2005, ada *situs* loker palsu di internet milik PT. Maxgain yang berlokasi di Gedung Bursa Efek Jakarta di kawasan SCBD kembali beredar yang memberitakan sebagai berikut [34] :

Data Entry Staff

Requirement : - Pria / wanita - Pendidikan min. SMU / Sederajat - Usia 18 tahun keatas - mampu mengoperasikan komputer

Basic salary : 2.000.000

Silahkan kirimkan resume dan aplikasi lengkap anda ke alamat email :
hrd_jobscorp@yahoo.com

Gambar (2)

Di ketahui *email-email* tersebut dikirim melalui IP 202.72.209.226, sedangkan alamat IP DNS *server* dari *www.maxgain.co.id* adalah 202.72.208.9 dan 202.72.208.8. Seluruh IP tersebut dimiliki oleh ISP yang sama. PT. Maxgain sendiri memang beroperasi di Gedung Bursa Efek Jakarta di kawasan SCBD, pelacakan dilakukan oleh pihak *whois* IT – center ternyata diketahui bahwa lokasi IP tersebut seperti berikut :

[34] Priadi, *Op Cit*

```
[whois.apnic.net]
% [whois.apnic.net node-2]
% Whois data copyright terms
http://www.apnic.net/db/dbcopyright.html

inetnum:      202.72.208.8 - 202.72.209.226
netname:      SCBD-NET
descr:        PT MAXGAIN
descr:        ISP
descr:        Sudirman Central Business District
country:      ID
admin-c:      HP95-AP
tech-c:       HP95-AP
remarks:      Send Spam & Abuse report to
abuse@scbd.net.id
mnt-by:       MNT-APJII-ID
mnt-lower:    MAINT-ID-SCBD
mnt-routes:   MAINT-ID-SCBD
status:       ALLOCATED PORTABLE
changed:      hm-changed@apnic.net 20040813
changed:      hrd_jobscorp@yahoo.com 20040813
source:       APNIC

person:       hendro prabowo
nic-hdl:      HP95-AP
e-mail:       hendro@arthatel.co.id
address:      Jl. Jend. Sudirman Kav. 52-53
address:      Jakarta , 12190
phone:        +62-021-5150000
fax-no:       +62-021-5150006
country:      ID
changed:      nikolas@arthatel.co.id 20040419
changed:      hrd_jobscorp@yahoo.com 20040813
mnt-by:       MAINT-ID-SCBD
source:       APNIC
```

Gambar (3)

Banyak cara yang ditempuh oleh para pelaku *scam* untuk menjerat korbannya, antara lain melalui[35]:

a. Faktor Pendekatan Sosial

   Kebanyakan para korban diberi pesan menarik dan dituntun ke dalam jebakan dengan tujuan agar korban mau melakukan beberapa tindak lanjut dari *e-mail* palsu tersebut dan korban memberikan informasi berharga kepada *scamer*.

[35] N.N, *Modus Scamer*, http://buletin.melsa.net.idjan1001scam2, Diakses Pada Tanggal 11 Maret 2010, Pukul 16:55 WIB

b. Pengiriman Pesan

Bisa melalui *e-mail spam*, *web-based delivery*, iklan jebakan dalam *web*, IRC dan *Instant Messaging* (*Yahoo Messenger*, MSN *Messenger*, AOL, ICQ dan lain-lain), dapat pula calon korban diajak untuk menuju situs buatan para *scamer* yang mengandung trojan, jadi saat korban membuka situs jebakan, secara tidak sadar terjadi proses infeksi sistem oleh trojan.

Berikut ini adalah *nama-nama perusahaan* dari kasus *scam* yang telah terjadi dan berhasil dikumpulkan oleh *puspomagic* Desember 20, 2008 [36] :

a. PT Abdi Karya Manunggal
b. Pharos Indomedica
c. PT. Sankyo Foods Manufacturing Indonesia
d. Multicorellab Coorporations
e. PT. Karya Buana Sejatera
f. PT. Multi Digital System
g. M.Managment Agency
h. HRD_Wilkins_BM
i. Polo Group
j. PT. Antikaraya Niaganusa Indonesia
k. Torishima Manufacture
l. PT. Abdi Cipta Indonesia
m. Era Guna Property
n. PT. Mas Jaya Pertiwi

[36] Puspomagic, *Nama Perusahaan Penipu*, http:// buletin.melsa.net// idjan1001loker5, Diakses Pada Tanggal 14 Maret 2010, Pukul 10:35 WIB

o. PT. Permata Citra Buana
p. PT.Garamond Omega Steel
q. PT. Cipta Rasa Manunggal
r. PT. Prima Citra Entertainment
s. PT. Estetika Arta Mandiri
t. PT. Bangun Cipta Kontraktor
u. PT Megah Kirana Pratama
v. PT. Permata Citra Buana
w. PT. Yamaji Otsuka Pharmacy
x. PT. Maxgain
y. PT. Ega Group
z. PT. Harjaya Group
aa. Nomura Internusa
bb. PT. Graha Finesa Berjangka (GFB)
cc. PT. Appco Dirrect
dd. PT. Granton Advertising
ee. PT. Solid Gold Berjangka
ff. PT. Trijaya Pratama
gg. PT. Inter Pan Pasifik
hh. PT. Tripar Multivision
ii. PT. MJ Network
jj. Mandiri Group di Plaza Benhill
kk. PT Kasaba di Arthaloka Plaza
ll. Mahetza Group di Wisma Bumiputera LT. 18
mm. Mitra Utama Global Ged.IDX
nn. PT Galaxindo Mandiri Mitra Utama (PT GMMU) Group (PT. Galaxindo/Gatrama/Mandiri Utama/Gama)

oo. PT. Cipta Sarana di Pondok Kelapa Jakarta Timur.

pp. PT Gama Tex/ Gatma Textilindo

qq. PT GMPK Karya/Petnostara Gasindo Atau PT GMP Karya Group/ PT Gama Pima Karya

rr. PT Gatmal Hotel

ss. PT Bahtera Okta Mandiri

tt. PT Harjaya Group

uu. Batavia Futures

vv. Harum Dana Berjangka

ww. Valbury Futures

xx. Fortune Channel

yy. Maxco Futures

zz. Dea U Trade

aaa. PT. Ekspresindo Global Artha JL. Gatsu Gedung Patrajasa LT. 1 Kav. 32-34

bbb. PT Platinum Berjangka

ccc. PT Ekspresindo Global Artha

ddd. Nisma Exis Jaya di ruko Mutiara Pondok Cabe

eee. PT Nomura Internusa Prisma

fff. PT Galaxindo Mandiri Mitra Utama (GMMU/ GATRAMA), Catatan: Nama PT ini dapat berganti menjadi PT. Galaxindo / Gatrama / Mandiri Utama Group / Gama / Galaxi Indo Group, DLL

ggg. PT Mam (Mahetza)

hhh. PT Kasaba Indonesia Group (PT. Karunia Surya Abadi)

iii. PT Gama Tex / Gatma Textilindo

jjj. PT GMPK Karya /Petnostara Gasindo Atau PT GMP Karya Group / PT Gama Prima Karya

kkk. PT Gatma Hotel

lll. PT Harjaya Group

mmm. PT. Mitra Utama Global

nnn. PT. Maxgain

ooo. PT. Mix Internasional

ppp. PT. MIF

qqq. PT. MGI

rrr. PT. MXI

sss. PT. BPF

ttt. PT. GFB

uuu. PT. MIF

vvv. PT. DIB

Hasil laporan milis IT-Center, nama-nama dari 74 perusahaan 50% disalahgunakan (dibajak) pelaku *scamer*, sisanya adalah penyedia jasa internet sebanyak 10%, jasa perbankkan 20%, institusi kenegaraan 10%, dan sektor ritel 10%[37].

2. Para Pihak dalam Informasi Lowongan Kerja yang Menyesatkan

Pihak-pihak yang terkait dalam tindak pidana penipuan dalam penyesatan informasi (*scam*) melalui pengiriman *e-mal* atau iklan yaitu :

a. *Scamer* adalah pelaku dari *scam*. *Scamer* menggunakan *e-mail*, *banner* atau *popup window* untuk menipu *user* ke suatu

[37] N.N. *Statistik Cybercrime*, http:// www. pentasi. netarticle, Diakses Pada Tanggal 11 Juni 2009, Pukul 09:20 WIB

situs *web* palsu, dimana *user* diminta untuk memberikan informasi pribadinya[38].

b. *Netter* adalah pengguna internet dalam hal ini adalah penerima *e-mail* yang dikirimkan oleh para *scamer*.
c. *Cracker* adalah sebutan untuk orang yang mencari kelemahan system dan memasukinya untuk kepentingan pribadi dan mencari keuntungan dari system yang di masuki seperti: pencurian data, penghapusan, penipuan, dan banyak yang lainnya[39].
d. Perusahaan adalah badan hukum yang dimiliki perseorangan ataupun persekutuan dalam menyediakan sebuah pekerjaan bagi masyarakat dalam pemenuhan kebutuhan ekonomi.
e. Dinas Tenaga Kerja dan Transmigrasi (Disnakertrans) adalah bandan hukum pemerintah yang bertindak sebagai pengatur dan penghubung antara pemerintah dan perusahaan dalam merumuskan juga melaksanakan kebijakan dan standarisasi teknis di bidang pembinaan, pelatihan kerja dan penempatan tenaga kerja serta sebagai penyedia sarana informasi kerja dari perusahaan terkait kepada masyarakat[40].

---

[38] *Ibid*.

[39] Fleah Lit, *Hacking No Comments*, Http//www.Trilogi.com//*hecker and Cracker*//, Di Akses Pada Tanggal 11 Februari 2009, Pukul 10.30 WIB

[40] Disnakertrans, *Peran Disnakertran*, Http//www.Disnakertran.go.id//, DiAkses Pada Tanggal 23 Mei 2010, Pukul 14.30 WIB.

B. Akibat yang Timbul dari Informasi Lowongan Kerja yang Menyesatkan pada Internet.

Kejahatan dengan menggunakan teknologi komputer termasuk penipuan dengan modus *scam* telah menyebabkan kerugian yang cukup besar bagi beberapa pihak diantaranya yaitu :

a. Bagi Manyarakat pada umum dan pencari kerja pada khususnya.
    1) Kejahatan komputer yang tidak terdeteksi oleh korban.
    2) Kesulitan masyarakat dalam melaporkannya kejahatan ini kepada pihak yang berwenang dikarenakan proses yang cukup memakan waktu lama dan banyak biaya.
b. Bagi Perusahaan.
    1) Rusaknya citra perusahaan di masyarakat
    2) Turunya kepercayaan masyarakat dan perusahaan lain terhadap perusahaan terkait.
c. Bagi Negara.
    1) Pengaruh negatif dari perkembangan pembangunan negara.
    2) Kerugian finansial

Tindak pidana penipuan menimbulkan kerugian secara materil maupun immateril, dalam hal ini masyarakat khusunya pencari kerja mengalami kerugian oleh tindakan *scam* yang membuat informasi palsu seperti *informasi lowongan kerja* untuk keuntungan pelaku, akibat *scam* juga menimbulkan kerugian bagi negara karena dengan adanya kejahatan tersebut dapat menurunkan citra dan nama baik bangsa indonesia sebagai salah satu negara terbesar yang melakukan kejahatan *cybercrime*.

Faktor-faktor penyebab laju perkembangan *cyber crime* cenderung mengalami peningkatan dari tahun ke tahun yaitu[41] :

a. Kesadaran Hukum Masyarakat

   Kesadaran hukum masyarakat sampai saat ini dalam menanggapi aktivitas *cyber crime* masih dirasakan kurang. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan masyarakat terhadap jenis kejahatan *cyber crime*. Kurangnya pemahaman dan pengetahuan ini menyebabkan upaya penanggulangan *cyber crime* mengalami kendala, dalam hal ini kendala yang berkenaan dengan penataan hukum dan proses pengawasan masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan *cyber crime.*

b. Faktor Keamanan

   Rasa aman akan dirasakan oleh pelaku kejahatan pada saat sedang menjalankan aksinya. Hal ini karena internet umumnya digunakan di tempat-tempat yang relatif tertutup. Akibatnya pada saat pelaku sedang malakukan kejahatan sangat jarang orang mengetahuinya. Di samping itu, apabila pelaku telah melakukan kejahatan maka dengan mudah pelaku dapat menghapus semua jejak kejahatan yang telah dilakukan. Pada saat pelaku tertangkap sulit bagi aparat penegak hukum untuk menemukan bukti-bukti kejahatan.

c. Faktor Penegak Hukum

   Faktor penegak hukum sering menjadi penyebab maraknya kejahatan *cyber*. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk-beluk teknologi informasi,

[41] Dikdik M Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, 2005, Hlm 89-95

sehingga pada saat pelaku tindak pidana ditangkap, aparat penegak hukum kesulitan untuk menemukan alat bukti yang dapat dipakai menjerat pelaku terlebih apabila kejahatan yang dilakukan memiliki sistem pengoperasian yang sangat rumit.

Penyalahgunaan komputer dan media internet sebagai salah satu dampak dari perkembangan tersebut tidak terlepas dari sifatnya yang khas sehingga membawa persoalan baru yang agak rumit untuk dipecahkan, berkenaan dengan masalah penanggulangannya maka kepolisian mengupayakan sebuah reformasi dengan membentuk *cyber police* dengan yaitu polisi yang dilatih dan dididik untuk melakukan penyidikan dan penyelidikan dalam bidang *cyber crime*[42].

Sistem pembuktian di era teknologi informasi saat ini menghadapi tantangan besar yang memerlukan penanganan serius, khususnya dalam kaitannya dengan upaya pemberantasan *cyber crime*. Hal ini muncul karena bagi sebagian pihak jenis-jenis alat bukti yang selama ini dipakai untuk menjerat pelaku tindak pidana tidak mampu lagi dipergunakan untuk menjerat pelaku kejahatan di dunia maya.

Alat bukti *cyber crime* biasanya berupa komputer, laptop atau alat elektronik lain yang dapat digunakan sebagai alat untuk melakukan kejahatan *cyber*. Alat bukti dalam kejahatan *cyber* khususnya *scam* ini menjadi suatu kendala lain, karena saat kasus diserahkan pada jaksa, biasanya jaksa mengatakan bahwa alat bukti tidak dapat digunakan karena dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP) tidak diatur mengenai alat bukti elektronik. Usaha Pemerintah dalam menanggulangi penyalahgunaan perkembangan teknologi dalam bidang *cyber* dengan membentuk polisi *cyber*

[42] Arief Wibowo, *Strategi Jangka Mnengah Dalam Penaggulangan Dampak*, Etika profesi dan Budi pekerti, Universitas Budi Luhur, Fakultas Teknologi Informasi, Bandung, 2010, Hlm 33

yang berbasis telematika dalam menanggapi alat bukti yang digunakan pelaku kejahatan teknologi informasi yaitu pembuktian surat elektronik, pelacakan alamat IP, keterangan ahli oleh pakar telematika dan keterangan para korban yang berupa pengaduan dijadikan bukti otentik suatu kejahatan dalam bidang *cyber* selain informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya, keterangan saksi (korban) dan surat dari hasil keterangan para ahli merupakan alat bukti hukum yang sah[43].

Adanya Kejahatan di dunia maya menyebabkan pihak kepolisian sebagai pihak yang melakukan penyelidikan dan penyidikan tentang ada atau tidaknya tindak pidana tersebut, dituntut untuk mengetahui lebih jauh bagaimana penanganan yang akan dilakukan apabila terjadi tindak pidana tersebut.

[43] Hasil wawancara melalui dunia maya, Mansyur Ridwan, *Alat Bukti Cyber*, Yahoo Messenger-Bandung-04, garut, Diakses Pada Tanggal 15 Mei 2010, Pukul 13.00 s/d 14.15 WIB.