MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

TINJAUAN TERHADAP KEMAMPUAN PENYIDIK POLRI DALAM MENYIDIK HAKING KOMPUTER SERTA AKTUALISASI PENEGAKAN HUKUMNYA

KERTAS KARYA PERORANGAN

(TASKAP)

Diajukan untuk memenuhi persyaratan Kurikuler Sekolah Staf dan Pimpinan Polri
Tahun Pelajaran 2000/2001, sesuai dengan Surat Keputusan Kepala
Sekolah Staf dan Pimpinan Polri No.Pol.: Skep/78/XI/2000
Tanggal 10 Nopember 2000

OLEH :

Drs. E. BRATA MANDALA
KOMISARIS POLISI NRP.62050798

PERWIRA SISWA SEKOLAH STAF DAN PIMPINAN POLRI
DIKREG KE – 36 / WIRA WIDYA ARYAGUNA
T.P. 2000 / 2001

Diperiksa dan disahkan oleh Panitian Ujian Taskap
Pasis Sespim Polri Dikreg ke-36/Wira Widya Aryyaguna
Tahun Pendidikan 2000 / 2001
Pada tanggal, 30 April 2001

KETUA

Drs. DRADJAT DWIYONO
KOMBES.POL. NRP.48010131

ANGGOTA

Drs. JACKY MANIHIN
KOMBES.POL. NRP.48120213

ANGGOTA

Drs. BAHRUDIN ISMAIL
KOMBES.POL. NRP.51010132

ANGGOTA / SEKRETARIS

Drs. BADRUN ARIFFIN
AKBP. NRP.53120170

ABSTRAK

Kemajuan masyarakat dan perkembangan bidang internet yang berkembang sangat pesat di Indonesia ternyata cukup besar manfaatnya dibidang komunikasi dan perkembangan ilmu pengetahuan serta ***kecepatan akses / transaksi*** di bidang perbankan, akan tetapi ***residunya berupa Haking komputer*** sangat merugikan terhadap individu, kelompok bahkan negara. Fenomena ini belum dikenal oleh para penyidik Polri , Haking komputer sangat asing bagi mereka sehingga sangat diragukan kemampuannya untuk menyidik kasus ini apabila terjadi. Untuk mampu menyidik kasus haking komputer, mereka harus mempunyai kemampuan sebagai programer komputer yang mengerti cara-cara mengoperasionalkan komputer, mengerti sistem internet (prosedur dan penggunaannya), mampu mengerti dan mengurai program-program jahat komputer (virus, worm, kuda troyan dan bom logika), serta mengerti seluk beluk para haker antara lain modus operandi dan kebudayaan mereka. Selain itu agar penyidikannya tuntas dan layak diajukan ke Jaksa penuntut umum merekapun harus didukung oleh saksi ahli yang mempunyai kemampuan mengaudit EDP dan perangkat komputer forensik.

Ternyata terdapat kesenjangan antara kemampuan penyidik dengan tantangan yang harus dihadapi (haking komputer), kemampuan-kemampuan seperti yang diuraikan di atas belum dimiliki serta belum ada bidang forensik komputer di laboratorium-laboratorium forensik Polri ditambah lagi yuridis formal yang belum memadai. Akibatnya penyidikan tidak bisa optimal, sehingga penegakan hukum terhadap hal tersebut aktualisasinya belum seperti yang diharapkan. Lazimnya ***secara hipotetis*** terhadap hal tersebut adalah ; " Apabila pengetahuan mereka cukup baik atau memadai , maka kemampuan untuk mengungkapnya akan cukup baik. Demikian pula apabila sebaliknya" .

Modus operandi haking komputer berkembang terus demikian juga upaya-upaya pengamanan terhadap sistem informasi dan komunikasi yang menggunakan komputer, namun para haker tetap mampu mengantisipasinya sehingga sistem-sistem tersebut tetap dapat ditembus. Hal ini terjadi karena para haker selalu mengaktualisasikan dirinya sehingga kasus-kasus yang merugikan publik / masyarakat akibat hal ini akan senantiasa terus terjadi, dan Polri akan dituntut untuk mampu mengantisipasinya bila ada anggota masyarakat yang mengeluh dan melaporkan atau atas inisiatif Polisi sendiri.

Secara umum hasil yang diharapkan dari penulisan ini adalah : untuk memberikan gambaran yang ***tepat dan detail*** mengenai Haking komputer dan perkembanganya,

serta dapat ***memberikan gambaran (membuktikan)*** bahwa " Para penyidik Polri *sangat minim* pengetahuan dan penguasaannya dibidang Haking komputer". Akibatnya kemampuan mereka dalam penyidikan Haking komputer sangat minim , sehingga *korelasi* terhadap aktualisasi penegakan hukum di bidang ini jauh dari yang diharapkan.

Sifat penelitian / penulisan ini deskriptif *tidak dimaksudkan* untuk langsung menemukan solusinya atau Problem solving (agar tidak meloncat / terjebak pada bidang pemecahan masalah). Diharapkan *ditindak lanjuti* oleh penulis / peneliti yang lain untuk mencari pemecahan masalahnya , sehingga solusinya *tepat dan mengandung kebenaran ilmiah* karena merupakan penelitian lanjutan yang berdasarkan dari penelitian sebelumnya (problematik dan simtom-simtomnya telah terdeskripsi).

KATA – PENGANTAR

Dengan memanjatkan Puji Syukur kehadirat Tuhan Yang Maha Esa, penulis akhirnya dapat menyelesaikan Taskap ini sesuai dengan jadwal waktu yang ditetapkan oleh Lembaga dalam memenuhi persyaratan kurikuler pada Pendidikan Sekolah Staf dan Pimpinan Polri Tahun Pelajaran 2000/2001.

Adapun Judul Penulisan Kertas Karya perorangan ini adalah : **"TINJAUAN TERHADAP KEMAMPUAN PENYIDIK POLRI DALAM MENYIDIK HAKING KOMPUTER SERTA AKTUALISASI PENEGAKAN HUKUMNYA."**

Selanjutnya dengan penuh rasa hormat, Penulis sampaikan terima kasih yang tak terhingga kepada :

1. Kepala Sekolah Staf dan Pimpinan Polri beserta seluruh Pejabat teras, para Pembina, Patun dan segenap keluarga besar Sespim Polri yang telah membimbing dan membina kami selama menjalankan pendidikan di Sespim Polri.

2. Komisaris Besar Polisi Drs. Bambang Sulardi Syam selaku Pembimbing Materi yang telah meluangkan waktunya untuk memberikan bimbingan, arahan dan petunjuk yang berharga sehingga penulisan Taskap ini dapat berjalan dengan baik dan lancar.

3. Prof. Dr. H. Dedi Supriadi, M.Pd. Direktur Pasca Sarjana Universitas Pendidikan Indonesia (Dosen Sespim Polri) , yang telah meluangkan waktunya memberikan konsultasi tentang penulisan karya ilmiah kepada penulis.

4. Prof. Dr. Ir. Anang Z Gani Staf Ahli Lembaga Afiliasi dan Penelitian Industri / LAPI – ITB (Dosen Sespim Polri), yang telah mengijinkan menggunakan perpustakaan pribadinya serta memberikan konsultasi tentang penulisan karya ilmiah kepada penulis.

5. AKBP Drs. Arif Darmawan Kepala Bagian Reserse Umum Polda Jawa Tengah, yang telah meluangkan waktunya untuk wawancara dengan penulis.

6. AKBP Drs. Desman Sinaga Kasubdit Fiskal Moneter dan Devisa Direktorat Tipiter Korps Reserse Mabes Polri, yang telah meluangkan waktunya untuk wawancara dengan penulis.

7. Orang Tua serta Keluarga tercinta (Heny, Cheaka, Dea dan Baby) yang senantiasa memberikan dorongan semangat dan do'a restu sehingga dalam penulisan Taskap ini dapat berjalan dengan lancar sesuai harapan penulis.

Akhirnya penulis menyadari sepenuhnya bahwa Taskap ini masih jauh dari sempurna untuk dikatakan sebagai Taskap yang berbobot dan bermutu, hal ini disebabkan oleh keterbatasan kemampuan, pengetahuan dan pengalaman penulis. Dan harapan penulis semoga segala bantuan yang telah diberikan kepada Penulis, mendapatkan balasan dari Tuhan yang Maha Kuasa. Amin.

Lembang, April 2001.

PENULIS.

The truth is out there pointed to it self !
Search and seek it by all cost ...

DAFTAR ISI

HALAMAN.

DAFTAR GAMBAR

Halaman

DAFTAR GRAFIK / TABEL

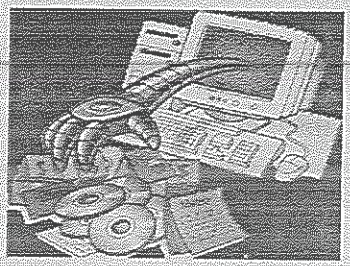
Halaman

DAFTAR KOTAK DIALOG

Halaman

MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

Bab. I



MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

TINJAUAN TERHADAP KEMAMPUAN PENYIDIK POLRI DALAM MENYIDIK HAKING KOMPUTER SERTA AKTUALISASI PENEGAKAN HUKUMNYA

BAB I

PENDAHULUAN

1. **Latar Belakang.**

a. Pada tahun 1970 Alfin Toffler sudah meramalkan apa yang akan terjadi pada akhir abad ke 20 atau pada awal abad 21, adapun ramalannya adalah sebagai berikut :

> "Suatu revolusi meremukkan lembaga dan hubungan kekuasaan. Justru inilah yang sedang terjadi dewasa ini pada semua bangsa berteknologi maju. Para mahasiswa di Berlin, New York, Turin dan Tokyo, menangkapi para dekan dan rektor mereka, membuat pabrik pendidikan yang berdentang-dentang berhenti dan bahkan mengancam untuk menggulingkan pemerintahan. Polisi berdiri di pinggir, ketika di perkampungan kulit hitam di New York, Washington dan Chicago, undang-undang hak milik yang kuno sedang terang-terangan dilanggar, Kaidah seksual ditumbangkan. Banyak kota besar dilumpuhkan oleh pemogokan, listrik mati, huru-hara. Banyak aliansi kekuatan internasional digoyahkan. Pemimpin keuangan dan politik gemetar dalam hati – bukan cemas karena kaum revolusioner komunis (atau kapitalis) akan menyingkirkan mereka, melainkan cemas karena seluruh sistem sedang melesat tak terkendalikan".[1]

Ramalan tersebut ternyata benar karena berbagai peristiwa telah terjadi, seperti yang diramalkannya. Gelombang informasi yang berbasis pada teknologi informasi canggih, serta alat transportasi modern telah menciutkan dunia menjadi kecil dan melahirkan apa yang disebut globalisasi. Akibatnya apa yang diramalkan terjadi juga di Indonesia yang puncaknya pada tahun 1998 pada saat jatuhnya rezim Suharto. Bukti-bukti dari hal tersebut adalah :

---

1 Toffler Alvin . *Kejutan Masa Depan.* Pantja Simpati, Jakarta , 1992. Hal 169.

1) Mahasiswa bersama unsur lapisan masyarakat lainnya melakukan gerakan moral secara intens dan massal merobohkan pemerintahan rezim Suharto .

2) Hukum sudah tidak diindahkan lagi, penjarahan dimana-mana, kerusuhan masal yang menimbulkan anarki , main hakim sendiri sampai tega membunuh atau membakar orang yang disangka sebagai pencuri / perampok tanpa proses pengadilan.

3) Para elit politik dan Birokrat pemerintahan saling bertikai, tidak tahu arah harus kemana (disorientasi), karena stabilitas keamanan dan ekonomi tidak pernah terwujud dan mereka sangat gemetar karena sewaktu-waktu akan tersingkir.

b. Dalam situasi tersebut Polisi tidak mampu berbuat banyak, benar-benar jadi pecundang sebagaimana yang dikatakan Ka Sespim Polri Irjen Polisi Drs, Chaerudin Ismail. Ini adalah fakta dan memang benar demikian, problema utamanya adalah kenapa hal ini bisa terjadi ? Kenapa jadi pecundang ? jawabannya antara lain demikian :

1) Ramalan dari Alvin Toffler, tanda-tanda atau peringatan yang dikirim tidak terbaca oleh para elit Polri / pemimpin Polri pada 30 tahun atau 20 tahun lalu, tidak terbaca karena terjebak pada Repelita (periode 5 tahun) Polri hanya mampu untuk berfikir 5 tahun kedepan saja.

2) Tanda-tanda akan terjadi kejatuhan ekonomi Indonesia telah terlihat ±15 tahun lalu, demikian juga dengan kejahatan intensitas tinggi sudah diperingatkan akan terjadi, seperti terorisme, ancaman/peledakan Bom, kejahatan ekonomi dan kejahatan komputer. Namun tidak ada upaya atau tindakan nyata yang siginifikan, hal-hal tersebut waktu itu hanya dijadikan wacana atau bahan-bahan diskusi para perwira Polri.

3) Mungkin yang terakhir ini sebagai jawaban yang paling tepat ; selama 30 tahun Polisi seperti katak dalam tempurung (tempurungnya adalah ABRI), tidak mampu mengembangkan profesionalismenya, sering dijegal bila ingin maju atau terlihat sudah maju di depan.

c. Akibat dari ketidak mampuan membaca kedepan dan berada dalam tempurung selama ± 30 tahun, Polri saat ini sedang mengalami future shock (kejutan masa depan). Polri dikejutkan dengan demonstrasi yang massive dan radikal, dikejutkan oleh kerusuhan-kerusuhan masa akibat konflik horizontal dan vertikal, bom meledak, terorisme juga kejahatan-kejahatan berdimensi baru yang menggunakan teknologi tinggi dibidang ekonomi (credit card fraud, e' commerce by computer crime / hacking). Dikatakan oleh Drs. Kunarto ciri-ciri kejahatan tersebut adalah sebagai berikut :

> "a. Kejahatan yang belum dikenal, belum pernah terjadi dan baru sekali ini terjadi. Berarti tidak tercakup dalam KUHP bahkan mungkin belum tertuang dalam Undang-Undang yang ada di Indonesia.
> b. Kejahatan konvensional yang dalam melaksanakannya memerlukan peralatan dengan menggunakan teknologi baru.
> c. Kejahatan yang dilakukan dengan memanfaatkan celah-celah hukum yang ada. Dengan kata lain, perbuatan kejahatan yang tidak terjangkau oleh hukum".2

Mengapa dikatakan future shock ? karena hal-hal tersebut masih dalam tahap diperbincangkan belum ada persiapan untuk antisipasinya, tiba-tiba terjadi dimuka atau didepan Polri saat itu juga. Pasti akan tergagap-gagap dan sangat diragukan untuk mampu mengantisipasinya dengan baik karena sumber daya manusia (SDM), anggaran dan sarana / prasarananya belum siap.

d. Future shock juga terjadi dan melanda dalam kehidupan masyarakat Indonesia sehari-hari (tidak bagi Polri saja), antara lain teknologi handphone dari segi fungsi

---

2. Sabadan Daan Drs .dan Drs. Kunarto. ***Kejahatan Berdimensi Baru***. *Cipta Manunggal*, Jakarta, 1999. Hal. vii.

sebetulnya untuk hal-hal emergency tetapi digunakan untuk bicara tanpa arah dan terjadi pemborosan pulsa, dari segi penguasaan teknologi sangat minim sehingga dalam suatu rapat tiba-tiba berdering dan menimbulkan kemarahan orang lain. Demikian juga dengan penggunaan internet , pada dasarnya digunakan untuk meningkatkan dan mengutamakan komunikasi serta memperlebar jaringan bisnis, sebagai wahana ilmiah untuk mencari referensi ke berbagai perpustakaan di seluruh dunia. Namun orang Indonesia mentalnya belum siap dengan teknologi baru ini, mereka banyak menggunakannya hanya untuk *chating* saja atau untuk berbicara tanpa arah, saling membalas mengirim virus, *berjam-jam* eksplorasi di *situs (web site) porno*, berjudi sehingga terjadi lagi pemborosan pulsa telepon, dana dan kerusakan moral.

Untuk masa yang akan datang Polri , harus belajar dari pengalaman pada saat ini yang sangat penting bagi Polri adalah menangani disintegrasi bangsa, legitimasi penegak hukum yang rendah, teror / bom dan kerusuhan masa akibat demonstrasi radikal ataupun akibat konflik horizontal. ***Namun*** kejahatan-kejahatan yang bernuansa teknologi tinggi (*hitech*), dan berdimensi baru yang sekarang sudah terjadi di Indonesia ***juga harus segera diantisipasi*** supaya dimasa yang akan datang tidak terkejut lagi (sudah siap).

e. Kejahatan komputer yang basis atau dasarnya adalah Haking komputer merupakan kejahatan yang perlu ditangani dengan serius, dan dalam mengantisipasi hal ini perlu rencana / persiapan yang baik sebelumnya. Karena kejahatan ini *potensial* menimbulkan kerugian dibidang ekonomi yang signifikan, bencana masal yang cukup mengerikan dan lebih memprihatinkan dibanding dengan ledakan bom di Bursa efek Jakarta, bahkan dimasa depan bisa melumpuhkan seluruh jaringan infra struktur yang berbasis teknologi elektronik (ATM / perbangkan, telepon, komunikasi satelit, jaringan listrik, lalu lintas penerbangan dsb).

Haking komputer di Indonesia, telah banyak menimbulkan korban akibat dari ulah Haker yang jahat (bad hacker) yaitu Kraker (cracker), Preker (phreaker), bahkan korbannya tidak tanggung-tanggung ***Polri sendiri***, pada tanggal 16 Nopember 1999 situs milik Polri diganggu gambarnya dirubah dan terpampang ***wanita telanjang***. Banyak korban lainnya terutama situs-situs komersial (e'commerce) ; seperti matahari departemen store, juga korban perorangan atau individu yang dirugikan sampai jutaan rupiah belum lagi yang dipermalukan secara umum tanpa bisa mengadakan perlawanan, serta rusaknya moral para remaja karena menjamurnya situs-situs porno (Contoh ; http://www.thehun.com).

Hanya tinggal menunggu waktu saja publik akan menuntut Polri mampu mengatasi hal tersebut diatas, tentunya mereka akan mencaci maki Polri ***bila tidak mampu*** dengan mengatakan tidak profesional dan sangat lamban bereaksi. Polri harus segera bereaksi tidak bisa menunggu lagi karena pada hakekatnya yang dihadapi Polri *tidak semata-mata* fenomena haking komputer, tetapi lebih dari itu seperti yang dikatakan Alvin Toffler :

> "Kita sedang menciptakan masyarakat yang baru. Bukan suatu masyarakat yang berubah. Bukan pula perluasan, versi yang lebih besar dari masyarakat kita yang sekarang ini. Tetapi suatu masyarakat yang baru. Premis sederhana ini belum mewarnai kesadaran kita. Akan tetapi jika kita tidak memahaminya, kita akan menghancurkan diri sendiri ketika mencoba menanggulangi hari esok".3

Jadi Polri sekarang sedang menghadapi masyarakat yang baru dan dunia yang baru, jangan lagi berpikir kebelakang atau *menganggap* situasi masih sama dengan hari-hari sebelumnya.

f. Agar Polri dapat mengantisipasi haking komputer perlu dilakukan penanganan secara serius dan terencana, karena kejahatan ini sangat intens, jangkauannya sangat

---

3. Ibid. Hal. 169.

luas serta pelaku-pelakunya rata-rata mempunyai intelektual yang tinggi dan mempunyai komunitas tersendiri juga terus mengembangkan dirinya agar lebih baik (hebat) dalam melakukan aksinya. Para haker seolah-olah mempunyai negara / kerajaan tersendiri yang unik (hacker dome), mempunyai bahasa tersendiri dan sekolah-sekolah privat yang gratis untuk mengembangkan diri agar menjadi haker sejati, selain itu mereka ada yang menganggap perbuatannya sebagai seni (bukan hal yang ilegal) untuk mencari tahu dan menunjukkan kehebatannya agar dihormati para haker lain, dan yang paling penting adalah siapa saja yang berminat dapat menjadi haker asalkan menguasai program-programnya yang cukup canggih tersebut.

Penyidik Polri harus menguasai seluk beluk diatas termasuk program-programnya untuk dapat menyidiknya, namun disatu sisi kemampuan sumber daya manusia (SDM) Polri dan sarana / prasarana Polri belum memadai untuk mampu mengantisipasi secara optimal, ditambah lagi dengan aspek *Yuridis* yang tidak sempurna (belum ada). Sehingga akan lebih menyulitkan bagi Polri dalam penyelidikannya. Agar dapat merencanakan pengembangan SDM secara cermat, *perlu diteliti* sejauh mana kemampuan dan pengetahuan para penyidik Polri dalam menangani haking komputer dan perlu diketahui sejauh mana perkembangan dan modus-modus dari kejahatan ini. Diharapkan bila hal tersebut sudah *diketahui secara pasti*, maka langkah - langkah antisipatif yang dilakukan *akan tepat* mengacu pada hasil temuan tersebut, mudah-mudahan tulisan ini dapat menyumbangkan data / informasi bagi Polri dalam upaya mengantisipasi haking komputer yang sudah secara luas terjadi di Indonesia.

2. **D a s a r.**

1) Surat Keputusan Kepala Kepolisian Republik Indonesia No.Pol. Skep/47 /VIII

/2000 tanggal 8 Agustrus 2000 tentang Penyelenggaraan Pendidikan Sekolah Staf dan Pimpinan Polri Dikreg ke –36 T.P. 2000/2001.

2) Surat Keputusan Kepala Sekolah Staf dan Pimpinan Polri No.Pol. Skep/78/XI/ 2000 tanggal 10 Nopember 2000 tentang Penetapan Judul serta Penunjukan Pembimbing Materi/Teknis Kertas Karya Perorangan Perwira Sespim Polri Dikreg ke-36 T.P. 2000/2001.

3. **Maksud dan Tujuan.**

a. Maksud.

Penulisan Kertas Karya perorangan (Taskap) ini dimaksudkan untuk memberikan gambaran mengenai fenomena haking komputer dan kemampuan para penyidik Polri dalam mengantisipasinya, serta aktualisasi penegakan hukumnya. Sekaligus untuk memenuhi salah satu persyaratan kurikulum dalam menyelesaikan pendidikan di Sespim Polri Dikreg ke-36 / Wira Widya Aryaguna T.P. 2000/2001.

b. Tujuan.

Penulisan Taskap ini adalah bertujuan untuk memberikan sumbangan pemikiran bagi Lembaga Sespim Polri dan Polri tentang fenomena haking komputer dan kemampuan para penyidik Polri dalam mengantisipasinya, serta aktualisasi penegakan hukumnya.

4. **Permasalahan dan Persoalan.**

a. Permasalahan.

Bagaimana *secara tepat mendeskripsikan* fenomena atau masalah Haking komputer (perkembangan, modus-modusnya dan motivasi para Haker), serta *sejauh*

mana pengetahuan para penyidik Polri terhadap fenomena tersebut yang korelasinya positif terhadap kemampuan mereka dalam penyidikan kasus tersebut.

b. Persoalan – persoalan.

1) Sejauh mana Haking komputer berkembang di Indonesia dan seberapa jauh aktivitasnya serta kerugian yang ditimbulkannya ?.

2) Pengetahuan serta keterampilan seperti apa *(konsepsi ideal)* agar mampu melakukan *penyidikan/penegakan hukum* terhadap Haking komputer, juga *sebagai tolok ukur* untuk mengetahui sejauh mana kemampuan para penyidik Polri ?.

3) Sejauh mana *kondisi aktual* pengetahuan dan pemahaman para penyidik Polri dalam bidang komputer dan Haking komputer, dan sejauhmana kemampuan mereka dalam menyidik Haking komputer ?.

4) Sejauh mana kemampuan para penyidik Polri dalam mengaktualisasikan penegakan hukum kasus –kasus Haking komputer ?.

5. **Metoda dan Pendekatan**

a. Metoda :

Metoda *penelitian* yang digunakan adalah Explorasi lapangan dan literatur serta studi komparatif terhadap kasus-kasus aktual Haking komputer / Aspek Yuridisnya. Metoda *pengumpulan data* digunakan wawancara dan dari data sekunder (dokumen), sedangkan untuk *analisa data* digunakan metoda Deskriptif analitis yaitu menggambarkan berdasarkan data yang di dapat kemudian dianalisa untuk mendapatkan kesimpulannya (secara deduktif).

b. Pendekatan :

Dalam penulisan Taskap ini pendekatan yang digunakan adalah *tehnis komputer* untuk menjelaskan masalah haking komputer, tehnis *penyidikan* untuk membahas masalah tingkat kemampuan penyidik. Serta *yuridis* untuk membahas masalah aktualisasi penegakan hukum.

6. **Ruang Lingkup.**

Ruang lingkup penulisan dan pembahasan Taskap ini dibatasi pada *deskripsi fenomena* haking komputer dan *kemampuan para penyidik* dalam mengantisipasi fenomena tersebut, serta *konsepsi metode penyidikan* terhadap haking komputer dan *konsepsi yuridis* yang perlu diadakan.

7. **Tata – Urut :**

Taskap ini terdiri dari *8 Bab*, secara singkat penjelasannya adalah sebagai berikut :

a. Bab I : Pendahuluan

Dikemukakan latar belakang yang mengggambarkan persoalan-persoalan mendasar, sehingga memotivasi untuk ditulisnya Taskap ini, kemudian dasar, maksud dan tujuan, permasalahan dan persoalan, ruang lingkup, metode dan pendekatan, tata – urut serta pengertian-pengertian menjelaskan istilah-istilah atau variabel-variabel yang diteliti.

b. Bab II : Kerangka teori dan perkembangan komputer.

Membahas *2 pokok masalah* yaitu *Kerangka teoritis*, untuk menjelaskan hubungan antara variabel-variabel dalam permasalahan / persoalan yang dibahas, serta bagaimana hubungannya menurut suatu teori tertentu. *Perkembangan komputer secara umum* menjelaskan hal ihwal komputer dan perkembangannya saat ini, serta gambaran

arah dari perkembangan komputer dimasa yang akan datang. *Maksud* pembahasan ini untuk memahami seluk beluk komputer dan permasalahannya, untuk mempermudah memahami Internet dan fenomena kejahatan komputer.

c. Bab III : Perkembangan Internet dan kejahatan komputer.

Membahas *2 pokok masalah* yaitu : *Perkembangan* jaringan komputer / Internet dan kejahatan komputer secara umum, perkembangan Internet meliputi sejarah Internet, cara kerja / fungsi dan aplikasi-aplikasinya. *Kejahatan kompte*r secara umum yang konvensional ataupun yang termasuk dalam cybercrime. *Maksud* pembahasan ini untuk memberikan *pemahaman* tentang haking komputer yang menggunakan Internet sebagai media untuk melakukannya, dan *memahami posisi* haking komputer diantara kejahatan-kejahatan komputer pada umumnya.

d. Bab IV : Haking komputer dan perkembangannya.

Membahas *masalah-masalah* sebagai berikut : *Perkembangan haking* komputer secara umum, menjelaskan apa sebenarnya haking komputer, siapa pelaku-pelakunya dan bagaimana budaya mereka serta apa motivasinya. *Perkembangan modus operandinya* di Indonesia, menjelaskan modus-modus yang dilakukan atau bagaimana biasanya mereka berbuat, apa yang bisa mereka lakukan dimasa yang akan datang. *Dampak* haking komputer terhadap Kamtibmas, menjelaskan seberapa jauh kerugian yang ditimbulkan dan kemungkinan buruk apa yang bisa terjadi, sehingga menimbulkan situasi Kamtibmas terganggu.

Maksud pembahasan ini agar *mendapatkan suatu konsepsi* penyidikan dan penegakan hukumnya terhadap hal tersebut diatas, konsepsi ini *dijadikan standar/ pembanding* untuk mengetahui sejauh mana kemampuan penyidikan dan dukungan komputer forensik serta perangkat hukumnya yang ada sekarang ini.

e. Bab V : Konsepsi ideal kemampuan penyidikan dan dukungan komputer forensik serta perangkat hukumnya.

Membahas *3 pokok masalah* yaitu : *Kemampuan penyidik* kasus Haking komputer, menjelaskan konsepsi-konsepsi ideal mulai dari titik awal penyidikan sampai mengarah pada tersangka, memeriksa tersangka, korban, saksi/saksi ahli dan arah interogasinya serta bagaimana mencari / menangani barang bukti yang diperlukan atau disita. *Komputer forensik* pendukung penyidikan Haking komputer, menjelaskan konsepsi kegiatan pendukung penyidikan forensik komputer dengan standard dari perusahaan jasa forensik komputer ***Vogon*** sebagai pembanding. *Perangkat hukum* khusus untuk bidang komputer, menjelaskan perangkat hukum yang sekarang ada

(ideal) merupakan konsepsi-konsepsi dari para ahli hukum.

Maksud dari konsepsi tersebut merupakan *suatu kondisi yang diharapkan* (ideal) bagaimana kemampuan penyidikan, dukungan komputer forensik dan perangkat hukumnya. Konsepsi ini dijadikan standar (tolok ukur) untuk mengetahui sejauh mana *kondisi aktual* (saat ini) kemampuan para penyidik Polri, dukungan komputer forensik yang ada serta hukum positifnya.

f. Bab VI : Pemahaman / Kemampuan para penyidik Polri menyidik Haking komputer.

Membahas *3 pokok masalah* yaitu : *Penguasaan dasar-dasar operasional komputer*, menjelaskan seberapa jauh para penyidik menguasai / mampu atau trampil mengoperasionalkan komputer pada tingkat dasar sebagai operator. *Pemahaman Haking komputer dan penyidikannya*, menjelaskan apakah para penyidik mengetahui fenomena Haking komputer, modus operandi dan bagaimana cara menyidiknya. *Faktor-faktor determinan* terhadap penguasaan dasar-dasar operasional komputer,

pemahaman Haking komputer dan penyidikannya.

Hal tersebut diatas *merupakan temuan* selama penelitian berlangsung, dengan tolok ukur konsepsi-konsepsi (kondisi yang diharapkan) sebagaimana yang telah diuraikan dalam bab V, mengacu pada standar penyidikan Vogon.

g. Bab VII : Aktualisasi penegakan hukum haking komputer.

Membahas dan *menganalisa* sejauh mana *hubungan* antara kemampuan penyelidikan / penyidikan Haking komputer, perangkat hukum yang ada (hukum positif) *dengan* hasil penegakan hukum terhadap Haking komputer yang merupakan aktualisasi penegakan hukum terhadap Haking komputer atau cybercrime lainnya.

Pada intinya adalah *membandingkan* secara deskriptif konsepsi ideal ketiga pokok masalah pada Bab V diatas, *dengan kenyataan yang ada* sehingga diketahui sejauh mana perbedaannya. *Diharapkan* dari data / fakta tersebut menjadi bahan dalam upaya untuk meningkatkan kemampuan para penyidik Polri (pada penelitian selanjutnya).

h. Bab VIII : Penutup.

Merupakan *konklusi* dari pembahasan-pembahasan dalam Taskap ini yang bersifat *deskriptif* bukan problem solving, dengan saran-saran yang bersifat rekomendasi terbuka. (karena *bukan* berdasarkan pada hasil pembuktian penelitian / riset problem solving , yang biasanya berupa saran tertutup).

8. **Pengertian-pengertian**.

Penjelasan istilah-istilah yang digunakan dalam Taskap ini maksudnya agar ada persamaan persepsi sekaligus membatasi masalah yang dibahas, adapun pengertian-pengertiannya adalah sebagai berikut :

a. Tinjauan.

Merupakan suatu metode ilmiah yang berasal dari kata descriptive, dijelaskan oleh Koentjaraningrat ;

> "Penelitian yang bersifat deskriptif, bertujuan menggambarkan secara tepat sifat-sifat suatu individu, keadaan, gejala atau kelompok tertentu, atau untuk menentukan frekuensi atau penyebaran suatu gejala atau frekuensi adanya hubungan tertentu antara suatu gejala dan gejala lain dalam masyarakat. Dalam hal ini mungkin sudah ada hipotesa, mungkin belum, tergantung dari sedikit banyaknya pengetahuan tentang masalah yang bersangkutan".4

Berdasarkan pengertian tersebut diatas, yang dimaksud tinjauan adalah kegiatan atau upaya menggambarkan objek-objek, gejala-gejala dari variabel-variabel yang diteliti dalam Taskap ini, untuk lebih mengetahui secara mendalam tentang masalah-masalah yang bersangkutan atau dibahas.

b. Penyidikan.

Dalam Undang-Undang tentang Hukum Acara Pidana pada Bab I pasal 1 ayat 2, disebutkan ; "Penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya".5

Yang dimaksud penyidikan dalam Taskap ini adalah proses untuk menuntaskan suatu perkara / kasus pidana mulai dari proses penyelidikan (untuk menentukan ada tidaknya tindak pidana), sampai pada tahap / proses penanganan TKP, penemuan / pengolahan barang bukti dan proses pemeriksaannya di laboratorium , penanganan tersangka/ saksi dari kasus Haking komputer yang terjadi. Sampai dengan ke proses

---

4. Koentjaraningrat. *Metode-metode Penelitian Masyarakat.* Gramedia, Jakarta, 1989. Hal. 29.

5. Nusantara Abdul Hakim G., SH, LLM, dkk. *.Kitab Undang-Undang Hukum Acara Pidana dan Peraturan-Peraturan Pelaksana.* Djambatan, Jakarta 1986. Hal. 5.

proses penerapan pasal-pasal dan pemberkasan perkara, untuk selanjutnya dikirimkan kepada Penuntut umum.

c. Kemampuan penyidik.

Kemampuan dalam Kamus Umum Bahasa Indonesia dijelaskan : " Mampu : 1. Kuasa (sanggup melakukan sesuatu, dapat, kemampuan : Kesanggupan; kecakapan ; kekuatan ; 2. Kemajuan."[6]

Penyidik dalam Undang-Undang tentang Hukum Acara Pidana pada Bab I pasal 1 ayat 1 disebutkan ; "Penyidik adalah pejabat Polisi Negara Republik Indonesia atau pejabat Pegawai Negeri Sipil tertentu yang diberi wewenang khusus oleh Undang-Undang untuk melakukan penyidikan"[7].

Berdasarkan penjelasan tersebut diatas yang dimaksud kemampuan penyidik dalam Taskap ini adalah , tingkat kecakapan untuk menguasai / kesanggupan melakukan penyidikan dari para penyidik Polri khususnya anggota Polri yang bertugas di Satfung Reserse, untuk melakukan penyidikan terhadap kasus Haking komputer dan penyalahgunaan komputer secara umum.

d. Haking Komputer.

Menurut Dr. Charles C. Palmer disebutkan bahwa , "Hacking is unauthorized used of computer and network resoursces"[8] ia adalah seorang manajer keamanan sistem komputer dari Network Security and Cryptography, IBM'S. Tetapi menurut salah seorang Haker yang terkenal dengan sandi : LOA – ASH , " Hacking is the act of

---

6. Poerwadarminta W.J.S. ***Kamus Umum Bahasa Indonesia.*** Balai Pustaka, Jakarta, 1999. Hal. 628.

7. Nusantara Abdul Hakim G. SH, LLM, dkk, Loc. Cit.

8. Palmer. Charles C.Dr. *Q & A with IBM's Charles Palmer* .[Online]. Tersedia http://www. cnn. com /TECH/specials/hackers/qandas/palmer.html . [15 Februari 2000].

penetrating computer system to gain knowledge about the system and how it works"[9]

Pendapat lain dalam majalah NetMag.com (Pakistan) adalah : "Hacking : An art in itself."[10] Dari pernyataan tersebut dapat disimpulkan bahwa : Haking komputer adalah seni bagaimana menembus system komputer untuk mendapatkan pengetahuan dan bagaimana system tersebut bekerja, yang merupakan perbuatan ilegal karena menggunakan komputer dan jaringan kerjanya secara tidak sah (tidak berhak).

Para haker mempunyai pendapat lain bahwa bila melihat-lihat saja mereka berpendapat tidak jahat / legal, tetapi bila merusak system dan mencari keuntungan materi atau mendobrak jaringan telepon supaya menggunakan telepon secara gratis baru disebut ilegal. Mereka ini disebut haker jahat (bad hacker) yaitu Kraker (Cracker) yang merusak system dan mencari keuntungan dan Preker (Phreacker) yang mendobrak dan mencuri pulsa telepon. Lebih jauh mengenai haker, kraker dan preker dengan segala seluk beluknya antara lain modus operandi, para pelakunya akan dijelaskan dalam bab tersendiri.

e. Aktualisasi penegakan hukum.

Aktualisasi berasal dari kata aktual sinonim dengan kata actual dalam bahasa Inggris yang artinya : "hangat; nyata"[11], adapun penegakan hukum menurut Hari Suharto, SH (dikutip R. Abdussalam) adalah " Suatu rangkaian kegiatan dalam rangka usaha pelaksanaan ketentuan-ketentuan yang berlaku baik yang bersifat penindakan maupun pencegahan mencakup keseluruhan kegiatan baik tehnis maupun administratif

---

9. Loa . Ash Revelation. ***The Ultimate Beginner's Guide to Hacking and Phreacking.*** [Online]. Tersedia: http://www.hackers.com /texts/neos/starhak.txt.[23 April 2000].

10. NetMag. ***Hacking : An art in itself.*** [Online]. Tersedia : http://www.netmag.com.pk/new/ hacking.htm. [26 Desember 2000].

11. Wojowasito, S. Prof. Drs. & W.J.S. Poerwadarminta. ***Kamus Lengkap.*** Hasta, Bandung, 1980. Hal. 2.

yang dilaksanakan oleh aparat penegak hukum, sehingga dapat melahirkan suasana aman, damai dan tertib demi untuk pemantapan kepastian hukum dalam masyarakat." [12] Dari uraian tersebut diatas,yang dimaksud dengan aktualisasi penegakan hukum adalah upaya untuk membuat nyata / mewujudkan pelaksanaan ketentuan-ketentuan hukum yang bersifat penindakan ataupun pencegahan, terhadap kasus haking komputer. Atau secara singkat adalah upaya mewujudkan proses penyidikan terhadap haking komputer, sehingga kasus tersebut bisa diajukan ke Penuntut umum.

f. Komputer.

Komputer berasal dari bahasa latin computare yang artinya menghitung (to compute atau reckon), menurut Donald H Sanders (dikutip oleh Jogiyanto Hartono) ;

> "Komputer adalah sistem elektronik untuk memanipulasi data yang cepat dan tepat serta dirancang dan diorganisasikan supaya secara otomatis menerima dan menyimpan data input, memprosesnya dan menghasilkan output dibawah pengawasan suatu langkah -langkah instruksi-instruksi program yang tersimpan di memori (stored program)."[13]

Sedangkan Jogiyanto Hartono sendiri menyimpulkan komputer berdasarkan karakteristik ;

> "... dapat disimpulkan bahwa komputer adalah ;
>
> 1) Alat elektronik.
> 2) Dapat menerima input data.
> 3) Dapat mengolah data.
> 4) Dapat memberikan informasi.
> 5) Menggunakan suatu program yang tersimpan di memori komputer (stored program).
> 6) Dapat menyimpan program dan hasil pengolahan.
> 7) Bekerja secara otomatis."[14]

---

12. Abdussalam, R. Drs, SH, MH. ***Pencegakan Hukum di lapangan oleh Polri.*** Perpustakaan Nasional, Jakarta., 1997. Hal. 18.

13. Hartono Jogiyanto, MBA, Ph.D. ***Pengenalan Komputer.*** Andi, Yogyakarta., 1999. Hal. 1

14. Ibid. Hal. 2.

Secara singkat komputer adalah alat elektronik untuk memproses / mengolah data, yang operasinya berdasarkan pada bahasa dan program tertentu.

g. Penyalah gunaan komputer.

Penyalah gunaan komputer (computer abuse) lebih tepat dibandingkan dengan kejahatan komputer (computer crime), karena sebenarnya *tidak ada* komputer yang jahat, yang terjadi adalah : 1) Komputer *disalah gunakan* oleh para penjahat, dengan menggunakan program-program tertentu yang merusak (program jahat), untuk kepentingan atau mendapatkan keuntungan secara tidak sah. ; 2) Komputer sebagai obyek kejahatan mereka, disini seolah-olah justru komputernya yang jadi korban.

Maksud dalam penyalahgunaan komputer dalam Taskap ini adalah ; penggunaan komputer yang ilegal dengan menggunakan program-program komputer tertentu, atau menyerang komputer tertentu yang dijadikan sasaran / obyek. Lebih populer disebut sebagai kejahatan komputer

h. Internet.

Internet merupakan media atau lahan subur bagi para haker untuk beroperasi atau melakukan haking, walaupun mereka bisa menggunakan media lainnya diluar internet. Adapun pengertian internet menurut Widi Iskandar, adalah "Semua jaringan yang menggunakan protokol IP yang bekerja sama membentuk jaringan yang lebih besar untuk para pemakainya."[15]

Internet protokol (IP) yaitu tata cara/prosedur yang lazim digunakan dalam operasional internet, jadi internet adalah sebuah system jaringan komputer yang saling berhubungan, dan berinteraksi satu dengan lainnya secara paralel dengan menggunakan program-program komputer sebagai fasilitasnya.(akan dijelaskan dalam bab tersendiri).

---

15. Iskandar Widi. ***Pemanfaatan Jaringan Komputer Global Internet untuk Pemerolehan Karya Ilmiah.*** Majalah Sanyata sumanasa wira, Sespim Polri. Lembang, 1997. Hal. 69.

MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

Bab. II

BAB II

KERANGKA TEORI DAN PERKEMBANGAN KOMPUTER

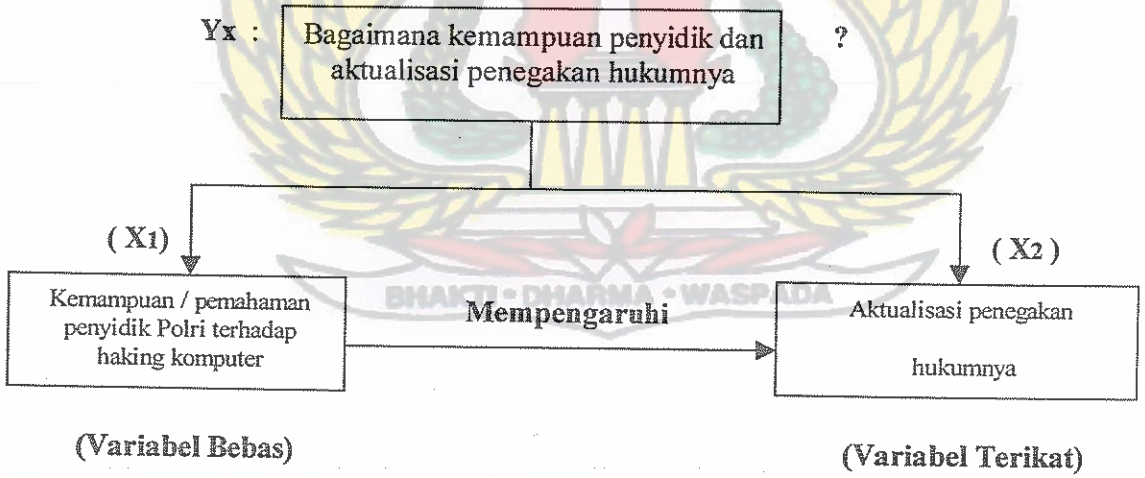
Pada Bab ini akan dibahas kerangka teoritis *sebagai pijakan* untuk mengetahui *hubungan* antara kemampuan penyidik Polri dan korelasinya dalam aktualisasi penegakan hukum kemudian dibahas perkembangan komputer secara umum, karena untuk mengetahui penyalah gunaan komputer / haking komputer harus mengerti dulu seluk beluk komputer secara umum.

9. **Kerangka Teori.**

Dari permasalahan yang terkandung dalam judul tulisan ini serta *pokok-pokok persoalannya* dapat digambarkan bahwa hubungan antara variabel-variabel yang menjadi persoalan adalah sebagai berikut :

Gambar . 1

Hubungan antar variabel



Hubungan dari kedua variabel diatas dijelaskan berdasarkan teori seorang pakar pendidikan Malaysia yaitu Norrizan Razali yang menyatakan sebagai berikut : " Education plays a vital role in determining the right quantity, types and quality of human resources. The higher education system, with one of its primary objectives that is to produce skilled

manpower for the country's human resource, obviously shoulders the bulk of the responsibility."16 Dikatakan bahwa pendidikan memegang peranan penting dan sangat menentukan kwantitas dari jenis-jenis dan kwalitas sumber daya manusia. Sistem pendidikan yang tinggi dengan tujuan utama menciptakan sumber daya manusia yang mempunyai kemampuan yang baik dari suatu negara, sangat nyata merupakan suatu tanggung jawab yang besar untuk dipikul di pundak (diwujudkan).

Dari pernyataan tersebut diketahui bahwa pendidikan memegang peranan penting dan sangat vital dalam merubah kemampuan serta kwalitas sumber daya manusia, karena pendidikan memberikan manusia pengetahuan yang kemudian akan dipahami dan selanjutnya kemampuannya (skill) akan meningkat. Sehingga dapat dikatakan bahwa apabila manusia *dididik dan diberikan* pemahaman-pemahaman serta kemampuannya ditingkatkan, maka *hasil dari pekerjaannya* akan meningkat pula baik secara kwalitas / kwantitas yang pada akhirnya misi / tujuan suatu organisasi akan tercapai pula secara optimal.

Analogi dari hal tersebut diatas bisa dikatakan bahwa, apabila *pengetahuan / pemahaman* para penyidik Polri ditingkatkan, sehingga pemahamannya meningkat terhadap masalah haking komputer, maka *kemampuan* dalam penyidikannya akan meningkat akibatnya penegakan hukum terhadap haking komputer akan optimal. Berdasarkan teori tersebut dapat diidentifikasi bahwa kemampuan / pemahaman penyidik Polri terhadap haking komputer merupakan *variable bebas (X 1)* yang mempengaruhi kwalitas dari aktualisasi penegakan hukum masalah haking komputer *variable terikat* (*X* 2), atau baik tidaknya aktualisasi penegakan hukum terhadap haking komputer tergantung dari baik tidaknya kemampuan / pemahaman penyidik Polri terhadap haking komputer. Relevan

---

16. Razali Norrizan. ***Higher Education Reform Towards Industrialization : A Malaysian File (Re-engineering Education : Perspectives, Priorities and Issues)*** dalam Laporan kedua UNESCO-ACEID International Conference. Asia-Pasific Centre of Educational Innovation (ACEID – UNESCO), Bangkok, 1996. Halaman 89.

dengan hal tersebut diatas maka hipotesis dari tulisan ini, adalah untuk membuktikan *secara deskriptif* bahwa ;

Ho 1 : - Kemampuan / pemahaman penyidik Polri terhadap haking komputer *(X 1)* belum seperti yang diharapkan.

- Sehingga aktualisasi penegakan hukumnya belum optimal *(X 2)*.

10. **Perkembangan komputer secara umum.**

Untuk mengetahui perkembangan komputer adalah dengan mengetahui perkembangan *piranti keras* dan *piranti lunak* (program / bahasa-bahasa) komputer. Adapun perkembangan tersebut adalah sebagai berikut :

a. Perkembangan perangkat keras komputer.

Perangkat keras komputer adalah alat-alat dari suatu unit komputer yang terdiri dari tiga bagian besar yaitu alat untuk memberikan masukan (*input devices*) yang sekarang dikenal dengan *keyboard* atau papan ketik, dalam perkembangannya ditambah dengan *skaner* (untuk pemindai gambar / tulisan), k*amera digital* dan *mikropon* (alat untuk memasukkan suara). Alat untuk memproses data (*process devices*) yang disebut dengan *Central processing unit* atau *CPU* , dan alat untuk mengeluarkan / menampilkan hasil pengolahan (*output devices*) data yang disebut dengan *monitor display* atau layar monitor.

Dalam perkembangannya ditambah dengan *printer* (alat untuk mengetik), *speaker* (alat untuk mengeluarkan suara) dan alat-alat mekanis untuk melakukan gerak tertentu sesuai dengan perintah / program sebelumnya.

Sebelumnya perangkat keras komputer tidaklah demikian namun sangat sederhana, perkembangannya digolongkan kedalam empat golongan menurut Jogiyanto Hartono sebagai berikut :

"1. Alat manual (*manual-device*), mempergunakan alat-alat sederhana, tangan masih memegang peranan penting.
2. Alat mekanik (*mechanical-device*), yaitu alat mekanik yang digerakkan secara manual dengan tangan.
3. Alat mekanik elektronik (*electro mechanical-device*), yaitu alat mekanik yang digerakkan oleh motor elektronik.
4. Alat elektronik (electronic-device), yaitu alat yang bekerjanya secara elektronik."17

Secara umum perkembangan perangkat keras tersebut adalah sebagai berikut :

1) Alat manual.

Alat ini telah digunakan sejak jaman primitip mulai dari menggunakan *tulang belulang* sampai dengan *penggaris geser Oughtred's*, berikut ini penjelasan dari alat-alat tersebut :

a) ***Tulang*** (300000 sm). Digunakan manusia untuk mengingat dan berkomunikasi, seperti halnya menghitung umur, mengukur jarak.

b) ***Petroglyphs*** (30000 – 14000 sm). Pada jaman primitip ini, bangsa Barbara menggunakan batu karang yang digores untuk mencatat data. Kadang-kadang batu karang ini digores membentuk gambar yang menunjukkan suatu kejadian. Batu karang yang digores ini sekarang disebut dengan petroglyphs.

c) ***Lempengan tanah liat*** (9000 – 5000 sm). Lempengan tanah liat digunakan di Timur Tengah sebagai alat perhitungan . Lempengan-lempengan tanah liat ini mempunyai bentuk-bentuk yang berbeda menunjukkan bilangan sepuluh dan enampuluh. Sistem perhitungan ini sekarang digunakan dalam system kita untuk menunjukkan *jam, menit dan detik.*

17, Jogiyanto Hartono, MBA. Ph.D. *Pengenalan Komputer.* ANDI. Yogyakarta, 1999. Hal. 13.

d) ***Abacus*** (2500 sm). Suatu alat untuk menghitung supaya lebih cepat telah dibuat dan disebut abacus. Alat ini dianggap sebagai *alat perhitungan digital yang pertama kali.* Belum jelas sumber asli dari abacus, ada yang memperkirakan berasal dari negara Babylon, ada juga yang memperkirakan dari negara Cina, atau berasal dari negara Mesir.

e) ***Batu terstruktur*** (***Stonehenge*** 900 sm). Stonehenge merupakan batu yang tersturktur di Salisbury Plain sebelah selatan Inggris, digunakan observasi dan peramalan musim dan gerhana.

f) ***Tali bersimpul / Quipus*** (1200 sm). Tali bersimpul yang disebut dengan quipus, digunakan oleh nenek moyang bangsa Peru digunakan untuk mencatat data administrasi, pajak dan perhitungan populasi.

g) ***Napier's Bones (1614).*** John Napier (1550 – 1617) ahli metematika Scotlandia, menciptakan alat yang dibuat dari tulang untuk perhitungan perkalian, yang disebut dengan nama Napier's Bones. John Napier dianggap sebagai *penemu perhitungan logaritma* dan alatnya sebagai dasar dari mistar hitung.

h) ***Oughtred's Slide Rule (1621).*** Ahli matematika Inggris, William Oughtred (1575 – 1660), memperkenalkan alatnya yang disebut dengan nama Oughtred's Slide Rule. Alat ini terdiri dari dua buah mistar terletak pada suatu piringan yang bisa digerakkan satu dengan yang lainnya. Dengan menggeser mistar pada posisi yang tertentu, bisa didapatkan hasil perkalian atau pembagian. Alat ini bekerjanya didasarkan pada prinsip Napier's Bones.

2) Alat mekanik.

Selanjutnya setelah manusia menemukan secara bertahap alat-alat untuk

membantu penghitungan yang dilakukan secara manual, karena kecepatannya yang kurang memadai kemudian dikembangkan alat-alat penghitung secara mekanik yang pada awalnya masih digerakkan oleh tangan, penjelasan alat-alat tersebut adalah sebagai berikut :

a) ***Mesin hitung yang pertama (1623).*** Wilhem Schickard (1392 – 1633) di Jerman, merancang suatu mesin penghitung didasarkan pada Napier's Bones yang dapat melakukan perkalian, pembagian menghitung logaritma dan sebaliknya. Mesin ini baru setengah jadi sudah terbakar dan belum sempat diperbaiki.

b) ***Mesin penghitung otomatis yang pertama (1642).*** Blaise Pascal (1623 – 1662) metematika dan ahli filsafat besar dari Perancis, menciptakan pertama kali alat penghitungan dengan mesin secara mekanik. Alat ini disebut dengan nama Pascal's Machine Arithmatique atau juga dikenal dengan nama The Pascaline. *Tehnik alat ini sekarang masih digunakan pada komputer modern.*

c) ***Mesin pengali yang pertama (1666).*** Sir Samel Mortland (1625 – 1695) menciptakan mesin yang bisa melakukan pertambahan, pengurangan, pengalian dan pembagian tetapi tidak otomatis seperti The Pascaline.

d) ***Leibnitz's calculating machine (1673).*** Gottfried Wilhem von Leibnitz (1646 – 1716), seorang ahli metematika dan filsafat dari Jerman, mengembangkan mesin yang dibuat oleh Pascal.

e) ***Mesin penghitung komersial (1820).*** Charles Thomas de Colmar (1785 – 1870) membuat mesin penghitung arithmatika yang dijual secara komersial dan sukses serta memenangkan medali pada

international Exhibition di London tahun 1862. Sampai 30 tahun kemudian kira-kira 1500 mesin ini telah diproduksi. Prinsip kerja alat ini berdasarkan cara kerja alat Leibnitz Calculating Machine.

f) ***Babbage's analytical engine (1833).*** Charles Babbage mengembangkan Babbage's Difference Engine dengan konsep yang lebih mendalam dan lebih umum. Mesin ini dinamakan Babbage's Analytical Engine, sumbangan Charles Babbage sangat besar untuk komputer jaman sekarang. *Prinsip kerja mesin ini yang merupakan dasar kerja dari komputer sekarang*, termasuk peralatan input kartu plong, memori komputer, alat pencetak, konsep stored program dan sebagainya. Karena mesin ini *Charles Babbage dianggap sebagai bapak komputer modern.*

g) ***Mesin penghitung dengan keyboard yang pertama (1850).*** D.D. Parmaker dari Amerika Serikat membuat mesin hitung dengan menggunakan keyboard.

h) ***Mesin penghitung saintifik yang pertama (1893).*** Otto Steiger (1858 – 1923) dari Zurich, mengembangkan suatu mesin hitung saintifik yang sukses dipasarkan. Antara tahun 1894 sampai tahun 1935 sejumlah 4655 buah mesin tersebut telah terjual dengan nama Millionaire.

3) Alat mekanik elektronik.

Perkembangan selanjutnya dari perangkat keras setelah alat mekanik adalah alat mekanik yang bekerja secara elektronik supaya bekerja lebih otomatis, penjelasan alat-alat tersebut adalah sebagai berikut :

a) ***Mesin tabulasi kartu plong mekanik – elektronik yang pertama (1890).*** Pada tahun 1890, seorang ahli statistik dari Buffalo, New York,

Amerika Serikat, Dr. Herman Hollerith (1860 – 1929), bekerja sama dengan biro sensus Amerika Serikat untuk mempercepat pengolahan data sensus. Tahun 1887, Dr. Herman Holerith telah membuat dan menyelesaikan mesinnya dengan menggunakan kartu plong. Tahun 1986, Dr. Herman Hollerith mendirikan perusahaan dengan nama Tabulating Machine Company. Pada tahun 1924, CEO dari perusahaan ini, yaitu Thomas J. Watson mengganti nama perusahaan menjadi nama yang terkenal sampai sekarang, yaitu IBM (International Business Machine) Corporatrion.

b) ***Komputer Analog yang Pertama (1931). Dr. Vannevar Bush (1890 – 1974)*** di M.I.T. (Massachussetts Institute of Technology) membuat komputer analog pertama untuk memecahkan persoalan persamaan differensial. Mesin ini disebut dengan nama Differential Analyzer.

4) Alat elektronik penuh / komputer.

Perkembangan selanjutnya dari perangkat keras tersebut adalah alat elektronik penuh, sudah merupakan komputer karena bekerja berdasarkan pada program-program instruksi.

a) ***Komputer generasi pertama (1946 – 1959).*** Walaupun komputer sebelum tahun 1946 sudah elektronik, tetapi tidak dimasukkan sebagai komputer generasi pertama. Komputer generasi pertama dimulai pada tahun 1946. Yang termasuk komputer generasi ini adalah komputer elektronik yang menggunakan konsep stored-program (operasi komputer di kontrol oleh program yang disimpan di memori komputer), sedang komputer elektronik sebelumnya program tidak dapat disimpan di

memori komputer, hanya tiap-tiap instruksi dibacakan ke komputer.

1) Komponen yang dipergunakan adalah tabung hampa udara (Vacumm tube) untuk sirkuitnya.

2) Program hanya dapat dibuat dengan bahasa mesin (machine language).

3) Menggunakan konsep stored-program dengan memori utamanya adalah magnetic core storage.

4) Menggunakan simpanan luar magnetic tape dan magnetikdisk.

5) Ukuran fisik komputer besar, memerlukan ruangan yang luas.

6) Cepat panas, sehingga diperlukan alat pendingin.

7) Prosesnya kurang cepat.

8) Simpanannya kecil.

9) Membutuhkan daya listrik yang besar.

10) Orientasinya terutama pada aplikasi bisinis.

ENIAC (Electrtonic Numerical Integrator And Calculator) adalah komputer dari jenis generasi pertama yang menggunakan tabung hampa udara, mulai dibuat tahun 1942 di Moore School of Electrical Engineering (University of Pensylvania) oleh Dr. John W. Mauchly dan J. Presper Eckert. ENIAC dibuat dengan tujuan utamanya membantu US Army untuk menghitung target sasaran bom, karena pada perang dunia ke 2, hanya 30% dari bom dapat mencapai sasaran dalam radius 300 m dari targetnya.

Komputer komersial generasi pertama paling popular / IBM (1954). Komputer IBM 650,. baik komputer IBM 701 maupun IBM 650 adalah komputer yang berorientasi pada aplikasi bisnis dan merupakan komputer yang paling popular sampai tahun 1959 IBM hanya mengharapkan membuat 50 buah komputer IBM 650 saja, tetapi permintaan pasar sangat mengejutkan. Ribuan komputer IBM 650 terjual pada usahawan Amerika yang mencoba meningkatkan teknologi pengolahan datanya, IBM 650 menggunakan magnetic drum untuk simpanan luarnya dan peralatan input / output kartu plong.

b) ***Komputer generasi kedua (1959 – 1964).*** Komputer generasi kedua mempunyai cirri-ciri sebagai berikut ini.

1) Komponen yang dipergunakan adalah transistor untuk sirkuitnya, dikembangkan di Bell Laboratories oleh John Bardeen, William Shokley dan Walter Brattain pada tahun 1947.

2) Program dapat dibuat dengan dengan bahasa tingkat tinggi (high level language), seperti misalnya Fortran, Cobol, Algol (the Algorithmic Language).

3) Kapasitas memori utama sudah cukup besar dengan pengembangan dari magnetic core storage, dapat menyimpan puluhan ribu karakter.

4) Menggunakan simpanan luar magnetic tape dan magnetic disk yang berbentuk removable disk atau disk pack.

5) Mempunyai kemampuan proses real-time dan time-sharing. Real-time dapat dilakukan karena menggunakan simpanan luar yang sifatnya direct access, seperti misalnya

magnetic disk, sehingga informasi yang dibutuhkan, seketika dapat dihasilkan. Sedang time-sharing memungkinkan beberapa pemakai menggunakan komputer secara bersama-sama dan komputer akan membagi waktunya (time-sharing) untuk tiap-tiap pemakai.

6) Ukuran pisik komputer lebih kecil dibandingkan komputer generasi pertama.

7) Proses operasi sudah cepat, dapat memproses jutaan operasi per-detik.

8) Membutuhkan lebih sedikit daya listrik.

9) Orientasinya tidak hanya pada aplikasi bisnis, tetapi juga ke aplikasi tehnik.

Komputer-komputer generasi kedua yang lainnya, diantaranya adalah sebagai berikut : 1) UNIVAC III, UNIVAC SS80, UNIVAC SS90, UNIVAC 1107 (pabrik pembuatnya Sperry Rand – UNIVAC) ; 2) Burroughs 200 (pabrik pembuatnya Burroughs).IBM 7070, IBM 7080, IBM 1400, IBM 1600 (pabrik pembuatnya International Bussiness Machine); 3) RC 300 (pabrik pembuatnya National Cash Register); 4) Honeywell 400, Honeywell 800 (pabrik pembuatnya Honeywell).

Komputer generasi ketiga (1964-1970). Komputer generasi ketiga mempunyai ciri-ciri sebagai berikut :

1) Komponen yang dipergunakan adalah IC (Integrated Circuits), yang berbentuk hybrid integrated circuits dan monolithic integrated circuits. Hybrid integrated circuits atau

Solid Logic Tehnology (SLT) adalah transistor dan dioda yang diletakkan secara terpisah dalam satu tempat.

2) Peningkatan dari softwarenya.

3) Lebih cepat dan lebih tepat, kecepatannya hampir 10000 kali dari komputer generasi pertama. Ukuran kecepatannya adalah microseconds (jutaan operasi perdetik), bahkan sampai nanoseconds (milyard operasi perdetik).

4) Kapasitas memori komputer lebih besar, dapat menyimpan ratusan ribu karakter.

5) Menggunakan penyimpan luar yang sifatnya random access (dapat memasok record data secara random), yaitu disk magnetic yang berkapasitas besar (jutaan karakter).

6) Penggunaan listrik lebih hemat dibandingkan komputer generasi sebelumnya.

7) Memungkinkan untuk melakukan multiprocessing, yaitu dapat memproses sejumlah data dari sumber-sumber yang berbeda pada waktu yang bersamaan dan dapat mengerjakan beberapa program sekaligus.

8) Pengembangan dari alat input-output yang menggunakan visual display terminal yang bisa menampilkan gambar-gambar dan grafik, dapat menerima dan mengeluarkan suara, serta penggunaan alat pembaca tinta magnetic yaitu MICR (Magnetik Ink Characters Recognition) reader.

9) Harga semakin murah dibandingkan dengan komputer generasi sebelumnya.

10) Kemampuan melakukan komunikasi data dari satu komputer dengan komputer lainnya, misalnya lewat alat komunikasi telepon.

Komputer generasi ketiga yang pertama (1964). Pada tanggal 7 April 1964, IBM mengumumkan sebuah komputer baru, yaitu IBM S/360 atau IBM System 360, menggunakan komponen IC. Dinamakan IBM S/360 karena mampu melakukan operasi satu lingkaran penuh (360 derajat) atau mampu melakukan proses yang dibutuhkan oleh aplikasi bisnis maupun aplikasi tehnik. Komputer-komputer generasi ketiga lainnya, diantaranya adalah : 1) UNIVAC 1108, UNIVAC 9000 (pabrik pembuatnya Sperry Rand-UNIVAC) ; 2) Burroughs 5700, Borroughs 6700, Borroughs 7700 (pabrik pembuatnya Burroughs) ; 3) NCR seri Century (pabrik pembuatnya National Cash Register); 4) GE 600, GE 235 (pabrik pembuatnya General Electric).

c) ***Komputer generasi keempat (sejak tahun 1970).*** Sejak dari generasi ketiga, orang sulit untuk membayangkan komputer generasi selanjutnya, karena sudah banyak sekali perkembangan-perkembangan yang telah terjadi yang sebelumnya belum terpikirkan. Tetapi sejak tahun 1970, ada dua perkembangan yang kemudian dianggap sebagai komputer generasi keempat.

Pertama adalah penggunaan Large Scale Integration (LSI) atau disebut juga dengan nama Bipolar Large Scale Integration. LSI merupakan pemadatan beribu-ribu IC yang dijadikan satu dalam sebuah chip. Istilah chip digunakan untuk menunjukkan suatu lempengan persegi empat yang memuat rangkaian-rangkaian terpadu (integrated

circuits). LSI kemudian dikembangkan menjadi VLSI (Very Large Scale Integration).

Kedua adalah dikembangkan komputer mikro yang menggunakan micro processor dan semiconductor yang berbentuk chip untuk memori komputer (internal memory), sedangkan generasi sebelumnya masih menggunakan magnetic core storage.

Komputer generasi keempat yang pertama (1970). IBM 370 telah menggunakan LSI yang merupakan komputer generasi keempat yang pertama, contoh lainnya adalah :

Personal komputer yang pertama (1977). yaitu Apple II Computer, Radio Shack dan Commodore. Komputer Apple II telah dikembangkan dari komputer Apple I sejak tahun 1976 oleh Steven Jobs dan Steve Wozniak. Mereka adalah pelajar dari Homestead High School (S.M.A. Homestead).

IBM PC/386 Komputer 32 bit yang pertama (1988). Seri selanjutnya dari IBM PC/AT adalah IBM PC/386 yang menggunakan microprocessor Intel 80386 (dengan kecepatan 16 sampai dengan 33 MHz). IBM PS/2 model 60 juga menggunakan Intel 80386. Komputer IBM PC/386 yang menggunakan Intel 80386 merupakan komputer 32-bit yang pertama.

IBM PC/486 (1990). Seri selanjutnya setelah IBM PC/386 adalah IBM PC/486 yang menggunakan microprocessor Intel 80486 dengan kecepatan 25 sampai dengan 66 MHz.

Pentium II (1997). Microprocessor Intel banyak digunakan di komputer IBM PC dan kompatibelnya, mulai dari Intel 8088, 80286,

80386, 80486 dan seri pentium (dikenal dengan Intel P6). Beberapa seri Pentium adalah Pentium 66 (66 MHz), pentium 75 (75 MHz), Pentium 200 (200 MHz). Pada bulan Mei 1977, perusahaan Intel memperkenalkan microprocessor Pentium II sebagai kelanjutan dari seri Pentium. Pentium II mempunyai seri Intel Pentium 233 MHz, Intel Pentium 266 MHz dan Intel Pentium 300 MHz. Selanjutnya sampai sekarang ini adalah Pentium IV dengan kecepatan 1040 MHz, yang beredar di Indonesia baru Pentium III 800 MHz.

d) ***Komputer generasi kelima.*** Komputer generasi kelima sedang dalam pengembangan. Komponen yang dipergunakan adalah VLSI (Very Large Scale Integration). Disamping VLSI, juga sedang dilakukan pengembangan terhadap Josephson Junction, teknologi yang kemungkinan bisa menggantikan chip. Josephson Junction mempunyai kemampuan memproses trilyun operasi perdetik, sedang teknologi chip hanya dapat memproses milyard operasi perdetik.

b. Perkembangan perangkat lunak komputer.

Perangkat lunak (software) merupakan instruksi-instruksi yang ditulis manusia agar perangkat keras komputer dapat berfungsi dan bereaksi atau melakukan langkah-langkah sesuai dengan instruksi - instruksi yang ada dalam perangkat lunak tersebut, perangkat lunak merupakan hal yang penting dalam beroperasi suatu komputer dikatakan oleh Jogiyanto Hartono sebagai berikut :

> "Perangkat keras komputer tidak akan dapat berbuat apa-apa tanpa adanya perangkat lunak. Teknologi yang canggih dari perangkat keras akan berfungsi bila instruksi-instruksi tertentu telah diberikan kepadanya. Instruksi-instruksi tersebut disebut dengan perangkat lunak (software). Instruksi –instruksi

perangkat lunak ditulis oleh manusia untuk mengaktipkan fungsi dari perangkat keras komputer."[18]

Secara umum piranti lunak komputer yang disebut juga dengan bahasa komputer dibagi dalam tiga bagian besar yaitu sebagai berikut :

"1. Perangkat lunak sistem operasi (operating system), yaitu program yang ditulis untuk mengendalikan dan mengkoordinasikan kegiatan dari system komputer.
2. Perangkat lunak bahasa (language software), yaitu program yang digunakan untuk menterjemahkan instruksi-instruksi yang ditulis dalam bahasa pemrograman ke dalam bahasa mesin supaya dapat dimengerti oleh komputer.
3. Perangkat lunak aplikasi (application software), yaitu program yang ditulis dan diterjemahkan oleh language software untuk menyelesaikan suatu aplikasi tertetu."[19]

Penjelasan secara umum dari ketiga sistem piranti lunak tersebut adalah sebagai berikut :

1) Perangkat lunak sistem operasi (operating system)

Merupakan perangkat lunak yang sudah ditulis oleh pabrik berfungsi sebagai penengah antara perangkat keras komputer dan perangkat lunak yang ditulis oleh pemakai komputer, sehingga pemakai komputer dipermudah karena tidak perlu mengerti betul bagaimana perangkat keras bekerja. Gunanya mengendalikan dan mengkoordinasikan komputer disingkat dengan OS.

Pertama kali dikembangkan untuk komputer IBM 701 pada tahun 1954 kemudian dikembangkan lebih lanjut oleh General Motor Research Laboratories pada tahun 1955.

Secara umum operating system dibagi ke dalam dua katagori yaitu control program dan operating system service, secara singkat penjelasan dari hal

---

18. Ibid. Hal. 359.

19 Ibid. Hal. 360.

tersebut adalah sebagai berikut :

a) ***Control program.***

Secara umum mempunyai fungsi sebagai pengatur dan pengkoordinasi di dalam manajemen memori (memory management), manajemen alat pengolah (processor management), manajemen alat-alat I/O (device management) dan manajemen informasi di disk (information management).

Control program umumnya sebagian disimpan di main memory tepatnya di ROM. Control program ini disebut juga dengan resident program atau resident routine. Sebagian control program atau transient routine. Control program yang tersimpan di disk disebut dengan disk operating system atau (DOS), karena tempatnya berada di disk dan yang terletak di tape disebut dengan TOS (Tape Operating System).

b) ***Operating System Service.***

Fungsi dari sistem ini adalah menjadikan penghubung antara pemakai komputer dengan mesin agar menghemat waktu dan mempermudah pembuatan program aplikasi. Selanjutnya pembuat program dapat memusatkan konsentrasinya pada logika dari program yang dibuat. Program aplikasi yang memanfaatkan service dari OS ini biasanya ditulis dalam bahasa perakit. Service dari OS merupakan suatu program bahasa mesin yang terdiri dari beberapa modul.

Disamping service OS juga biasanya menyediakan utility (program manfaat) seperti misalnya *text editor, linkage editor, debugger* dan beberapa *command* untuk menangani disk, file serta peralatan lainnya.

Manfaat program-program tersebut adalah sebagai berikut :

(1) *Text editor* (pengedit text).

Program yang digunakan untuk menuliskan suatu text dalam suatu program aplikasi dengan cara menambah, menghapus, menyisipkan dan membetulkan text untuk selanjutnya direkam dalam suatu file di piringan magnetic. Contoh dari program ini antara lain program paket pengolah kata yang dipakai pada komputer mikro untuk membuat source program (program sumber) antara lain Word star dan Microsoft word.

(2) ***Linkage editor.***

Disebut juga linker merupakan program yang digunakan untuk mengkonfirmasikan object program yang sudah diterjemahkan ke dalam bahasa mesin ke dalam bentuk program yang siap untuk dijalankan (executable program), linker juga dapat digunakan untuk menggabung beberapa object program yang dikompilasi.

(3) ***Debugger.***

Debugger atau debugging aid (pelacak) merupakan program fasilitas OS untuk melacak dan membetulkan kesalahan program yang sudah berbentuk bahasa mesin.

(4) *Command.*

Disamping sejumlah fasilitas diatas, OS juga menyediakan fasilitas-fasilitas lainnya yang dapat diaktipkan dengan suatu perintah langsung (command) tertentu. Command

ini dapat digunakan untuk menangani disk, file dan peripheral. Command dapat berbentuk internal command atau extrernal command. Sebagai contoh pada MS-DOS atau PC-DOS, operating system yang dipergunakan pada komputer IBM PC, internal command terdiri dari beberapa command yang disimpan bersama-sama menjadi satu dalam file di disk dengan nama file COMMAND.COM.

2) Piranti lunak bahasa (language software).

Bila language software tidak tersedia, maka pembuat program harus menulis programnya langsung dengan bahasa mesin yang berbentuk bilangan-bilangan binary. Suatu instruksi program yang ditulis dalam bahasa mesin dapat berbentuk sebagai berikut :

000100110010

Untuk itu diperlukan language software agar pengguna komputer lebih mudah berkomunikasi dengan komputernya, adapun bahasa-bahasa tersebut antara lain Assembler (perakit), Compiler dan Interpreter (penterjemah), bahasa-bahasa tersebut adalah sebagai berikut :

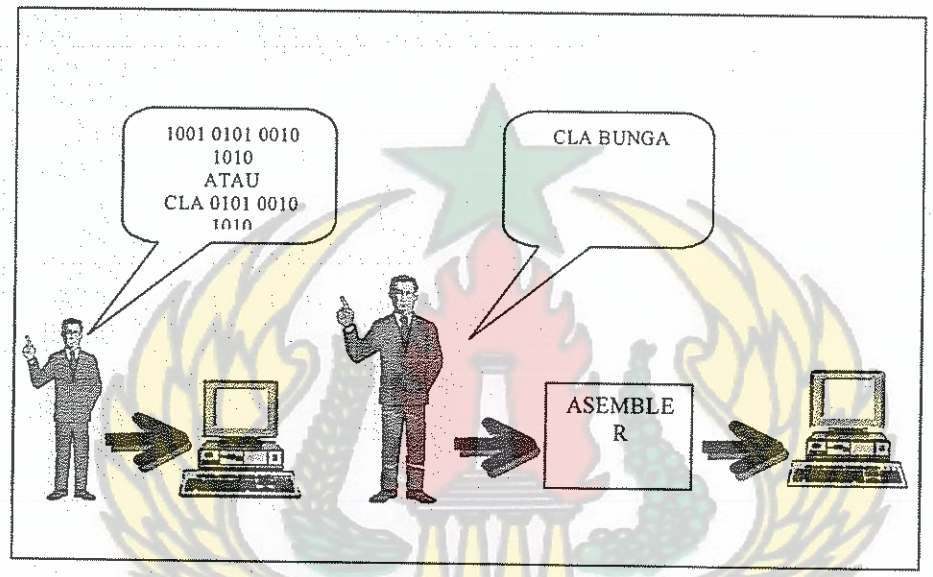
a) Assembler.

Assembler merupakan program yang digunakan untuk menterjemahkan program aplikasi yang ditulis dengan bahasa perakit (assembly language), atau bahasa pemrograman simbolik (symbolic programming language) menjadi bahasa mesin. Dengan bahasa simbolik, masing-masing op-code dalam bahasa mesin tidak ditulis dengan bentuk bilangan binary, tetapi dengan suatu kode simbolik singkatan tertentu yang disebut dengan *mnemonic*.

Instruksi program yang ditulis dengan mnemonic akan diterjemahkan ke dalam bentuk bilangan binary bahasa mesin dengan menggunakan assembler. Program yang ditulis dengan bahasa simbolik tersebut disebut dengan *source program* (program sumber) dan hasil penterjemahan ke dalam bahasa mesin disebut dengan object program (program obyek).

Gambar . 2

Bahasa Mesin danAssembler



b) Compiler / Interpreter.

Assembler masih dekat dengan bahasa mesin artinya masih terlalu tehnis dan menyulitkan bagi pengguna komputer, sehingga masih diperlukan lagi bahasa tingkat tinggi (high level language) yaitu compiler dan interpreter. Keduanya merupakan bahasa penterjemah adapun perbedaannya adalah sebagai berikut : *compiler* menerima seluruh source program secara utuh dan lengkap kemudian diterje-mahkan secara utuh, sedangkan *interpreter* menterjemahkannya secara

terpotong-potong atau instruksi per instruksi langsung diterjemahkan.

Contoh bahasa tingkat tinggi yang sifatnya compiler diantaranya ialah FORTRAN, COBOL, PASCAL dan C language. Sedang yang bersifat interpreter antara lain BASIC yang sekarang sangat popular dan sering digunakan terutama oleh IBM.

1) Piranti lunak aplikasi (application software).

Program-program tersebut diatas sangat membantu pemakai komputer untuk berkomunikasi dengan komputernya namun program-program tersebut belum dapat menyelesaikan permasalahan tertentu yang dihadapi oleh pemakai komputer, berbagai persoalan manusia sangat banyak dan beragam sehingga program aplikasipun ribuan macamnya dan digunakan untuk memecahkan masalah yang sedang dihadapi oleh pemakai komputer. Contoh dari masalah yang dihadapi pengguna komputer adalah perlunya menulis surat atau membuat model pesawat terbang sehingga, untuk memecahkan masalah tersebut perlu menggunakan program aplikasi Microsoft word untuk menulis dan Auto CAD untuk membuat model pesawat terbang.

Program aplikasi ini bisa ditulis atau diprogram sendiri oleh pengguna komputer dengan menggunakan Assembler, Compiler ataupun Interpreter menjadi language software tertentu, ataupun membeli yang sudah jadi. Berikut ini beberapa contoh program aplikasi yang berdasarkan pada penggunaan komputer secara umum :

a) Bidang tehnik dan ilmu pengetahuan.

Komputer yang digunakan untuk bidang ini pada umumnya super komputer yang mempunyai kecepatan proses sangat tinggi, diantaranya digunakan untuk memetakan susunan melekul DNA

manusia, contoh piranti lunaknya antara lain adalah untuk grafik dan rancang bangun adalah Computer Aided Design (CAD) .

b) Dalam bidang bisnis.

Informasi dalam bidang bisnis sangat vital karena untuk pengembangan bisnis diperlukan informasi yang sebanyak-banyaknya dan ketepatan yang tinggi, komputer digunakan untuk mengolah data sehingga dapat menyediakan informasi secara cepat dan tepat dalam bidang ini komputer digunakan untuk Management information system (MIS) yaitu suatu istem informasi yang didasarkan pada komputer, dirancang untuk mendukung operasi dengan menyediakan informasi kepada manajemen untuk pengambilan keputusan.

c) Bidang Industri.

Secara umum dalam bidang ini digunakan untuk pengawasan numerik produksi (numerical control) dan untuk pengawasan proses produksi (process control), lebih jauh lagi digunakan dalam pelaksanaan proses itu sendiri terutama program-program komputer untuk robot-robot mekanik pengganti pekerjaan manusia yang berbahaya atau yang memerlukan ketepatan tinggi. Contoh bahasa komputer ini, diantaranya APT (Automatically Programmed Tools) dan IBM's AUTOSPOT (Automatic System for Positioning Tools).

d) Bidang Perbangkan.

Pada umumnya dipergunakan untuk mempercepat proses transaksi sekaligus memproses dan mengontrol transaksi. Salah satu contoh piranti lunak dibidang ini adalah Card Pack digunakan dibidang kartu kredit mulai dari aplikasi kartu sampai dengan transaksi kartu

kredit.

e) Bidang Pendidikan.

Dibidang ini paling sangat banyak piranti lunak aplikasi sebanyak bidang ilmu / mata pelajaran yang menjadi objek pada suatu lembaga pendidikan – pendidikan yang ada sekarang ini.

f) Bidang kedokteran.

Paling banyak digunakan untuk sistem diagnosa tubuh manusia guna menganalisa organ tubuh manusia bagian dalam yang sulit untuk dilihat, sistem CAT (Computerized Axial Tomography) pertama kali digunakan pada tahun 1973 untuk membuat gambar otak. Sistem yang baru disebut dengan DSR (Dynamic Spatial Reconstructor) digunakan untuk organ tubuh yang bergerak.

Contoh lainnya adalah SPECT (Simple Photon Emission Computer Tomography) juga merupakan sistem komputer yang mendeteksi partikel-partikel tubuh yang ditampilkan dalam bentuk gambar, SPECT menggunakan gas radioaktip, selanjutnya adalah PET (Position Emission Tomography) juga merupakan sistem komputer yang menampilkan gambar yang mempergunakan isotop radioaktip.

g) Bidang Penerbangan.

Program aplikasi Instrumen landing system (ILS) yang gunanya menuntun pesawat terutama pada saat malam hari / cuaca berkabut, untuk mendarat yang berdasarkan pada instrumen-instrumen pendaratan (bukan visual), program dan alat ini sangat vital karena apabila gagal dapat menyebabkan jatuhnya pesawat terbang.

h) Bidang kriminalitas.

Dikembangkan program komputer yang cukup canggih untuk hal ini yaitu dengan nama Crime Analysis Support System. (CASS), program ini dapat mengidentifikasikan suatu daerah yang kemungkinan akan terjadi kriminalitas.

Program komputer lainnya yang digunakan di bidang kriminalitas diantaranya adalah :

- PROMIS (Prosecutor Offender Management Information System). System ini dikembangkan oleh Institute of Law and Social Research di Washington D.c. PROMIS dapat memberikan informasi mengenai masalah-masalah kriminalitas mana yang paling penting dan dapat memberikan informasi ngenai bukti-bukti dari tertuduh untuk dibawa ke pengadilan.
- CATCH (Computer Assisted Terminal Criminal Hunt). Sistem ini digunakan di kota New York. CATCH menyediakan informasi mengenai deskripsi secara mendetail dari orang-orang yang dicurigai dan akan ditampilkan di layar komputer.
- MOTION (Metropolitan Orleans Total Information Online Network). Sistem ini digunakan di New Orleans. MOTION menyediakan informasi sekitar 150.000 orang-orang yang mempunyai latar belakang kriminalitas, meliputi sidik jarinya, nama-nama samarannya dan data mendetail lainnya.
- ARJIS (Automated Regional Justice Information System). Sistem ini digunakan di San Diego. ARJIS dapat menyediakan informasi mengenai sidik jari dan tingkah laku dari pelaku

kriminalitas yang dicurigai.

i) Bidang permainan.

Selain untuk hal-hal yang serius komputer juga digunakan untuk mengisi waktu luang dengan berbagai macam aplikasi permainan (computer games). justru dibidang inilah tidak terhitung jumlahnya karena aplikasinya sangat beragam. Pada permainan tertentu mirip dengan simulasi pertempuran sehingga aplikasi ini kadang-kadang digunakan dan ditingkatkan menjadi simulator pertempuran oleh pihak militer (war game simulator).

Dari uraian tersebut disimpulkan bahwa komputer adalah sistem elektronik yang mampu memproses data secara cepat dan akurat serta yang dirancang / diorganisasikan supaya secara otomatis menerima dan menyimpan data input, memprosesnya dan menghasilkan out put dibawah pengawasan suatu langkah-langkah instruksi-instruksi program yang tersimpan di memori (stored program), singkatnya komputer adalah alat elektronik untuk memproses / mengolah data yang operasinya berdasarkan pada bahasa dan program tertentu.

Sampai sekarang telah ada lima generasi komputer dan akan terus berkembang, perkembangan piranti keras dan piranti lunaknya sangat pesat terutama perkembangan piranti lunaknya (hampir tiap bulan ada yang baru dan lebih canggih). Penggunaan komputer sangat luas hampir disemua bidang namun terjadi juga penyalahgunaan komputer yang populer disebut dengan kejahatan komputer, kejahatan ini makin berkembang setelah adanya Internet (cyberspace) menyebabkan timbulnya cybercrime (Haking, Preking dan Kraking).

MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

Bab. III

BAB III

PERKEMBANGAN INTERNET DAN KEJAHATAN KOMPUTER

11. Perkembangan jaringan komputer / Internet.

a. Sejarah Perkembangan Internet.

Departemen pertahanan Amerika dalam upaya untuk membuat jaringan komputer yang bisa saling berhubungan antara yang satu dan lainnya melakukan suatu eksperimen 20 tahun yang lalu, eksperimen itu disebut ARPAnet yang diharapkan tetap berfungsi, meskipun terjadi gangguan pada sebagian jaringan tersebut.

Pada saat yang hampir bersamaan, LAN berbasis Ethernet mulai dikembangkan. Pada umumnya LAN tersebut menggunakan UNIX yang dilengkapi perangkat lunak jaringan IP. Pada saat itu banyak organisasi yang membangun jaringannya sendiri menggunakan protokol komunikasi seperti yang disebut oleh ARPAnet sebagai IP. Hal tersebut memungkinkan komputer pada suatu LAN dapat mengakses fasilitas ARPAnet. Jaringan tersebut makin banyak dan disempurnakan, sehingga terbentuk Internet seperti yang ada sekarang ini.

b. Cara kerja Internet.

Internet terhubung satu sama lainnya melalui satu set peralatan atau komputer yang disebut router yang menghubungkan jaringan-jaringan menjadi satu jaringan yang sangat besar. Bagian-bagian internet yang dimaksud dapat berupa berbagai jenis LAN, komputer mini, mainframe, supers computer, bahkan hanya sebuah PC.

c. Aplikasi-aplikasi di Internet.

Saat ini telah banyak jenis aplikasi yang dapat dijalankan di internet. Aplikasi-aplikasi tersebut diantaranya adalah, Telnet, atau remote Login, FTP, Electric, Mail.

News, Gopher, Wais serta WWW (World Wide Web).

1) Telnet (Remote Login).

Telnet atau Remote Login (masuk ke jaringan dari jauh) adalah proses login dari satu komputer yang terhubung ke internet ke suatu server (komputer lain) yang terhubung juga ke internet.

Fasilitas remote login atau telnet merupakan fasilitas standar yang biasanya tersedia pada sistem operasi UNIX. Jika berhadapan dengan terminal UNIX yang terhubung ke internet, pada dasarnya dapat melakukan proses telnet atau remote login ke server manapun di internet.

2) FTP (File Transfer Protokol).

FTP (File Transfer Protokol) adalah fasilitas untuk memindahkan file dari satu komputer ke komputer lain melalui jaringan internet. File tersebut dapat diloading ke komputer para pengguna (user) melalui fasilitas FTP ini.

Untuk mempercepat transfer file yang berukuran besar, file-file yang disediakan untuk proses FTP biasanya dalam keadaan terkompres, sehingga ukuran filenya menjadi jauh lebih kecil.

3) Electronic Mail.

Electronic Mail atau E-mail adalah fasilitas untuk mengirimkan surat secara elektronik. Konsepnya persis sama seperti pengiriman surat biasa melalui pos, hanya surat kita disini dibuat dalam bentuk file teks. Beberapa fasilitas yang biasanya disediakan dalam perangkat lunak electronic mail, diantaranya adalah : a) Folder, yaitu fasilitas untuk menyimpan dan mengelompokkan daftar surat yang masuk atau sudah dikirim :. b) Forwarding, yaitu fasilitas untuk meneruskan surat yang diterima ke user lain ; c) Replay, yaitu fasilitas untuk membalas surat kepada pengirimnya. ; d) Mailing list, yaitu fasilitas

untuk melihat daftar surat, misalnya surat-surat yang baru masuk dan belum dibaca.

E-mail menggunakan protokol SMTP (Simple Mail Transfer Protokol) yang bekerja diatas protokol TCP/IP.

4) News.

Dengan menggunakan electronic mail pada dasarnya dapat diciptakan forum diskusi yang melibatkan sejumlah orang. Surat-surat untuk tujuan tersebut yang ingin terlibat dalam diskusi. Cara ini kurang effisien untuk jumlah user yang besar, oleh karena itu muncul aplikasi baru yang disebut News.

5) WWW (World Wide Wibe).

Salah satu bentuk aplikasi internet, yang relatif baru dan paling populer adalah WWW (World Wide Web) atau sering hanya disebut Web saja. WWW adalah aplikasi yang paling banyak menggunakan fasilitas grafik, multi media serta menyediakan kemampuan lingking yang sangat fleksibel. Web memungkinkan melakukan Highlight kata atau gambar pada suatu dokumen untuk di link pada media lain yang mungkin berbentuk dokumen (file), frase (bagian tertentu dari suatu file), klip video, atau file suara. Web juga menyediakan pilihan yang banyak sekali untuk memudahkan memformat tampilan dokumen.

d. Sistem Infromasi dalam Bentuk Web.

Melihat kemampuan-kemampuan yang dimilikinya, juga berdasarkan tinjauan bahwa kecepatan saluran komunikasi data yang semakin meningkat terus, maka aplikasi Web ini akan memegang peranan yang sangat penting di masa yang akan datang. Kini Web telah banyak diharapkan untuk berbagai tujuan, diantaranya adalah

1) Sarana pendidikan dan pengetahuan umum, misalnya berbentuk museum multi media, sistem informasi tentang tata surya, kebun binatang multi media dan sebagainya ; 2) Majalah atau surat kabar elektronik ; 3) Catalog produk ; 4) Pelayanan informasi on-line dari berbagai perguruan tinggi ; 5) Pelayanan informasi on-line dari berbagai organisasi lokal maupun internasional ; 6) Promosi pariwisata dan sebagainya.

e. Guna/manfaat Internet.

Secara umum Internet mendukung bisnis global, akademi, dan komunitas yang mewakili pribadi lebih tiga puluh juta di lima benua. Terdapat 4 fungsi internet yaitu :

1) Fungsi Komunikasi ; 2) Fungsi Resource Sharing (berbagi bahan informasi) ; 3) Fungsi Resource Discovery ; 4) Fungsi Komunitas.

Sebagaimana produk teknologi lainnya internet merupakan produk hasil kemajuan teknologi komputer, teknologi informasi, teknologi komunikasi yang mempunyai kemampuan yang luar biasa. Telah kita ketahui beberapa negara maju kini sedang mengembangkan teknologi komputer dengan kecepatan proses yang sangat tinggi, yaitu berupa komputer optik dengan kecepatan proses diperkirakan mampu mendekati kecepatan cahaya. Apabila teknologi komunikasi juga berkembang dengan cepat pula maka internet akan mempunyai kemampuan yang jauh di atas kemampuannya sekarang ini.

Dapat diperkirakan di kemudian hari transaksi-transaksi bisnis dengan menggunakan internet akan semakin meningkat. Masalah yang perlu dipikirkan lebih lanjut adalah pengaman data informasi yang bersifat rahasia perusahaan, mengingat besarnya jaringan internet peluang untuk hal-hal negatif masih tetap terbuka kemungkinannya.

12. Kejahatan komputer secara umum.

Kejahatan komputer merupakan *bahasa yang salah kaprah* karena sebenarnya komputer tidak melakukan kejahatan yang melakukan kejahatan adalah orangnya atau pengguna komputer, mereka dengan cara tertentu menyalahgunakan komputer untuk melakukan kejahatan (*alat kejahatan*) atau menyerang peralatan komputer sebagai *sasaran kejahatan*. Sebenarnya yang tepat adalah ***penyalahgunaan komputer*** atau ***kejahatan dengan sasaran komputer***, pada suatu saat nanti bisa saja terjadi kejahatan komputer yang sesungguhnya yaitu apabila piranti lunak komputer sudah dapat berpikir sendiri atau mempunyai artifisial intelijen (intelijen buatan), dan perangkat kerasnya sudah dapat dengan bebas berinteraksi dengan lingkungannya melalui indra-indranya yang sudah sangat maju, sehingga benar-benar komputer tersebut dengan keinginannya sendiri melakukan suatu kejahatan tertentu.

Apabila mendengar kejahatan komputer sekarang ini sesungguhnya adalah komputer dijadikan alat kejahatan atau komputer yang dijadikan sasaran kejahatan, terdapat beberapa katagori kejahatan komputer sebagaimana dikatakan oleh David Icove dan kawan-kawan sebagai berikut :

> "There are many ways to categorize computer crimes. You might divide them according to who commits them and what their motivation might be (e.g., professional criminals looking for financial gain, angry ex-employees looking for revenge, crakers looking for intellectual challenge). Or, you might divide these crimes by how they are perpetrated (e.g., by physical means such as arson, by software modification, etc). "20

dapat dikatagorikan bahwa kejahatan tersebut antara lain berdasarkan pada : *Motivasi* mereka yaitu penjahat professional yang mencari keuntungan, karena *Balas dendam* disebabkan dipecat atau hanya untuk *Menguji intektualnya*. Bisa juga dikatagorikan atau dibagi berdasarkan pada *Cara-cara melakukannya* antara lain dengan secara fisik seperti dirusak atau

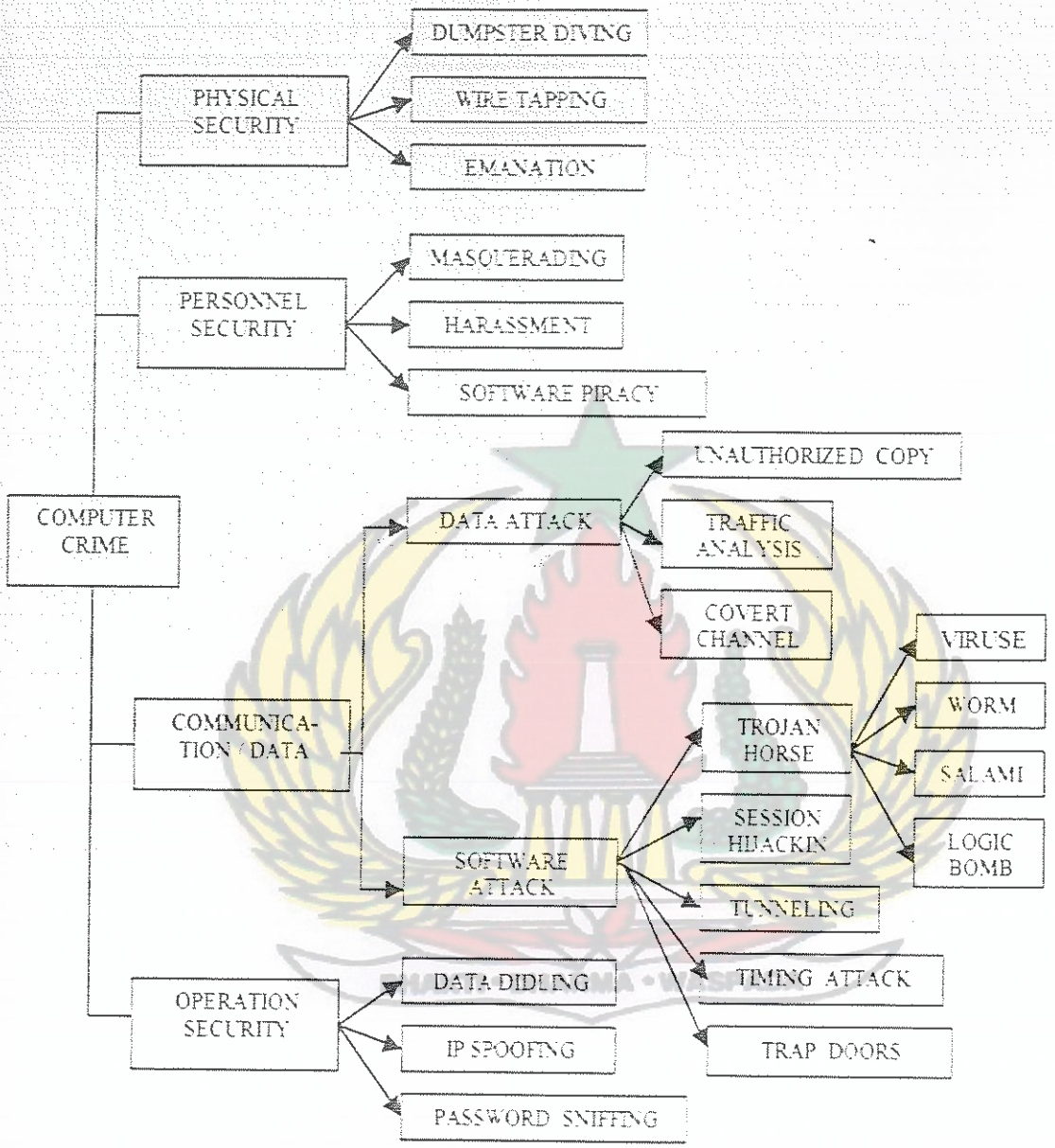
---

20. Icove David, dkk. ***Computer Crime A Crimefighter's Handbook.*** O'Reilly Online Catalog [Online]. hal 2. Tersedia : http://www.oreilly.com/catalog/crime/chapter/ch_2.html. [25 April 2000].

dibakar, memodifikasi piranti lunak dan sebagainya.

Gambar : 1

Diagram kejahatan komputer.



Katagori lainnya adalah berdasarkan pada *Cara-cara bagaimana perangkat komputer diserang* sebagaimana dalam diagram tersebut diatas (akan tetapi sebagian dari hal tersebut ada yang bukan kejahatan hanya membuat kesal pemilik komputer), jenis-jenis kejahatan tersebut garis besarnya adalah terhadap Keamanan secara fisik (Breaches of Physical

Security), terhadap Keamanan personil (Breaches of Personnel Security), terhadap Keamanan jalur komunikasi (Breaches of Communications and Data Security) dan terhadap Keamanan operasional (Breaches of Operations Security). Penjelasan kejahatan - kejahatan tersebut adalah sebagai berikut :

a. Breaches of Physical Security (Jenis Keamanan fisik).

Keamanan fisik menyangkut perlindungan secara fisik terhadap komputer, peralatan komputer, media komputer dan seluruh fasilitas fisik dari gangguan alam atau bencana , berbagai macam kecelakaan dan kemungkinan gangguan / serangan secara fisik. Sebagaimana yang dikatakan oleh David Icove dkk, "Physical security is concerned with physical protection of the computer, computer equipment, computer media, and the overall physical facility from natural disasters, accidents of various kinds, and intentional attacks."21

Namun dalam kenyataannya tetap terjadi kejahatan yang menyerang bidang ini, kejahatan-kejahatan tersebut adalah sebagai berikut :

1) Dumpster Diving (Menyelami sampah).

Kejahatan ini adalah memanfaatkan kertas-kertas buangan yang ada ditempat sampah dari ruang komputer.

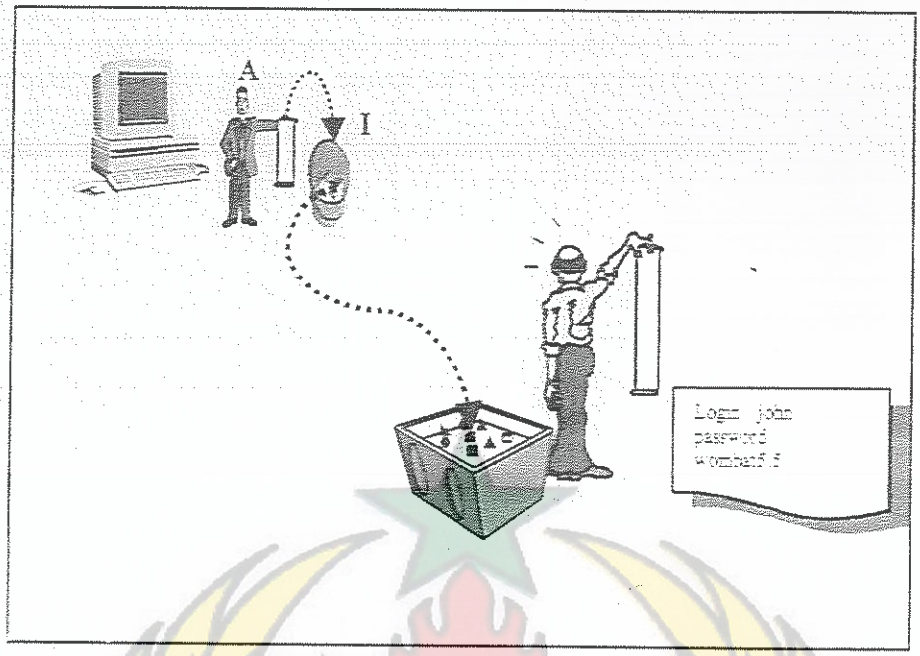
Cara lain dari jenis ini adalah dengan memanfaatkan data-data di komputer yang dihapus operator namun belum terhapus secara penuh, selanjutnya oleh pelaku kriminal data ini direkonstruksi kembali dan dimanfaatkan. Hal-hal seperti ini sangat biasa terjadi dilakukan oleh perusahaan-perusahaan yang saling bersaing untuk mendapatkan rahasia dari saingannya.

---

21. Ibid.

Gambar. 4

Dumpster Diving



2) Wire Tapping (Penyadapan kawat telepon).

Seringkali kabel-kabel jaringan telepon tidak terlindungi sebagaimana mestinya sehingga para penyusup memanfaatkan kelemahan ini, dengan cara secara fisik merusaknya (mengelupas kabel) kemudian menempelkan kabel penyadap dan mengambil data dari informasi yang berjalan di kabel tersebut.

3) Eavesdropping on Emanations (Menampung pancaran Emisi).

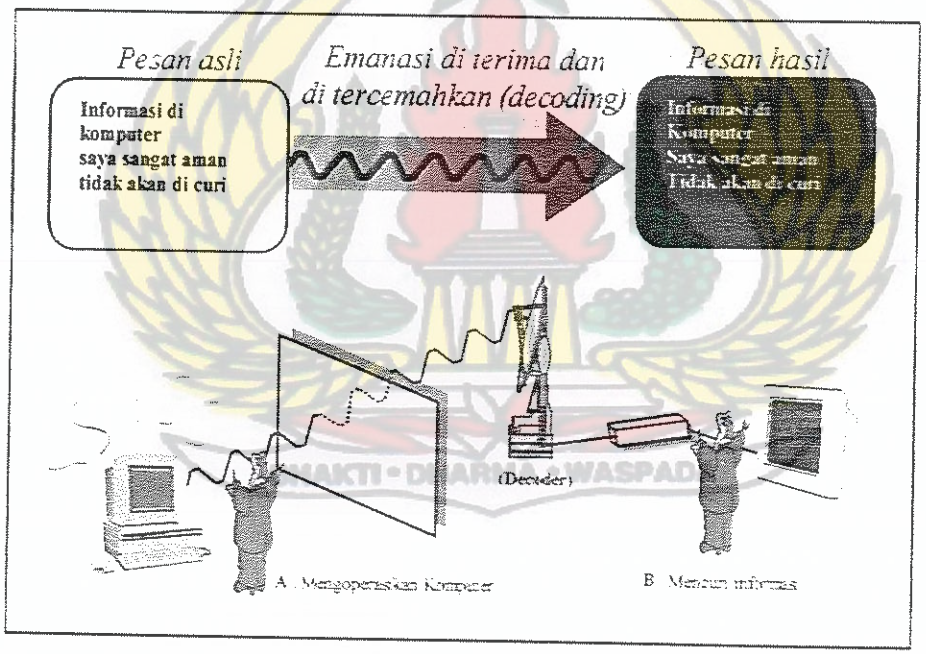
Seperti alat-alat elektronik lainnya apabila sedang bekerja akan memancarkan gelombang elektromagnit . gelombang memancar kesegala penjuru dengan pancaran yang bentuknya menyerupai proses yang sedang berlangsung. Pancaran ini dengan satu alat ditangkap dan diterjemahkan kembali, sehingga proses yang terjadi di *komputer pusat pancaran* dapat dibaca dan dilihat oleh penerima pancaran tersebut dengan cara menterjemahkan

kembali pancaran tersebut (Decoding).

Hal tersebut bisa terjadi karena komputer-komputer yang digunakan tidak dilengkapi dengan pelindung gelombang atau ruangan komputernya tidak dilindungi dengan pelindung gelombang. sehingga gelombang yang dipancarkan oleh komputer yang sedang bekerja dapat ditangkap oleh suatu Reciver (alat penerima) kemudian diterjemahkan oleh Decoder (alat pengurai) akibatnya apa yang sedang dikerjakan dapat dibaca dengan jelas oleh orang yang tidak berhak.

Gambar. 5

Emanations



b. Breaches personnel Security (Jenis Keamanan personil).

Ruangan komputer yang menyimpan data-data sensistif dan penting diamankan secara fisik agar tidak mudah dimasuki oleh orang yang tidak berhak. digabungkan dengan sistem pengaman personelnya dimana operator-operator komputer bekerja

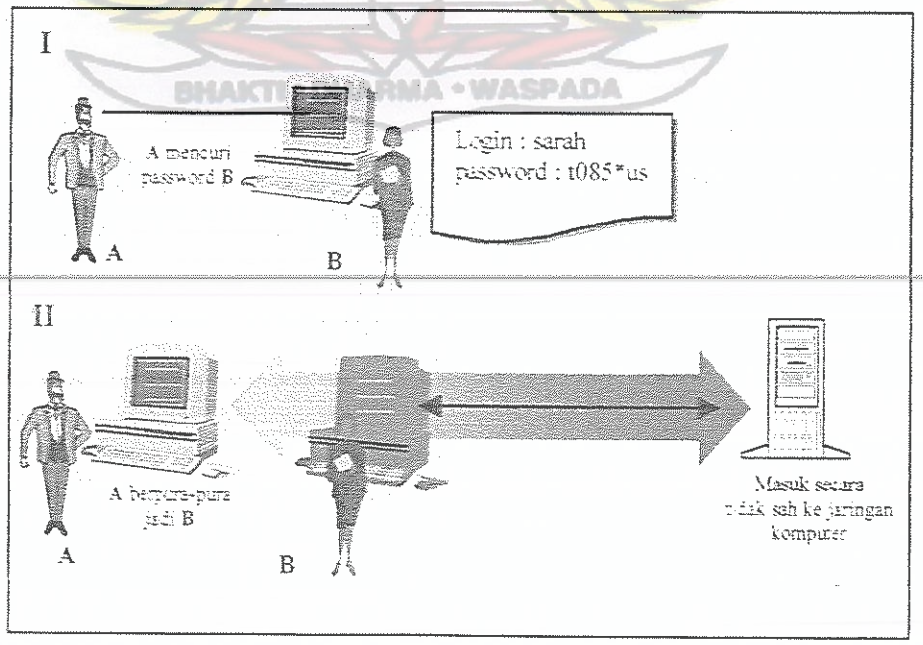
sesuai dengan jadwal yang sudah diatur. memakai seragam / pakaian tertentu atau tanda pengenal tertentu, diberikan kunci untuk akses ke ruangan komputer juga diberikan kepadanya password untuk login (ID Login) atau berhubungan dengan jaringan komputer. Namun kelemahan-kelemahan dalam bidang ini tetap dimanfaatkan oleh para pelaku kejahatan sebagai berikut :

1) Masquerading (Barisan topeng).

Cara seperti ini dengan menggunakan suatu samaran tertentu kemudian orang tersebut beriringan dengan operator komputer yang berwenang masuk keruang komputer (seolah-olah bagian dari pada operator komputer di ruangan tersebut). kemudian ia mencuri identitas *password* atau Personal identification number (PIN) . selanjutnya mengakses komputer atau mengintip orang yang sedang mengakses komputer. bisa juga dengan kemudian mencuri data-data yang sensitif dari komputer yang dijadikan sasarannya.

Gambar. 6

Masquerading



2) Harassment (Gangguan / penghinaan).

Beberapa pengguna komputer yang tidak bertanggung jawab melakukan penghinaan atau ancaman melalui fasilitas email dan secara terbuka ditayangkan kepada umum, dalam papan bulletin (bulletin board) pada sistem newsgroup dalam internet. Presiden Abdurahman Wahid menjadi korban dari hal ini, gambar yang menghina dan membuatnya malu ditayangkan secara vulgar.

3) Software piracy (Pembajakan piranti lunak).

Sasarannya adalah program-program komputer yang sangat dibutuhkan atau mempunyai harga tinggi, program tersebut digandakan secara illegal tanpa ijin dari pemiliknya kemudian dijual kepada umum dan tanpa sedikitpun memberi kompensasi kepada pemilik program tersebut.

c. Breaches of Communications and Data Security (Jenis komunikasi dan keamanan data).

Sasaran kejahatan ini adalah data komputer dan piranti lunaknya serta terhadap proses komunikasi dari data itu sendiri atau terhadap proses transportasi data dari satu komputer ke komputer lainnya, secara umum dibagi dalam dua bagian besar yaitu *Data attacks* dan *Software attacks*.

1) Data Attacks (Serangan terhadap data pencurian data).

Kejahatan ini dilakukan dengan mengganggu pengguna komputer yang sah dengan cara mengambil bagian-bagian kecil data kemudian menggabungkan bagian-bagian kecil tersebut sehingga menjadi kesatuan data yang lebih besar, dilakukan terhadap titik-titik kebocoran data kemudian mengakses melalui aliran data secara illegal. Beberapa modus pencurian

data tersebut adalah sebagai berikut :

a) Unauthorized copying data (Mengkopi data secara tidak sah).

b) Traffic Analysis data (Menganalisa lalu lintas data).

Beberapa data dari lembaga pemerintah atau dari perusahan-perusahaan resmi diinformasikan kepada publik secara sengaja untuk kepentingan masing - masing, namun ada beberapa data tersebut yang tersirat kemudian dianalisa terutama waktu data tersebut ditranmisikan dan waktu data tersebut ditayangkan. Untuk metode ini memerlukan cara analisa komputer yang canggih karena data-data tersembunyilah yang dianalisa bukan data-data yang sengaja diumumkan. Hasil analisa tersebut kemudian disalahgunakan.

c) Covert Channel (Saluran rahasia).

Cara ini memanfaatkan bocoran data dimana seorang penyusup yang pintar menyembunyikan data yang dicurinya dalam suatu output yang seolah-olah tidak penting dan boleh dibaca oleh siapapun juga. contohnya adalah dengan menggabungkan laporan-laporan yang berisi laporan biasa kemudian dirubah secara sederhana dengan digabungkan informasi rahasia yang hanya orang-orang tertentu saja boleh melihatnya.

Seolah-olah pelaku disini membuat terowongan rahasia dan dia bisa melihat data tersebut karena dimodifikasi seolah-olah data biasa. biasanya yang menjadi objek adalah password. kode-kode yang diluncurkan serta lokasi-lokasi dari informasi yang sensitif. sasaran lainnya adalah informasi yang berhubungan dengan sistem waktu. informasi -informasi yang penting atau dirahasiakan.

sistem pengendali proses yang berhubungan dengan waktu-waktu sebelumnya yang sebenarnya dirahasiakan.

2) Software attack (Serangan terhadap Piranti lunak).

Pada bagian inilah sebenarnya *cara-cara haking dilakukan* atau para *Haker* melakukan aksinya karena yang menjadi objek mereka adalah piranti lunak. adapun cara-cara kejahatan komputer dalam bidang ini adalah sebagai berikut :

a) Trap doors (Pintu jebakan).

Cara ini merupakan cara klasik atau sering dilakukan dalam menyerang piranti lunak komputer dijelaskan oleh David Icove dkk. "A trap door is a quick way into a program, it allows program developers to bypass all of the security built into the program now or in the future."[22]

Cara ini adalah cara yang paling cepat untuk memasuki program memungkinkan para penyusup program untuk melakukan jalan pintas terhadap sistem keamanan yang dibangun dalam program tersebut, Trap doors sebenarnya adalah kunci dari suatu program yang diletakkan pada akhir program. kunci ini menggunakan password tertentu untuk masuk keseluruh program tersebut.

Trap doors dibuat biasanya setelah program ini ditest dan bila berfungsi dengan baik kemudian program ini ditutup pintunya serta diamankan dengan password namun kadang-kadang password tersebut tertinggal sehingga disalahgunakan oleh para haker / kraker.

---

22. Ibid. Hal. 12.

Apabila mereka dapat masuk ke pintu ini dengan sendirinya mereka bisa merubah program dengan sekehendak mereka sendiri dan secara diam-diam, mereka bisa mengambil keuntungan dari hal ini atau hanya cukup untuk memenuhi rasa penasaran mereka saja.

b) Pembajak musiman (Session Hijacking).

Cara ini sangat simpel, pada saat seorang operator meninggalkan terminal komputer kemungkinan untuk minum atau makan sesuatu seseorang yang dekat dengan dirinya mungkin saja rekan kerja yang sebetulnya tidak mempunyai wewenang, langsung melihat ke komputer yang ditinggalkan tersebut membaca datanya atau merubah programnya, dijelaskan oleh David Icove dkk, "In the simplest type, an unauthorized user gets up from his terminal to go get a cup of coffee. Someone lurking nearby-probably a coworker who isn't authorized to use this particular system-sits down to read or change files that be wouldn't ordinarily be able to access." 23

c) Tunneling (Membuat terowongan).

Cara ini hampir sama dengan covert channel hanya dilakukan dengan program yang lebih canggih dan sasarannya adalah data-data yang ditransfer melalui jaringan komputer, sedangkan Covert channel langsung pada Personal Computer tidak melalui jaringan komputer.

d) Timing attack (Serangan dengan irama waktu).

Timing attack merupakan salah satu jenis tehnik kejahatan

---

23. Ibid. Hal. 13.

komputer yang cukup kompleks dalam upaya mendapatkan akses secara illegal pada suatu piranti lunak. cara ini termasuk menyalahgunakan kondisi yang berganti secara cepat seolah-olah berlomba antara dua proses operasi komputer dalam sistem dan tergantung kepada siapa yang paling cepat memasuki sistem tersebut. Artinya para pelaku dapat memasuki suatu piranti lunak data kemudian secara cepat menghapus suatu data dan mengganti dengan file yang mereka punyai.

e) Trojan horse (Kuda Trojan).

Beberapa abad yang lalu selama perang Trojan Kerajaan Yunani menyembunyikan tentara-tentaranya di dalam perut patung kuda raksasa yang dirancang oleh Odysiuss. kemudian kuda tersebut didorong dimasukkan melalui gerbang kedalam kota musuhnya yang akan diserang. Selanjutnya tentara-tentara yang bersembunyi di dalam patung kuda tersebut. serentak keluar dari perut patung tersebut dan langsung menyerang musuhnya yang ada dalam kota.

Dalam bidang komputer mirip dengan taktik tentara Troyan tadi dimana program-program jahat disembunyikan dan dikemas sedemikian rupa seolah-olah program biasa. kemudian dimasukkan pada suatu piranti lunak dan setelah masuk instruksi-instruksi dalam program jahat tersebut beraksi untuk merusak. mengambil atau merubah program / data dalam komputer yang diserangnya. Dijelaskan oleh David Icove sebagai berikut :

> "A Trojan horse is a method for inserting instruction in a program so thar program performs an unauthorized function while apparently performing a useful one. Trojan horses are a common technique for planting other problems in computers, including viruses. worms. logic bombs. and salami attacks (more

about these later). Trojan horses are a commonly used method for committing computer-based fraud and are very hard to detect."24

Taktik kuda Troyan termasuk Virus komputer. Cacing komputer, Bom logika dan Serangan Salami biasanya digunakan sebagai dasar para penjahat melakukan penipuan dengan komputer dan sangat sulit untuk dideteksi , namun sebagian besar tidak dipakai untuk melakukan penipuan tetapi untuk merusak atau menjahili pemakai komputer lainnya. Penjelasan dari hal tersebut adalah sebagai berikut :

(1) Viruses and Worms (Virus dan Cacing komputer).

Banyak orang bingung antara virus dan cacing komputer mereka mempunyai persamaan masuk dengan tehnik kuda Troyan akan tetapi sebenarnya sangat berbeda, diterangkan oleh David Icove dkk. sebagai berikut :.

"A virus is a program which modifies other so they replicate the virus. In other words, the healthy living cell becomes the original program, and the virus affects the way the program operates. How ? It inserts a copy of itself in the code. Thus, when the program runs, it makes a copy of the virus. This happens only on a single system. (Viruses don't infect networks in the way worms do, as we'll explain below). However, if a virus infect programs on that computer. This is how a computer virus spreads."25

Virus adalah program yang memodifikasi program lainnya dan mereka memperbanyak virus tersebut dengan kata lain, sel hidup yang sehat sebagai program asal kemudian virus masuk menyebabkan program tersebut berfungsi sesuai dengan instruksi

24. Ibid. Hal. 15.
25. Ibid.

-instruksi yang ada dalam virus, tentu saja gejalanya menjadi tidak sehat persis seperti pada sel tubuh manusia yang sehat kemudian dimasuki dan virus-virus tersebut beraksi mengakibatkan sel-sel tersebut tidak berfungsi normal dan mengakibatkan sakit pada manusia.

Demikian juga dengan komputer ketika program sehat terinfeksi virus akibatnya program tersebut menjadi tidak normal mengakibatkan gangguan terhadap operasi komputer. Bagaimana hal tersebut bisa terjadi ? virus masuk dan mengkopi dirinya dalam bentuk suatu kode. ketika program dijalankan program Tersebut mengkopi virus tadi dan ini bisa terjadi hanya dalam suatu sistem tunggal karena virus tidak menginfeksi jaringan komputer. virus berkembang dan menyebar terhadap komputer harus dikopi secara fisik melalui disket dan ditransfer ke komputer lain.

Cacing komputer berdiam dalam program itu sendiri. cacing ini eksis tidak tergantung kepada program lainnya dan untuk menjalankannya tidak memerlukan program lain. cacing dengan mudah memperbanyak dirinya sendiri dalam satu komputer dan dapat menginfeksi komputer lainnya apabila terhubung dalam satu jaringan kerja yang sama. Disinilah perbedaan menyolok antara virus dan cacing. dimana cacing komputer menginfeksi komputer lainnya secara otomatis melalui jaringan komputer tanpa perlu dikopi secara fisik seperti halnya virus.

Berbagai macam virus banyak terdapat misalnya Virus *Michaelangelo* menyebabkan mesin macet dan kehilangan data atau menyebabkan gangguan yang tidak diharapkan dalam bentuk kode-kode yang berinteraksi dalam piranti lunak tertentu secara tidak normal. contoh lainnya adalah *Cacing pohon natal* yang menyerang sistem komputer IBM dan mengganggu kerjanya, cacing ini tidak merusak namun menyebabkan jaringan komputer terganggu sehingga perlu waktu untuk membersihkannya sehingga menyebabkan kehilangan produktivitas para penggunanya.

Cacing ini baru benar-benar merusak apabila masuk kedalam sistem dan seluruh jaringan dan menyebar serta memperbanyak diri, sehingga mengganggu dan komputer harus dimatikan untuk menghentikan infeksi.

(2) Salami attack (Serangan Salami).

Salami adalah salah satu tehnik yang secara otomatis menciptakan perubahan angka dan memindahkan angka *dari angka asalnya* yang lebih besar, termasuk salah satu penyalahgunaan komputer dibidang *data finansial* yang digunakan oleh pelakunya untuk memperkaya diri dan sejauh mungkin tidak dirasakan oleh korbannya. Penjelasan tehnik kejahatan ini adalah sebagai berikut, program jahat disisipkan dalam suatu program atau piranti lunak akunting dimana setiap angka yang bernilai Rp.100,- dihilangkan atau dibulatkan contohnya : apabila si A mempunyai tabungan dan tercatat

jumlahnya Rp.75.100,- angka tersebut secara otomatis dikurangi atau dibulatkan menjadi Rp.75.000,- sedangkan yang Rp.100,- secara otomatis dimasukkan kedalam rekening penjahat tersebut.

Tentunya korban tidak merasakan hal ini karena Rp.100,- itu sangat kecil, apabila korban mempunyai rekening dalam jumlah besar (jutaan rupiah). Namun penjahat tersebut (Kraker) akan mendapatkan untung besar dari ratusan nasabah yang mengadakan transaksi. apalagi jika program tersebut *waktu operasinya* diset setiap 24 jam artinya dalam setiap 1 X 24 jam dia akan bertambah rekeningnya 100 X jumlah nasabah yang ada (apabila nasabahnya ada 5000 orang maka setiap 24 jam rekeningnya akan bertambah 5000 X Rp.100 = Rp. 50.000.-).

(3) Bomb Logic (Bom Logika).

Bom logika mirip cara kerjanya dengan bom waktu (Timer bom) dimana bom tersebut disembunyikan kemudian *waktunya diset* dan meledak apabila tiba pada waktunya, bom logika komputer beraksi pada waktu-waktu tertentu yang telah ditentukan atau pada saat terjadi kondisi khusus tertentu contohnya beraksi pada saat hari Natal (25 Desember) atau setiap hari Minggu jam 24.00 kemudian contoh lainnya adalah beraksi pada saat pengguna komputer menjalankan instruksi print (cetak) atau menjalankan isntruksi copy.

Reaksi dari bomb logic apabila bekerja sangat bermacam-macam antara lain pada layar komputer tertulis kata-kata "*Kena*

kamu." atau menghapus data secara otomatis bahkan mematikan operasi komputer secara tiba-tiba sehingga penggunanya kehilangan data yang belum sempat direkam.

d. Breaches of Operations Security (Keamanan Operasional).

Keamanan operasi termasuk mengatur prosedur-prosedur preventif dan untuk mendeteksi seluruh gangguan pada sistem dan personil, namun sistem inipun tetap bisa direkayasa dan dicari kelemahannya. Cara-cara tersebut antara lain adalah sebagai berikut :

1) Data Diddling (Penipuan data).

Cara ini dengan memalsu atau memasukkan data secara tidak benar atau data dimodifikasi sebelum / setelah data dimasukkan ke dalam komputer, hal ini dilakukan agar pemalsu data mendapatkan keuntungan yang lebih dari yang seharusnya, dijelaskan oleh David Icove dkk. "Data diddling, sometimes called false data entry, involves modifying data before or after it is entered into the computer."[26]

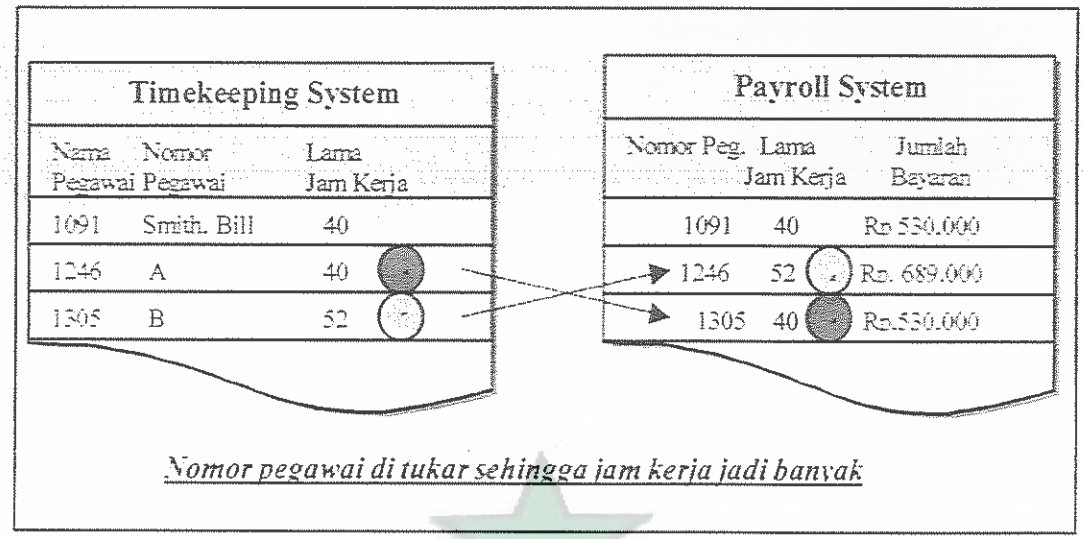
Contoh hal ini adalah sebagai berikut : seorang pencatat waktu dalam suatu perusahaan bekerja sama dengan A salah seorang pegawai untuk memanipulasi waktu kerja dengan cara. A bekerja selama 40 jam akan mendapat upah Rp. 530.000,- sedangkan B bekerja 52 jam akan mendapat upah Rp. 689.000,- oleh X data A dirubah seolah-olah bekerja 52 jam dan data B dirubah menjadi 40 jam sehingga A mendapat bayaran Rp.689.000,- (diuntungkan) keuntungan ini dibagi dua dengan X.

---

26. Ibid. Hal. 18.

Gambar. 7

Data diddling



2) Membohongi Internet protocol (IP Spoofing).

Metoda yang dipakai sama dengan Masquerading perbedaannya adalah yang menjadi sasaran Internet protocol pada satu jaringan internet yang berbasis pada program UNIX. sistem ini menjalankan program dengan mencari / melakukan otentifikasi terhadap individu-individu pengguna jaringan tersebut. Para Haker memalsukan adres pada paket data dengan mengirim data seolah-olah ia anggota dari dalam jaringan tersebut sehingga ia dipercaya dan menggunakan sistem tersebut tanpa ditanya lagi password atau otentifikasinya. Secara singkat cara ini adalah menggunakan metode menembus sistem dari luar. dijelaskan oleh David Icove sebagai berikut :

> "A method of masquerading that we're seeing is various Internet attacks today is known as IP spoofing (IP stands for Internet Protocol. one of the communications protocols that underlies the Internet). Certain UNIX programs grant access based on IP addresses essentially. the system running the program is authenticated . rather than the individual user.

> The attacker forges the addresses on the data packets he sends so they look as if the came from inside a network on which systems trust each other. Because the attacker's system looks like an inside system. he is never asked for a password or any other type of authentication. In fact, the attacker is using this method to penetrate the system from the outside."27

3) Mengintip Password (Password Sniffing).

Para pengintip password ini caranya sangat sederhana mereka mengumpulkan 128 bytes atau lebih dari jaringan – jaringan komputer yang berhubungan dan dapat termonitor. apabila salah satu pemakai dan menggunakan passwordnya untuk memanfaatkan layanan internet seperti FTP atau Telnet mereka, mengumpulkan password tersebut juga informasi lainnya kemudian menggunakannya sesuai dengan dengan keperluan mereka (biasanya mengambil password-password yang tidak di samarkan). Dijelaskan oleh David Icove dkk, sebagai berikut :

> "Password sniffers are able to monitor all traffic on areas of a network. Crakers have installed them on networks used by system that they espicially want to penetrate. like telephone systems and network providers. Password sniffies are program that simply collect the first 128 or more bytes of each network connection on the network that's being monitored."28

4) Memindai (Scanning).

Tehnik inilah yang biasa digunakan oleh Kraker pemula disebut cara skaning atau perang mendial nomor telpon (War dialing) juga salah satu cara untuk mengetahui bagus tidaknya pertahanan dari sistem keamanan operasi . prinsipnya adalah menggunakan program untuk menghubungi nomor-nomor telpon secara acak dan mencatat nomor telepon yang merespon dihubungi.

---

27. Ibid. Hal. 18.
28. Ibid.

mereka menggunakan list nomor telpon, list password atau nomor kartu telpon panggil kemudian dipindai terus menerus sampai mendapat respon , dijelaskan oleh David Icove dkk, sebagai berikut :

> "With scanning, a program known as a war dialer or demon dialer processes a series of sequentially changing information, such as a list of telephone numbers, passwords, or telephone calling card numbers. It tries each one in turn to see which ones succeed in getting a positive response."29

Contoh dari tehnik ini adalah sebagai berikut telpon BCA untuk transaksi dirahasiakan akan tetapi dapat diperkirakan nomornya berada antara nomor 741-0000 s/d 741-1000, para Kraker memindai nomor tersebut dengan suatu program khusus dari nomor 0000- s/d nomor 1000.

Dilihat fakta-fakta tersebut diatas dapat diketahui kejahatan komputer modusnya ada 2 *macam* yaitu : menyerang *secara fisik* dan menyerang *piranti lunaknya*. Haking komputer adalah jenis yang kedua dan menyerang sistem komunikasi data serta sistem keamanan operasi. kedua sistem ini berada pada medium cyberspase (Internet) sehingga kejahatan ini lebih populer disebut cybercrime. Internet terus berkembang berbagai aplikasi baru muncul (fasilitas baru) antara lain : remote Login, File transfer protocol, Electronic mail dan Website. Aplikasi-aplikasi tersebut sangat rentan terhadap Haking, Preking juga Kraking, karena modus kejahatan-kejahatan ini menggunakan Internet sebagai media utamanya.

Spektrum cybercrime tersebut antara lain : Data diddling, Password Sniffing, IP Spoofing, beberapa cara yang lebih spesifik antara lain : Trojan horse, Session hijacking, Tunneling, Timing attack dan Trap doors. Beberapa program perusak yang biasa digunakan para Haker antara lain : Viruse, Worm, Salami attack dan Logic bomb. Artinya Haking, Kraking dan Preking meliputkan segala sesuatu yang termasuk dalam spektrum cybercrime.

---

29. Ibid. Hal. 20.

MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

Bab. IV

BAB IV

HAKING KOMPUTER DAN PERKEMBANGANNYA

13. Profil, Budaya dan jaringan pelakunya.

Perkembangan haking komputer di luar negeri sangat pesat demikian juga di Indonesia, ini sangat berbeda dibandingkan dengan kejahatan biasa seperti perampokan. Contohnya : perampokan Bank di kota New York tidak akan ada pengaruh dan hubungannya dengan perampokan Bank di kota Jakarta, tetapi haking komputer di NewYork mempengaruhi haking komputer di Indonesia, sebab para haker di New York dapat secara langsung menyerang *website* yang ada di Indonesia.

Karena itu perlu untuk mengetahui perkembangan haking komputer di luar Indonesia, berikut ini dibahas apa itu Hacking (haking), Cracking (kraking) dan Phreaking(preking), Profil para pelaku, Budaya para haker serta Jaringan para haker.

a. Haking, Kraking dan Preking.

Haking merupakan suatu *seni* dalam menembus sitem komputer untuk mengetahui seperti apa sistem tersebut dan bagaimana berfungsinya. sebagaimana dikatakan Revelation Loa-Ash :

> "Hacking is the act of penetrating computer system to gain knowledge about the system and how it works. Hacking is illegal because we demand free acces to ALL data, and we get it. This pisses people off and we are outcasted from society, and in order to stay out of prison, we must keep our status of being a hacker / phreaker a secret."30

Haking adalah illegal karena masuk dan membaca data seseorang dengan tanpa ijin dengan cara sembunyi-sembunyi sama saja dengan *pissing people off* atau membodohi

---

30. Loa-Ash Revelation. Ibid. Hal 3

orang, sehingga para haker / preker selalu menyembunyikan identitas mereka. Namun apabila didalami tidaklah demikian, karena dilingkungan para haker ada budaya dan aturan-aturan tertentu, serta mempunyai motif dan tujuan yang berbeda, disebutkan oleh *pakar haker* Emmanuel Goldstein dari Amerika Serikat bahwa :

> "One of the common misconceptions is that anyone considered a hacker is doing something illegal. It's a sad commentary on the state of our society when someone who is basically seeking knowledge and the truth is assumed to be up to something nefarious. Nothing could be further from the truth.
> Hackers, in their idealistic naivete, reveal the facts that they discover, without regard for money, corporate secrets or government coverups"31

Walaupun illegal para haker tidak seluruhnya jahat, haker yang baik motivnya hanya untuk mencari tantangan dan kesenangan saja, membuktikan dirinya mampu menembus system, dikatakan Eric Steven Raymond :

> "Being a hacker is lots of fun, but it's a kind of fun that takes lots of effort. The effort takes motivation. Successful athletes get their motivation from a kind of physical delight in making their bodies perform, in pushing themselves past their own physical limits. Similarly, to be a hacker you have to get a basic thrill from solving problems, sharpening your skills, and exercising your intelligence."32

menjadi haker sangat menyenangkan, dan akan memperoleh pengetahuan dasar-dasar memecahkan masalah, meningkatkan keterampilan serta mempertajam kepandaian .

Haker seperti itu disebut *Real hacker* atau haker sejati (baik). Ilustrasi dari kebaikan mereka adalah sebagai berikut :

> "There is a community, a shared culture, of expert programmers and networking wizard that traces its history back through decades to the first time-sharing minicomputers and the earliest ARPAnet experiments. The members of this culture originated the term 'hacker'. Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work. If you are part of this culture, if you have

---

31. Goldstein Emmanuel. *Q & A with Emmanuel Goldstein of 2600: The Hacker's Quarterly*. [Online]. hal 1. Tersedia : http://cnn.com/TECH/specials/hackers/profiles/goldstein.html. [15 Februari 2000].

32. Raymond Eric Steven. *How To Become A Hacker*. [Online]. hal 3. Tersedia : http://www.tuxedo.org/~esr/faqs/hacker-howto.html. [24 Desember 2000].

contributed to it and other people in it know who you are and call you a hacker, you're a hacker."33

Sejak eksperimen ARPAnet, para haker ikut membangun internet, membuat piranti lunak Unix dapat secanggih sekarang, mereka juga meluncurkan Usenet dan membuat World Wide Web (WWW) bekerja dengan baik. Memang dalam perkembangannya muncullah Kraker yang merusak sistem, menyebarkan program-program Trojan Horse atau mengambil keuntungan finansial. Kemudian muncul *Preker* dalam Net Mag dijelaskan : " Phreaking is basically hacking with a telephone. Using different "boxes" and "tricks" to manipulate the phone companies and their phones, you gain many things, two of which are : knowledge about telephones and how they work, and free local and long distance phone calls."34

Preking adalah *Haking dengan telepon*, menggunakan berbagai box telepon yang berlainan dan cara-cara tertentu, dengan motif untuk *mengetahui* bagaimana jaringan telepon tersebut bekerja dan *mencuri pulsa* agar bebas membayar dalam melakukan perkacapan lokal atau perkacapan jarak jauh (interlokal / keluar negeri). Cara-cara Haker sama dengan Kraker yang berbeda adalah *motivasinya*, (Kraker merusak dan mencuri). Preker motivasinya sama dengan Kraker yang berbeda adalah cara dan sasarannya. Kraker sasarannya jaringan komputer serta piranti lunaknya sedangkan Preker sasarannya jaringan telepon serta piranti lunak pencatat pulsa telepon.

Sebenarnya Haker (sejati) bisa dijadikan pamer para penyidik Polri dalam upaya menyidik para Kraker dan Preker serta menyeretnya ke meja hijau, karya Haker sejati yang diakui semua orang antara lain :

---

33. Ibid. Hal 2.
34. NetMag . Ibid. Hal 3.

1) Menulis sumber piranti lunak terbuka (open source software) yang tidak komersil sehingga siapapun dapat memanfaatkan dan mengembangkannya, antara lain piranti lunak **Demigods** (manusia setengah dewa) dimana setiap orang dengan bebas menulis secara luas dan menggunakannya.

2) Membantu mengetes kelemahan-kelemahan piranti lunak terbuka.

3) Mempublikasikan informasi-informasi yang berguna dalam BBS's dan FAQs (Frequently Asked Questions lists).

4) Membantu agar infra struktur jaringan komputer tetap berjalan dengan baik.

Para Haker sejati banyak di rekrut oleh perusahaan-perusahaan komputer untuk meningkatkan sistem keamanan jaringan komputernya dan produk piranti lunak sebelum diedarkan. diantaranya *Kevin Mitnick* mantan kraker yang pernah menjadi buronan FBI serta pernah di penjara selama beberapa tahun, sekarang mendirikan perusahaan untuk mengamankan jaringan komputer.

Kotak dialog : 1

Apakah berbuat baik itu harus dengan cara legal ? (Apakah illegal jahat ?).

Suatu malam sepasang suami istri bermesraan dikamarnya, tanpa disadari seekor ular kobra diatas ranjangnya sewaktu-waktu bisa mematuk mereka. Seorang haker mengetahuinya dan secara diam-diam tanpa dilihat masuk kekamar dan membunuh ular kobra tersebut, kemudian secara diam-diam pula haker itu keluar dari kamar. Mereka menyebutnya haker baik karena menyelamatkan seseorang dari bahaya, memang ia masuk tanpa ijin (karena *kalau minta ijin ! namanya bukan haker lagi*). Jelas bahwa si haker illegal tetapi apakah ia jahat ?

seorang haker menyusup pada jaringan komputer Bank (BCA), kemudian ia memperbaiki kebocoran tersebut secara diam-diam, dan dilakukan test debugging sampai benar-benar aman, lalu ia diam-diam keluar dari sistem tersebut dan sebelumnya jejak-jejak dia dihapus. Network BCA itu sekarang keamanannya lebih baik. Haker mengetahui rekening nasabah tapi tidak diseberkan dan dimanfaatkan. Orang ini disebut Real haker, ia illegal masuk tanpa ijin, membaca data rahasia, memperbaiki sistim dan keluar diam-diam tanpa jejak, apakah ia jahat ?

Inilah *hal yang mendasar* harus diketahui para penyidik Polri, membedakan dengan jelas Hacker, Cracker dan Phreaker. Cracker apabila sudah masuk akan merusak sistim, atau mencuri rekening orang atau menyeberkannya seperti kasus "Rekening Andi Ghalib" beberapa waktu silam.

b. Profil para pelaku.

Para Haker profilnya tidak menyeramkan seperti umumnya para perampok dan tidak juga trendi / berdasi dan berjas seperti umumnya pelaku white collar crime, dari segi umur juga beragam mulai dari anak SMP umur 13 tahun sampai kakek-kakek berumur 65 tahun. Status merekapun beragam bisa pelajar, ibu rumah tangga, Direktur suatu perusahaan, pejabat tinggi pemerintah bahkan seorang Polisi. Namun ada beberapa *karakter umum* yang menjadi ciri-ciri dari para Haker, antara lain :

1) Pemuja kesenangan.

Para Haker kalau berhasil membobol suatu situs (Website) atau jaringan komputer yang diamankan secara canggih, akan sangat gembira juga bangga, apalagi bila data-datanya sangat menarik, *berharga* dan *tinggi nilai* kerahasiaannya, para Haker selain mencari kesenangan mereka juga menguji dan mengasah otaknya masing-masing.

2) Manusia-manusia kreatif.

Melakukan Haking perlu kreativitas yang tinggi, karena sumber daya mereka biasanya terbatas namun harus berhadapan dengan masalah-masalah yang menantang dan sukar, dikatakan oleh Eric Steven Raymond : "Creative brain are valuable, limited resource. They shouldn't bewasted on reiverting the wheel when there are so many problem waiting out there:"[35]

3) Ulet dan bukan pembosan.

Seorang Haker perlu duduk berjam - jam di depan komputernya, sering melakukan pekerjaan yang berulang-ulang dan membosankan. Sehingga syarat menjadi seorang Haker adalah harus ulet dan tidak mudah bosan, mereka

---

35. Raymond Eric Steven. Ibid. Hal 7.

kadang-kadang perlu 48 jam didepan komputer hanya untuk memecahkan password, atau mengamati lalu-lintas data / kegiatan yang berlangsung pada suatu jaringan komputer. Keuletan dan kesabaran para Haker sangat menonjol dan merupakan ciri khas dari kelompok ini, terutama dalam hal mencari cara-cara baru. .

4) Menginginkan kebebasan absolut.

Mereka adalah tipe manusia yang *apabila dilarang* justru malah melakukan. atau bila disuruh malah diam. Birokrasi dan otoritas dari pemerintah yang selalu membuat sensor dan banyak merahasiakan sesuatu, *sangat dibenci* oleh mereka dan bila diperlakukan seperti ini akan dengan sekuat tenaga mereka tembus.

> " There are only two ways to get rid of Hackers and Phreakers. One is to get rid of computers and telephone. in wich case we would send other means of getting what we want. (Like that in really going to happen). The other way is to give us what are want. wich is free access to all information. ***Until one of those two things happen, we are not going any where***"[36]

Mereka dengan tegas mengatakan bila belum mendapatkan akses yang bebas ke seluruh informasi. mereka tidak akan kemana-mana dan akan terus ngotot sampai mendapatkannya.

Dalam perkembangannya para Haker tidak hanya terbatas para remaja walaupun mereka mayoritas. bisa saja para gadis dan anak kecil. Namun sebagian besar para Haker *berasal dari dalam* perusahaan atau organisasi mereka sendiri yang menggunakan suatu jaringan komputer tertentu. fakta menunjukkan bahwa serangan dari dalam organisasi lebih hebat dari pada yang dari luar organisasi. Berdasarkan survey yang dilakukan Charles Palmer . diketahui bahwa :

---

36. Loa-Ash Revelation. Ibid. Hal. 3.

> "No longer are hackers limited to the teen-age, soda-slurping misfits, although they're probably the majority. There are girls and even younger kids. Many companies think all hackers come from outside, but surveys continue to show that the threat from inside an organization is greater than from outside."37

Profil-profil dan sifat mereka harus dikuasai oleh para penyidik Polri agar mereka dapat secara tajam melokalisir para tersangka dari berbagai macam tersangka, ketajaman ini diperlukan agar tidak salah sasaran dan agar tehnik / taktiknya tepat dalam menangani tersangka para Haker.

c. Budaya para Haker.

Para Haker adalah suatu komunitas bagian dari masyarakat mereka mempunyai aturan / adat yang berlaku diantara mereka, bahasa tertentu yang dipakai untuk bergaul serta sarana (media) untuk berkomunikasi, menurut Eric Steven Raymond :

> "The hacker culture' is actually a loosely networked collection of subcultures that is nevertheless conscious of some important shared experiences, shared roots, and shared values. It has its own myths, heroes, villains, folk epics, in-jokes, taboos and dreams. Because hackers as a group are particularly creative people who define themselves partly by rejection of normal values and working habits, it has unsually rich and conscious traditions, and of inclusion and exclusion."38

Para Haker saling membagi pengalaman-pengalaman yang penting mempunyai mitos, pahlawan, penjahat atau cerita-cerita yang hidup diantara mereka, banyolan-banyolan, tabu-tabu dan impian-impian yang mereka dambakan. karena mereka adalah kelompok manusia kreatif dan *mendefinisikan dirinya* sebagai kelompok yang berada diluar nilai-nilai serta kebiasan yang normal. Adapun bagian dari budaya mereka tersebut adalah sebagai berikut :

1) Aturan berlaku dikalangan para Haker / Preker :

a) Jangan pernah merusak sistem komputer, karena akan menyebabkan masalah bagi anda.

---

37. Palmer. Charles.C. Dr. Ibid. Hal. 3.
38. Raymond Eric Steven. *Jargon File Resources*. [Online]. Hal 2. Tersedia : http://www.tuxedo.org/~esr/jargon/jargon.html. [24 Desember 2000].

b) Jangan merubah dan menukar sistim arsip (file) kecuali sangat diperlukan, serta dijamin tidak akan terdeteksi.

c) Jangan membagi informasi tentang proyek / kegiatan Haking anda pada seseorang yang kurang dapat dipercaya.

d) Ketika menyebarkannya di BBS's (Bulletin Board System) lakukan penyamaran (vague) sebaik mungkin, karena BBS's dapat dimonitor oleh para penegak hukum.

e) Jangan menggunakan nama asli dan telepon nomor yang sebenarnya ketika menyebarkannya di BBS's.

f) Jangan meninggalkan ciri-ciri / jejak anda pada suatu sistem yang sedang anda lakukan Haking.

g) Jangan melakukannya terhadap sistem komputer pemerintah.

i) Jangan pernah membicarakan proyek Haking dengan menggunakan jalur telepon rumah (bisa disadap penegak hukum).

j) Jadilah paranoid, simpan dengan baik seluruh bahan-bahan Haking di tempat yang tersembunyi dan aman.

k) Untuk menjadi seorang Haker yang baik anda harus banyak melakukannya (praktek), tidak dapat hanya duduk saja membaca dan membiarkan BBS's begitu saja.

l) Jangan menggunakan box telepon jalur rumah anda.

m) Jangan pernah membiarkan bahan-bahan Preking diluar secara terbuka, simpan di tempat yang aman.

n) Jangan sampai tertangkap.

Aturan - aturan ini cukup ditaati oleh mereka karena kalau tidak mereka akan dikucilkan dianggap tidak taat aturan (dianggap membahayakan

kelompoknya), mereka patuhi takut ditangkap atau diketahui oleh orang lain yang akan merugikan mereka. *Aturan-aturan inilah* yang menyebabkan kenapa para Haker, Kraker dan Preker sulit dideteksi dan disidik , sehingga *harus dimengerti serta dipahami* oleh para penyidik Polri agar tahu secara pasti bagaimana menyidiknya.

2) Bahasa para Haker.

Para Haker mempunyai bahasa tersendiri biasanya mereka menggunakan slang (bahasa para preman / kasar) serta mempunyai tata bahasa yang khusus, gunanya agar para Haker mengenal satu dengan yang lainnya. Dengan bahasa tersebut mereka dapat mengetahui apakah seseorang itu dari luar kelompoknya, atau sebagai pendatang baru yang belum menguasai bahasa mereka secara benar. Sebagaimana yang dikatakan oleh Eric Steven Raymond sebagai berikut :

> "As usual with slang, the special vocabulary of hackers helps hold their culture together – it helps hackers recognize each other's places in the community and expresses shared values and experiences. Also as usual, not knowing the slang (or using it inappropriately) defines one as an outsider, a mundance or (worst of all in hackish vocabulary) possibly even a suit. All human cultures use slang in this threefold way – as a tool of communication and of exclusion."[39]

Adapun struktur bahasa mereka tersebut adalah sebagai berikut :

a) Verb Doubling / Tripling (menggandakan kata).

Berikut ini adalah contoh menggandakan dari kata lose, flame dan chomp :

> "The disk heads just crashed." "Lose, lose."
> "Mostly he talked about his latest crock. Flame, flame."
> "Boy, what a bagbiter ! Chomp, chomp !"

---

39. Raymon Eric Steven, Ibid. Hal 2.

mereka mengatakan *pembaca disk* baru saja rusak dan datanya hilang (lose), mereka tuliskan sebanyak dua kali (lose, lose), begitupun dengan kalimat lainnya.

b) Soundalike slang (menggunakan slang).

Para Haker biasanya menggunakan ritme tertentu untuk merubah bahasa baku menjadi sesuatu yang lebih menarik atau dibumbui, contohnya sebagai berikut :

Data general --- Dirty Genitals
IBM 360 ------- IBM Three-Sickly
Government Property --- Do Not Duplicate (on key)
Government Duplicity --- Do Not Propagate
For historical reasons --- for hysterical raisins
Microsoft ---------- Microsloth
Internet Explorer --- Internet Exploiter

Mereka merubah *data umum* menjadi kelamin kotor, *IBM 360* menjadi IBM tiga-tiganya sakit , *milik pemerintah jangan digandakan* menjadi gandakan pemerintah jangan *dipropaganda*, *alasan menurut sejarah menjadi rasa histeris*, *piranti* lunak mikro diganti menjadi si kecil tolol.

c) The P convention (menggunakan hurup *P*).

Berikut ini dalam suatu perkacapan dan seseorang menanyakan (Q) lokasinya, kemudian orang yang ditanya (A) tersebut menegur karena menanyakan lokasi secara jelas adalah hal yang *tabu* !.

Q : "State-p Florida?"
A : "Been reading JARGON.TXT again, eh?"

Seorang Haker menanyakan kepada Haker lainnya apakah anda di Negara Bagian Florida ? , kemudian dijawab dengan kesal Haker oleh yang ditanya, *eh baca lagi JARGON TXT !*. Dapat diketahui

bahwa penanya adalah seorang Mundance (makluk asing / aneh yang baru belajar), belum menguasai bahasa para Haker.

d) Overgeneralization (generalisasberlebihan).

Para Haker sangat menyenangi mengubah tingkat gramatikal kata (kalimat) dibuat secara umum dan dilebih-lebihkan, terutama dengan menambah *akhiran-akhiran yang salah* agar menjadi kata benda atau kata kerja. Contohnya sebagai berikut :

Mysterious => mysteriosity
Ferrous => ferrosity
Obvious => obviosity
Dubious => dubiosity

e) Spoken inarticulation(berbicara tanpa artikulasi jelas).

Kadang-kadang mereka menggunakan kata-kata / huruf yang tidak mempunyai artikulasi seperti suara seseorang menarik nafas panjang, mengeluh atau mengerang. Contohnya sebagai berikut :

Hhhh ... (mendesah / kesal)
Grrrr !!! (mengerang)
Ssshh ...(menarik nafas panjang)

Dari bahasanya tersebut dapat diketahui bahwa Haker adalah kelompok yang eklusif sangat peka terhadap pendatang baru atau orang asing, mereka tidak begitu saja menerima pendatang baru bahkan cenderung menolak orang asing tersebut. Bahasa mereka pada saat melakukan *chating* di depan komputer *digunakan* pula pada saat mereka berkumpul secara rahasia pada suatu tempat tertentu, di Mal /Supermaket atau disudut tertentu di kampus mereka.

Apabila seorang penyidik melakukan *undercover* (penyamaran) untuk masuk ke dalam grup mereka dengan cara chating terlebih dahulu akan tetapi *tidak mengusai bahasanya*, maka ia akan segera dianggap sebagai *Alien* dan

ditolak untuk masuk ke grup tersebut. Akan tetapi apabila ia menguasai bahasanya, diharapkan dalam melakukan chating dapat diterima dan tidak dicurigai (*in group*), maka selanjutnya akan bisa mengikuti pertemuan-pertemuan sesungguhnya diluar meja komputer.

3) Strata Sosial para Haker.

Komunitas suatu masyarakat yang berbudaya pasti mempunyai strata sosial namun dalam budayannya mereka tidak mengenal adanya pemimpin *semuanya statusnya sama* , tetapi mereka mempunyai pahlawan jadi idola, aliran / kelompok (Tribalisme), serta juru bicara dan penulis hikayat atau risalah (historian).

Tempat yang paling terhormat bagi mereka bukanlah menjadi pimpinan akan tetapi menjadi idola dan tempat bertanya (dianggap sebagai Begawan / Guru besar), menjadi anggota yang baik dan diterima oleh kalangan mereka secara penuh merupakan hal yang *sangat diidam-idamkan* oleh kelompok ini. Ada beberapa aturan tak tertulis agar dengan tangan terbuka diterima oleh masyarakat Haker, antara lain sebagai berikut :

a) Jangan menggunakan nama yang hebat atau menyebalkan sebagai *User ID* atau *Screen name*.

b) Jangan mengobarkan peperangan dalam *Usenet* atau dimanapun juga.

c) Jangan menyebut diri sendiri sebagai *Cyberpunk*, dan jangan pula menghabiskan waktu dengan seseorang yang seperti ini.

d) Jangan mengirim (posting) atau menulis e`mail penuh dengan kata / huruf yang salah dan tata bahasa yang buruk, hal ini sangat wajar karena bila suatu *program* salah titik koma

saja apalagi huruf akan berakibat program tidak jalan dan perlu melakukan tes Debuging atau harus melakukan tes untuk mencari kutu (kesalahan). Tentunya hal ini akan sangat mengesalkan bagi penerima e'mail karena seolah-olah diberikan informasi / program yang salah.

Karakter dan hobi mereka sama dan perlu hal ini diperhatikan , supaya cepat diterima dan masuk dalam kelompok mereka . ada beberapa kiat agar dapat dengan cepat diterima antara lain sebagai berikut :

a) Selalu belajar menulis dengan baik dan menggunakan bahasa Inggris dengan baik (walaupun mereka mempunyai bahasa khusus), banyak ditemukan para Haker yang baik mempunyai kemampuan menulis yang baik pula.

b) Mengembangkan apresiasi terhadap permainan-permainan kata dan kata-kata sindiran atau kata-kata yang sangat lucu, sehingga membuat orang senang atau tertawa (seorang Haker adalah seorang humoris juga).

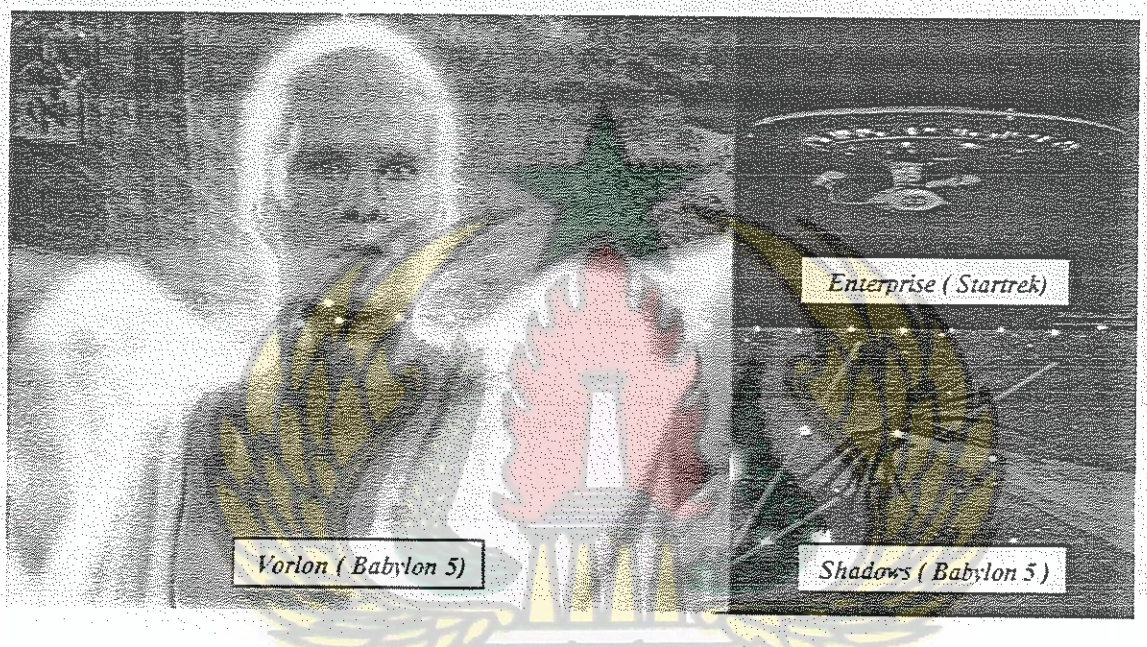
c) Menyenangi musik serta menghargai musik.

d) Membaca dan menonton cerita-cerita fiksi ilmiah (Science fiction) bahkan dianjurkan untuk pergi ke konvensi-konvensi / seminar yang membahas Science fiction hal ini merupakan jalan terbaik untuk bertemu dengan para Haker senior dan para Haker pemula. Mereka sangat menyenangi cerita film seperti Star trek juga sangat mengagumi Starship Interprise. akhir-akhir ini mereka menyenangi Vorlon dan The Shadows dalam cerita fiksi *Babylon 5*. biasanya mereka maniak computer game.

Apabila pada suatu seminar atau gedung bioskop ditayangkan hal-hal seperti tersebut diatas dapat dipastikan *sebagian dari yang hadir* adalah para Haker baik yang senior ataupun pemula, media tersebut digunakan juga oleh mereka untuk berkomunikasi dan saling bertukar informasi / pengalaman.

Gambar . 8

Tokoh dan Model Siencefiction idola para Haker



Dapat disimpulkan bahwa para Haker dalam kebudayaannya terutama dalam strata sosialnya tidak mengenal adanya pemimpin, mereka hanya mengenal idola dan pahlawannya, serta para penutur hikayat (historian) dan sebagai anggota kelompok namun status mereka sama atau sejajar. Apabila ingin diterima oleh mereka, diakui dan dijadikan kelompoknya perlu mengadaptasi karakter tertentu dan hobi mereka.

d. Jaringan para Haker.

Para Haker saling berhubungan dengan membentuk suatu *Nerd Connection*.

dalam aktifitasnya mereka sering menggunakan *terminologi Harsher* (kasar, lalim dan kejam) serta *Geek* (orang yang belum ahli / masih bodoh) sebagai suatu *Badge* atau lambang kebanggaannya. Haker pemula disebut *Newbies* , mereka membentuk jaringan informasi untuk saling meningkatkan kemampuan mereka. Adapun jaringan-jaringan tersebut adalah sebagai berikut :

1) World Wide Web site para Haker dan Preker.

Berikut ini adalah data Website yang di dalamnya terdapat media para haker dan preker. adapun alamat situs tersebut adalah sebagai berikut :

http://www.attrition.org
http://www.outerlimits.net/lordsome/index.html
http://web2.airmail.net/km/hfiles_free.html
http://www.rit.edu/~jmb8902/hacking.html
http://pages.prodigy.com/FL/drgz94a/files2.html
http://www.2600.com
http://draco.centerline.com:8080/~fran1/crypto.html

beberapa Website terbaik antara lain adalah http://www.attrition.org , http://www.2600.com dan http://www.outerlimits.net/lordsome/index.html.

2) Text Files para Haker dan Preker.

Berikut ini adalah kumpulan text files para haker dan preker yang terbaik dan dapat di download secara mudah dari internet :

A Novice's Guide To Hacking
Alt.2600 Hack Faq
The Hacker's Handbook
The Official Phreaker's Manual
The Hacker Crackdown
The Ultimate Beginner's Guide To Hacking And Phreaking
Computer Hackers : Rebels With A Cause

3) Majalah para Haker dan Preker.

Berikut ini adalah kumpulan majalah para haker dan preker yang terbaik seluruhnya diterbitkan di Negara Amerika Serikat ;

Pharck Magazine

2600 Magazine

Tap Magazine

Phantasy Magazine

4) Gopher site para Haker dan Preker.

Berikut ini adalah kumpulan Gopher site para haker dan preker yang terbaik :

Gopher.Ba.com

Gopher.Csrc.ncsl.nist.gov

Gopher.acm.org

Gopher.Spy.org

Gopher.Wiretap.spies.com

5) Ftp site para Haker dan Preker.

Berikut ini adalah kumpulan Ftp site para haker dan preker yang terbaik :

ftp.2600.com

ftp.agl.gatech.edu/pub

ftp.asylum.sf.ca.us

ftp.clark.net/pub/jcase

ftp.armory.com/pub/user/kmarmind

ftp.fc.net/pub/defcon/BBEEP

ftp.fc.net/pub/phrack

ftp.giga.or.at/pub/hacker

6) Bulletin Board System para Haker dan Preker.

Berikut ini adalah kumpulan *Ftp site* para haker dan preker yang

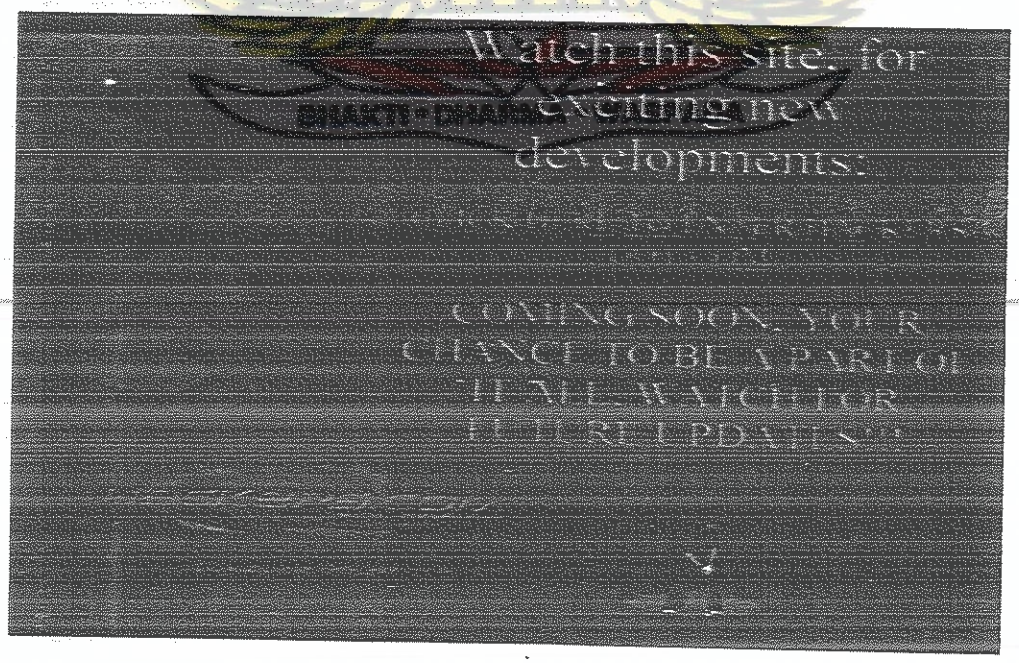
Dianggap terbaik selama tahun 2000 :

Kode area :	Nomor telepon :	Nama :
203	832-8441	Rune Stone
303	343-4053	Hacker's Haven
315	656-5135	Independent Nation

Banyak sekali para Haker dan Preker yang handal diantara mereka ada yang sangat kooperatif untuk diajak kerja sama, mereka bisa dihubungi melalui jaringan para Haker dan Preker diatas, antara lain ; Silicon Toad, Logik Bomb/Net Assasin, Ole Buzzard, Lord Somer dan Weezel. Jaringan para Haker / Preker tersebut merupakan media untuk berekspresi serta mengakumulasikan kemampuan para Haker / Preker, dilengkapi lagi dengan media berupa *cerita film*. Antara lain yang terkenal adalah cerita film yang berjudul *Hackers, War game* dan *The Netters*. Dengan mengetahui dan menguasai jaringan – jaringan tersebut diharapkan para penyidik Polri akan lebih memperdalam pemahaman terhadap kelompok para Haker / Preker yang dihadapinya.

Gambar . 9

Haker.Com Website Haker Terkenal



14. **Tehnis / Modus Operandi dan dampak Haking komputer.**

Pada bagian ini akan dibahas bagaimana seorang Haker pemula mulai belajar dan mencoba Haking, cara melakukan haking serta preking serta modus-modus yang menjadi kebiasaan atau favorit para Haker / Preker.

a. Dasar- dasar Haking / Preking.

Para Haker pemula belajar bagaimana cara membuat program, mendapatkan program / piranti lunak UNIX dari sumber terbuka di internet kemudian mempelajari bagaimana *menggunakan* dan *menjalankannya*. Selanjutnya belajar bagaimana menggunakan / memanfaatkan World Wide Wib site dan menulis HTML (Hyper Text Mailing List), adapun cara -cara tersebut adalah sebagai berikut :

1) Mempelajari dan membuat program.

Para Haker senior merekomendasikan Haker yunior yang sama sekali belum mengerti cara melakukan Haking, untuk mulai belajar dengan piranti lunak *Python* karena program ini sangat berbobot dan fleksibel serta paling mudah. Bahasa lain yang perlu dipelajari adalah piranti lunak *Java*, mereka dianjurkan menggunakan program ini sebagai bahasa kedua.

Kemudia mempelajari *masalah-masalah dalam melakukan pemograman* serta bahasa program lainnya antara lain *Bahasa C+*, *Perl* untuk mempelajari mengaktifkan halaman Web dan sistem administrasinya serta *Lisp* untuk meningkatkan pengalamannya . Lalu meningkat ke UNIX dan LINUX yang merupakan basis dari operasinya internet atau jaringan kerja komputer (Computer Network). Maksudnya untuk meningkatkan keterampilan dalam *membaca* dan *menulis* kode-kode, karena pada hakekatnya program-program komputer adalah serangkaian kode-kode

2) Mendapatkan program / mempelajari UNIX.

Para Haker perlu mencari dan mendapatkan program UNIX dan LINUX karena hal ini merupakan piranti lunak sistem operasi internet. Dikatakan oleh Eric Steven Raymond, sebagai berikut : "While you can learn to use the Internet without knowing UNIX, you can't be an Internet hacker without understanding UNIX. For this reason , the Hacker culture today is pretty strongly UNIX-centered."[40]

Para Haker mendapat bahan-bahan ini dari sumber-sumber terbuka antara lain :

The Loginataka (pelajaran lanjutan UNIX).

Where can I get LINUX (untuk mendapatkan LINUX).

www.bsd.org (untuk mendapatkan BSD UNIX),

selain itu dapat juga dihubungi *Linux Internet Co-operative*, juga mencari di saluran *IRC* (Internet Relay Chat).

3) Menggunakan World Wide Web dan menulis HTML.

Website sekarang ini merupakan hal penting bukti dari hal tersebut adalah kasus ketika transkrip Berita Acara Pemeriksaan (BAP) Presiden Amerika Serikat : "*Bill Clinton vs Monica Lewensky*" disebar di BBS`s. juga di Indonesia BAP ex Presiden Suharto disebarkan di BBS`s .

Karena pentingnya mempelajari *Website* dan menulis *HTML*, mereka memulai dengan cara membuat *Homepage pribadi*, serta membuatnya agar menjadi semenarik mungkin. Kegiatan selanjutnya adalah melakukan *Listing* dengan menggunakan LINUX, dimulai dari *List ing 1* sampai dengan *Listing 4*

---

40. Raymond Eric Steven. Ibid. Hal 5.

Fungsi listing tersebut adalah sebagai berikut :

Listing 1 : untuk konfigurasi File Fetchmail.

Listing 2 : untuk Fetchmailrc.

Listing 3 : untuk Fungsi Metaclass.

Listing 4 : untuk kode memanggil Fungsi Metaclass.

Berikut ini *contoh listing 4* , yang lainnya tidak ditulis kerana terlalu panjang :

"Listing 4. Code that Calls Metaclass Function "[41]

```
# The tricky part – initializing objects from the
# configuration global
# Configuration' is the top level of the object
# tree we're going to mung
configuration = Controls ( )
Copy_instance (Configuration, configuration)
Configuration.servers = [ ] :
For server in configuration [ 'servers ' ] :
        Newsite – Server ( )
        Copy_instance (Newsite, server)
        Configuration.servers.append (Newsite)
        Newsite.users = [ ] :
        For user in server [ 'user' ] :
                Newuser = User ( )
                Copy_instance (Newuser, user)
                Newsite.users.append (Newuser)
```

Setelah para Haker pemula mampu menguasai hal - hal tersebut yang menjadi *dasar pengetahuan* untuk melakukan Haking, mereka meningkat mempelajari hal yang lebih tehnis lagi yaitu praktek Haking dan

---

41. Linux Journal. ***Metaclass Function.*** [Online]. Hal. 1. Tersedia : http://noframes.linuxjournal.com/lj-issues/issue73/3882l4.html . [24 Desember 2000].

Preking, berikut ini diuraikan tehnis-tehnis melakukan haking dan preking

b. Tehnis melakukan haking.

Secara *garis besar* para Haker melakukan aksinya atau haking, dilakukan dengan tahap-tahap sebagai berikut :

Langkah ke 1 : SCANNING.

Menjalankan program Scanner seperti yang telah dijelaskan sebelumnya untuk mendapatkan akses *root*, setelah itu menginstall backdoor (pintu belakang) dan menutup semua kelemahan umum yang ada.

Langkah ke 2 : ROUTER to BRIDGE.

Upaya menembus jaringan internal (intranet) dengan cara mengubah sebuah *Router* menjadi *Bridge* (Jembatan) , yang kemudian digunakan sebagai batu loncatan untuk masuk ke jaringan internal tersebut. Antara jaringan luar (internet) dan jaringan intranet perusahaan tersebut ditengahnya dibuat pengaman disebut *Firewall* atau *Proxy server*, untuk mencegah user illegal masuk ke jaringan intranet. Para Haker dapat mengakalinya dengan menembus mail *server external* selain itu, dengan menggunakan *Aggressive –SNMP scanner* dan program yang memaksa SNMP community string unutk mengubah sebuah router menjadi bridge (jembatan).

Langkah ke 3 : CLOACKING.

Untuk langkah berikutnya melakukan *cloacking* (penyamaran) dengan cara melompat dari mesin yang telah ditaklukkan (compromise) melalui program *Telnet* atau *RSH* , atau melompat dari program *Wingate* apabila mesin perantaranya menggunakan Windows atau melalui *perangkat Proxy* yang konfigurasinya kurang baik.

Langkah ke 4 : PROBING.

Para Haker dalam jaringan yang jadi korban serangannya melakukan Probing

(seolah-olah memasang pasak) , hal ini dilakukan setelah berhasil *melompat dan memasuki* sistem lainnya gunanya untuk mengumpulkan informasi-informasi yang dibutuhkan. Ada beberapa cara Probing tersebut adalah :

1) Menggunakan *nslookup* untuk menjalankan perintah *'ls <domain or network>'*.

2) Melihat file HTML di webserver, untuk mengidentifikasi mesin lainnya.

3) Melihat beberapa dokumen di beberapa server.

4) Menghubungkan diri ke mail server dan menggunakan perintah *'expn <user>'*.

5) Mem*finger* user di mesin-mesin eksternal lainnya.

Langkah ke 5 : WEAKNESS IDENTIFICATION.

Langkah selanjutnya para Haker mengidentifikasi komponen jaringan yang dipercaya oleh sistem apa saja, antara lain *mesin administrator* dan *server* (dianggap paling aman di jaringan) untuk mencari komponen *jaringan yang lemah* dan bisa ditaklukkan. Dimulai dengan check akses dan expor NFS keberbagai direktori yang kritis seperti /usr/bin./etc. dan /home. Eksploitasi mesin melalui kelemahan Common Gateway Interface (CGI), dengan akses ke file /etc/hosts.allow. Program yang digunakan antara lain adalah LINUX seperti *ADMhack, mscan, nmap* dan banyak scanner kecil lainnya. kemudian program seperti *'ps'* dan *netstat* dibuat Trojan.

Langkah ke 6 : PISSING DAEMON.

Setelah berhasil mengidentifikasi jaringan yang lemah dan bisa ditaklukkan selanjutnya para Haker akan menjalankan program untuk menaklukkan program *Daemon* (setan tersembunyi) yang lemah di server. Daemon adalah program di server yang biasanya berjalan di belakang layar , keberhasilan penaklukkan program ini akan memungkinkan seorang Haker memperoleh akses sebagai *root* (administrator

tertinggi di server) yang mempunyai *password supervisor*.

Administrator ini posisinya adalah orang yang memiliki *otoritas terluas dan tertinggi* untuk memanfaatkan, menggunakan atau merubah sistem komputer dalam organisasinya. Pada perusahaan-perusahaan umum biasanya yang menjadi administrator tertinggi di server adalah seorang Direktur atau Kepala bidang bagian informasi / telekomunikasi.

Langkah ke 7 : EXPLOITING.

Selanjutnya seorang Haker dapat menggunakan mesin yang sudah ditaklukkan untuk kepentingan sendiri misalnya membaca informasi sensitif yang seharusnya tidak dibacanya, memasang *Sniffer* untuk melihat dan mencatat berbagai lalu lintas komunikasi yang sedang berjalan. Pada titik inilah *(langkah ke 7)* para ***penyidik harus mengetahui perbedaan*** seorang Haker dengan Kraker. Kraker akan *melanjutkan* kegiatannya untuk melakukan *kraking (pengrusakan)* terhadap mesin lainnya dengan cara melompat dari mesin yang ditaklukkannya.

Biasanya mereka *mencuri informasi* kemudian memanfaatkannya atau menjualnya untuk kepentingan pribadi. Bahkan mematikan sistem / jaringan dengan cara menjalankan perintah *rm-rf/&*, akibatnya akan sangat fatal karena seluruh sistem akan hancur sama sekali semua software yang diletakkan di hardisk akan hancur dan diperlukan proses *reinstal* diseluruh sistem.

Langkah ke 8 : CLEANUP OPERATION.

Langkah terakhir adalah menghilangkan jejak dengan melakukan operasi pembersihan, dengan cara membersihkan berbagai *logfile* dan menambahkan program untuk masuk dari pintu belakang (*backdooring*), serta mengganti *file host di /usr/bin* untuk memudahkan akses ke mesin yang ditaklukkan melalui *rsh dan csh*.

Berikut ini ini *secara rinci* cara-cara para Haker melakukan aksinya : Pertama yang diperlukan adalah mendapatkan copy dari PKZIP atau piranti lunak lainnya untuk melakukan unzipping (Unziping utility) yaitu piranti lunak *untuk mengkompres dan mengembalikan hasil kompresi* pada bentuk semula.

Kemudian melakukan *Prefic Scanner*, pekerjaan ini disebut juga dengan pekerjaan *War dialer* yaitu menggunakan program yang secara otomatis melakukan dialing nomor-nomor telepon yang dimulai dengan 3 nomor terdepan (prefic) yang telah dispesifikasi terlebih dahulu. Gunanya adalah untuk mengetes dan melihat apakah nomor-nomor tersebut sebagai nomor pembawa informasi, kemudian berusaha terus untuk melakukan skaning pada area prefik nomor-nomor telepon yang sangat sibuk.

Biasanya menggunakan *autoscan* atau *a-Dial* karena sangat gampang digunakan serta bekerja secara cepat dan efisien. program-program seperti disebut dengan *Tools* (alat-alat), secara otomatis mendeteksi kelemahan-kelemahan *Host local* maupun *Host remote*, sehingga seorang user di New York dapat mengetahui secara langsung kelemahan sistem keamanan jaringan kumputer di Indonesia. Tools scanner ini digunakan untuk menyerang kelemahan *port TCP/IP* dan *servis-servisnya* (telenet, ftp, dan http), dan *mencatat responnya* dari komputer target.

Menurut pakar internet ITB Onno W. Purbo dan Tony Suhardjito ada beberapa Tools Scanner yang sangat sering digunakan oleh para Haker, berikut ini adalah alamat tempat scanner atau tools terbaik yang disenangi para Haker yang sangat mudah di akses melalu internet :

- SATAN (http://www.fish.com)
- JAKAL (http://www.giga.or.at/pub/hacker/unix)
- IdentTCPScan (http://www.giga.or.at/pub/hacker/unix)
- CONNECT (http://www.giga.or.at/pub/hacker/unix)

- XSCAN (http://www.giga.or.at/pub/hacker/unix)
- FSPScan (http://www.giga.or.at/pub/hacker/unix) " 42

Setelah melakukan skaning dan mendapat nomor-nomor telepon yang dapat digunakan untuk menembus suatu jaringan. kemudian langkah selanjutnya adalah dari terminal komputer Haker melakukan dialing sampai terdengar nada *Beep* yang artinya telah berhasil menyambung pada remotte komputer. Apabila tersambung akan tertulis seperti "CONNECT 9600 " selanjutnya segera sistem tersebut diidentifikasi. Apabila tidak terjadi apa-apa setelah ada tanda "CONNECT 9600 " . di coba lagi beberapa kali dengan menekan tombol enter. apabila tetap tidak berhasil segera dirubah *Parity-parity data bit. Stop bit. Baud rate* dan sebagainya sampai usaha tersebut berhasil.

Cara lain untuk menyambung ke remote komputer adalah melalui *Telnet* (network komputer yang luas) dengan cara sebagai berikut :

1) Dial salah satu telepon nomor yang sudah berada dalam list hasil dari skaning sebelumnya upayakan agar tersambung dari terminal.

2) Tekan tombol enter sampai keluar hurup "TERMINAL=" kemudian segera ketik pada terminal emulasi. apabila tidak tahu hal ini tekan lagi tombol enter sehingga keluar *prompt* seperti "@" .

3) Selanjutnya ketik "C" kemudian sambungkan ke NUA (Network User Address) yang anda kehendaki. setelah tersambung hal penting yang *harus segera ditemukan* adalah bagaimana tipe sistem tersebut yang sedang dijalankan(apakah UNIX. VAX/VMS. PRIME dan lain-lainnya).

---

42. Purbo W. Onno dan Wihardjito Tony. ***Keamanan Jaringan Internet.*** Elex Media Komputerindo. Jakarta. 2000. Hal. 10.

Telenet sangat digemari para Haker untuk memulai melakukan haking karena sangat aman, disebabkan oleh banyaknya nomor-nomor yang dipakai untuk berkomunikasi. Mereka melakukan komunikasi biasanya selama jam-jam sibuk (pagi hari atau sore hari), sehingga perbuatan mereka sulit diketahui karena pada saat itu banyak orang-orang online dalam Telenet tersebut.

Berikut ini adalah List beberapa Telenet Commands serta fungsi-fungsinya yang biasa dipakai para Haker :

Command	Function
C	Connect to a host.
Stat	Shows network port.
Full	Network echo.
Half	Terminal echo.
Telemail	Mail.(need ID and password)
Mail	Mail (need ID and password)
Set	Select PAD parameters
Cont	Continue.
D	Disconnect.
Hangup	Hangs up.
Access	Telenet account. (ID and password).

Berikut ini adalah nomor-nomor Telenet yang dapat dihubungi (hasil dari skaning secara illegal) yang berada di Negara Amerika Serikat termasuk negara bagian, kota dan area kode sebagai contoh dari nomor-nomor telenet yang *berhasil dicuri* oleh para Haker (data di Indonesia sangat sulit didapat karena para Haker lokal belum terorganisasi dengan baik / informasi-informasi belum tersusun dengan baik) :

State, City :	Area Code :	Number :
AL. Anniston	205	236-9771

AL, Birmingham	205	328-2310
AL, Decatur	205	355-0206
AL, Dothan	205	793-5034
AL, Florence	205	767-7960
AL, Huntsville	205	539-2281

Berikutnya para Haker melakukan haking berdasarkan pada piranti lunak UNIX karena sebagian operating sistem dalam Telenet juga memakai piranti-piranti lunak UNIX, mereka berusaha untuk mendapatkan *"S" prompt* atau beberapa karakter khusus lainnya, dibawah ini adalah contoh dari login dan passwordnya :

Login :	Password :
Root	root
Root	system
Sys	sys
Sys	system
Daemon	daemon
Uucp	uucp
Tty	tty
Test	test
Unix	unix
Unix	test
Bin	bin
Adm	admin
Sysman	sysman
Who	who
Learn	learn
Uuhost	uuhost
Quest	quest
Nuucp	nuucp
Rje	rje
Games	games
Games	player

Satu hal yang penting apabila sudah mendapatkan password-password tersebut segera direkam (save) dengan cara sebagai berikut : ***Cat /etc/passwd*** , apabila password tersebut tidak menampakkan diri digunakan password shadowing (bayangan) yang dapat diambil dari *alt : 2600*. password shadowing tersebut adalah sebagai berikut :

UNIX System Type :	**Path :**	**Toke :**
AIX 3	/etc/security/passwd	!
or	/tcb/auth/files/<first letter of username>/<username>	=
A/UX 3.Os	/tcb/files/auth/*	
BSD4.3-Reno	/etc/master.passwd	*
ConvexOS 10	/etc/shadpw	*
ConvexOS 11	/etc/shadow	*
DG/UX	/etc/tcb/aa/user	*
EP/IX	/etc/shadow	x
HP-UX	/.secure/etc/passwd	*
IRIX 5	/etc/shadow	x
Linux 1.1	/etc/shadow	*
OSF 1	/etc/passwd[.dir/.pag]	*

Para Haker harus mengerti bahwa karakter-karakter pada password aging data mengikuti aturan-aturan tertentu yaitu. *angka maksimum* setiap minggu passwordnya dapat digunakan tanpa ada perubahan. sedangkan *angka minimum* dalam setiap minggu passwordnya harus digunakan sebelum ada perubahan. beberapa password aging data dapat dibaca kembali (decoded) dengan menggunakan karakter dan nomor sebagai berikut :

Character	Number :	Character	Number
.	0	6	8
/	1	7	9
0	2	8	10
1	3	9	11
2	4	A	12

Character	Number :	Character	Number
3	5	B	13
4	6	C	14
5	7	D	15

Apabila langkah-langkah tersebut sudah dilakukan serta password berhasil diambil dan dengan leluasa masuk kesistem, mereka dengan leluasa dapat mengekplorasi sistem komputer yang jadi sasarannya dengan bebas. dapat melakukan pencarian informasi dan merubah sistem yang ada, atau meletakkan program jahat seperti *Trojan Horse*, *Worm*, *Sniffer* dan sebagainya.

Berikut ini dasar-dasar melakukan haking pada sistem VAX yang menjalankan sistem operasi VMS (Virtual Memory System), adapun VAX/VMS haking tersebut adalah sebagai berikut :

Username :	Password :
SYSTEM	OPERATOR
SYSTEM	MANAGER
SYSTEM	SYSLIB
OPERATOR	OPERATOR
SYSTEST	TEST
SYSMAINT	SERVICE
SYSMAINT	DIGITAL
FIELD	SERVICE
GUEST	unpassword
DECNET	DECNET

Berikut ini adalah beberapa VAX / VMX Commands yang biasa digunakan serta diperlukan untuk melakukan VAX / VMS haking :

Command :	Function :
HELP (H)	Give help and list of commands.
TYPE (T)	View contents of a file.
RENAME (REN)	Change name of a file.
PURGE (PU)	Deletes old versions of a file.

Command :	**Function :**
PRINT (PR)	Prints a file.
DIRECTORY (DIR)	Shows list a file.
DIFFERENCES (DIF)	Show differences between files.
CREATE (CR)	Creates a file.
DELETE (DEL)	Deletes a file.
COPY (COP)	Copy a file to another.
CONTINUE (C)	Continue session.

Password file dalam VAX's akan tersedia apabila mengetik dengan command : *SYSSSYSTEM:SYSUAF.DAT*, password pada sebagian besar file VAX tidak tersedia apabila dalam system UNIX normal. Disini perlu hati-hati apabila sedang melakukan haking karena seluruh *login illegal yang sengaja* masuk akan dicatat dan direkam. apabila Haker tersebut sudah ahli dan bukan pemula hal ini tidak menjadi masalah.

Berikut ini adalah dasar melakukan haking terhadap PRIME. sistem ini akan memperkenalkan anda pada *Primecon 18.23.05*. adapun username dan password dari Prime haking adalah sebagai berikut (yang lengkap di lampiran) :

Password :

aaa
academia
ada
adrian
aerobics
airplane
albany
albatross
albert

Apabila para Haker tersebut sudah masuk ke sistem dengan cara seperti diatas, selanjutnya mereka mengetikkan *NETLINK* disinilah mereka akan bersenang-senang atau mendapatkan apa yang mereka inginkan. Pada tahap inilah suatau sistim jaringan komputer dapat mereka lihat atau rubah.

c. Tehnis melakukan Preking.

Para Preker dapat melakukannya dengan menggunakan telepon manapun tapi seperti yang sudah disebutkan sebelumnya sangat bodoh apabila melakukan hal tersebut dengan melalui jaringan telepon dirumah sendiri, yang paling pertama diperlukan adalah *mengkonstruksikan* kotak-kotak (boxes) yang diperlukan. Berikut ini beberapa boxes dan deskripsi kegunaannya :

Box :	Description :
Red Box	generates tones for free phone calls
Black Box	when called, caller pays nothing
Green Box	generates coin return tones
Cheese Box	turns your phone into a payphone
Acrylic Box	steal 3-way calling and other services
Aqua Box	stops F.B.I. lock-in-trace
Bloto Box	shorts out all phones in your area
Bud Box	tap neighbors phone
Chrome Box	manipulates traffic
Clear Box	free calls
Dayglo Box	connect to neighbors phone line
Divertor Box	re-route calls
Gold Box	dialout router
Infinity Box	remote activated phone
Jack Box	touch-tone key pad
Light Box	in-use light
Magenta Box	connect remote phone line to
Neon Box	external microphone
Olive Box	external ringer
Party Box	creates party line
Rainbow Box	kill trace
Silver Box	create DTMF tones for A.B.C. and
Tan Box	phone conversation
Urine Box	create distrubance on phone
Violet Box	stop payphone from hanging
White Box	DTMF key pad
Yellow Box	add line extension

Selanjutnya merencanakan penggunaan box, disini box berwarna merah adalah alat yang paling utama untuk digunakan ada dua cara untuk membuat red box, *Pertama* : pergi ke toko alat–alat radio untuk membeli *Tone dialer* dan

Kristal 6.5536 Mhz, untuk digunakan menelpon jarak jauh (SLJJ). *Kedua* : metode lebih mudah dengan menggunakan red box khusus untuk telepon umum, yang tidak berfungsi dalam *COCOT* (Customer Owned Customer Operated Telephone) yaitu semacam sistem telepon umum atau warung telepon (Wartel). Caranya untuk komunikasi jarak jauh dengan tidak membayar dari sistem COCOT adalah dengan mendial nomor *1 sampai dengan 800*, namun nomor-nomor ini belum tentu digunakan saat ini karena pemilik COCOT selalu merubahnya.

Cara lain adalah dengan mengetahui nomor-nomor ANAC (Automated Number Announcment Circuit) yaitu rangkaian nomor-nomor otomatis yang digunakan oleh umum, contohnya : nomor darurat pemadam kebakaran, rumah sakit atau kantor Polisi (di Indonesia nomor 110, di Amerika nomor 911). Adapun contoh dari nomor-nomor tersebut adalah sebagai berikut :

Area code :	**ANAC Number :**
201	958
202	811
203	970
205	300-222-2222
205	300-555-5555
205	300-833-3333
205	557-2311
205	811
205	841-1111

Berikut ini adalah *Rainbow box* yaitu seri buku - buku pelangi yang merupakan evaluasi pemerintah dan berbagai macam lainnya yang sangat berguna bagi para Preker, adapun daftar dari buku-buku tersebut dan penjelasannya adalah sebagai berikut :

Color :	Description :
Orange 1	D.O.D. Trusted Computer Systems
Green	D.O.D. Password Management
Yellow	Computer Security Requirements

Color :	Description :
Tan	Understanding Audit In Trusted Systems
Bright Blue	Trusted Product Evaluation
Neon Orange	Understanding Discretionary Access
Teal Green	Glossary Of Computer Terms
Orange 2	Understanding Configurations
Red	Interpretation Of Evaluation
Burgundy	Understanding Design Documentation
Dark Lavender	Understanding Trusted Distrobution
Venice Blue	Computer Security Sub-Systems
Aqua	Understanding Security Modeling
Dark Red	Interpretation Of Environments
Purple	Formal Verification Systems
Gray	Selecting Access Control List
Lavender	Data Base Management Interpretation
Yellow 3	Understanding Trusted Recovery
Bright Orange	Understanding Security Testing

d. Modus Operandi dan akibat-akibatnya.

Umumnya modus operandi para Haker (Kraker) di seluruh dunia, adalah menyerang Website, kemudian disusul dengan perusakan-perusakan sarana / instalasi-instalasi yang dikendalikan melalui jaringan komputer, modus para Haker (Kraker) tersebut dikategorikan sebagai berikut :

1) Menyerang mengganggu situs-situs (Website) dengan tujuan :

a) Menghalangi akses masuk ke situs.

b) Merubah tampilan situs dan fungsinya.

c) Merusak situs dan membuat tidak berfungsi.

2) Menyerang pada suatu komputer Network (Internet, Intranet, WAN serta LAN), untuk melakukan hal-hal sebagai berikut :

a) Mencuri informasi untuk kepentingan industri (Spionase bisnis).

b) Merubah program / piranti lunak agar tidak berfungsi secara normal.

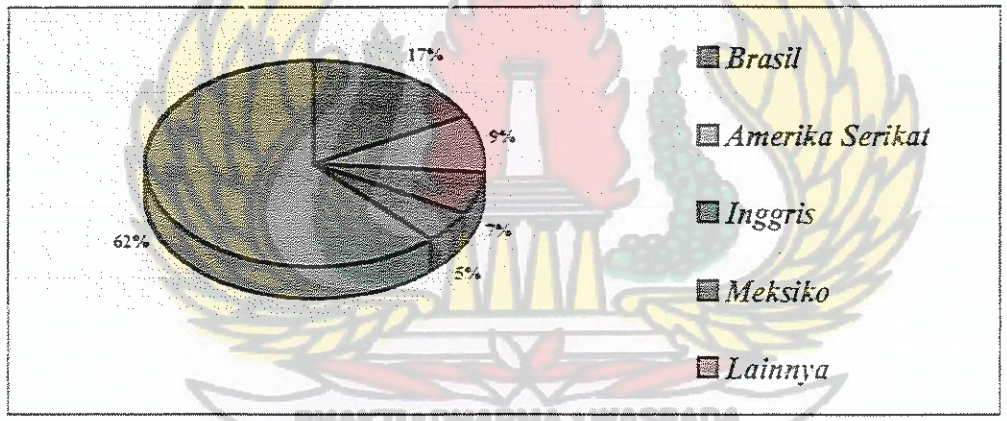
3) Melakukan transaksi palsu pada perusahaan-perusahaan *Dotcom* (.Commerce) dengan memanfaatkan fasilitas *e'commerce*, dan menggunakan kartu kredit milik orang lain secara tidak sah.

Berdasarkan data dari *Majalah Panji*, kwantitas dari modus-modus tersebut diatas adalah sebagai berikut : " Dari total 8.378 situs yang diserang, situs negara yang kena mencapai 36 %. Yang terbesar adalah situs komersial berakhiran .com yang posisinya mencapai 40 % kemudian menyusul yang berakhiran .org, .edu dan .net."[43]

Sedangkan negara-negara yang diserang (menjadi korban) data dari http://www.attrition.org , menunjukkan sebagai berikut :

Grafik / tabel . 1

Korban berdasarkan Country domain (Agustus – Oktober 2000).



(Sumber data : http://www.attrition.org)

Jumlah seluruh kasus adalah *3.045* kasus. Negara Brasil paling tinggi *522* kasus *(18 %)*. Negara-negara lainnya adalah *1.885* kasus *(60 %)*, didalamnya terdapat Indonesia *17* kasus *(0,2 %)*.

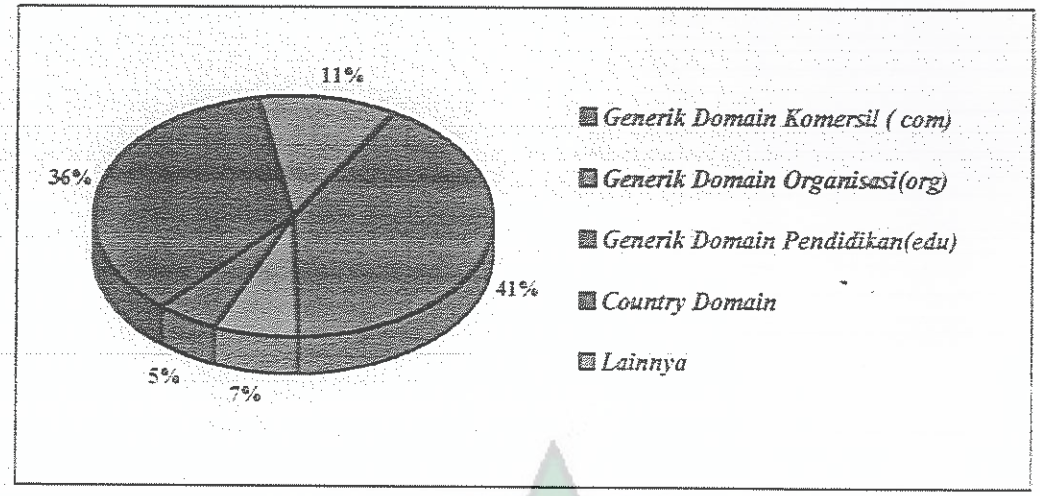
Berdasarkan Website domain atau jenis-jenis Website jumlah korbannya *8.145* domain. dengan rincian sebagai berikut

---

43. Supriyanto Akhmad , *Menyelusuri Jejak Para Penyusup*. Majalah Panji No.29 Tahun IV, Jakarta, 8 November 200. Hal. 74.

Grafik / tabel . 2

Korban berdasarkan domain (Agustus – Oktober 2000).

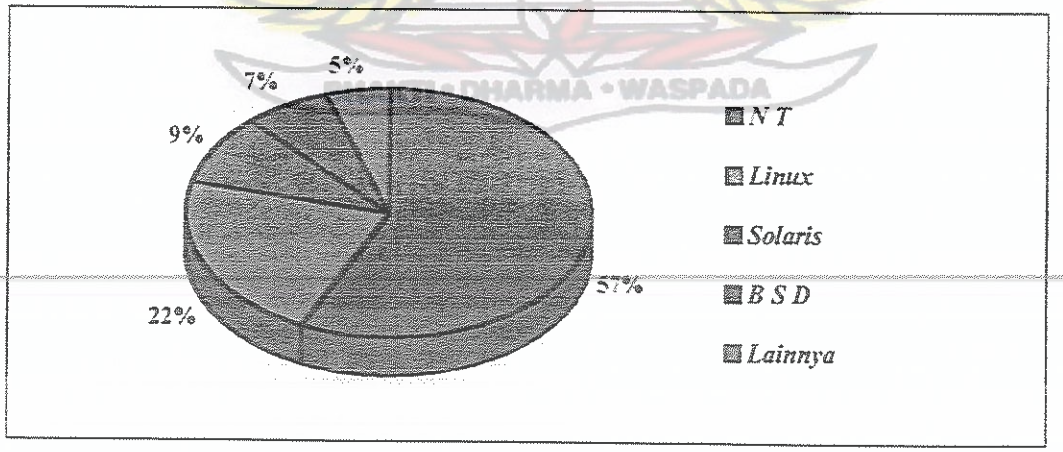


(Sumber data : http://www.attrition.org)

Sedangkan berdasarkan *sistem operasi* yang menjadi korbannya, dari kasus sebanyak *8.145* tersebut, komposisinya adalah sebagai berikut :

Grafik / tabel . 3

Korban berdasarkan sistem operasi (Agustus – Oktober 2000)



(Sumber data : http://www.attrition.org)

Adapun para Haker jahat (Kraker) yang teraktif di dunia yang sering melakukan serangan (berdasarkan nama samarannya), adalah sebagai berikut :

Grafik / tabel . 4

Ranking : 10 Haker (Preker) teraktif Tahun 1999 – 2000.

RANKING	NAMA HAKER	JML SITUS	SERANGAN TERAKHIR
1.	forpaxe	156	01 Ags 2000
2.	antichrist	142	10 Des 1999
3.	dhc	116	08 Ags 2000
4.	gh	115	06 Ags 1999
5.	gforcepakistan	110	16 Ags 2000
6.	crimesboy	102	10 Juli 2000
7.	mcm4nus	100	07 Ags 2000
8.	pakistanhc	99	01 April 2000
9.	acidklown	94	04 Jun 2000
10.	ph33rtheb33r	76	07 Ags 2000

Sumber : http://www.attrition.org

Jumlah situs yang diserang seluruhnya 995 kali *Forpaxe* adalah yang paling aktif menyerang sebanyak 156 kali, disusul oleh *Antichrist*, belum ada data atau informasi bahwa ke 10 Haker (Preker) tersebut dapat diungkap oleh para penegak hukum di masing-masing negaranya.

Akibat-akibat yang ditimbulkan dari ulah para Haker / Preker tersebut adalah sebagai berikut :

1) Kevin Mitnick, 31 tahun diduga telah mencuri data bernilai miliaran dollar AS melalui jaringan maya. Dia juga dituduh menyabot sistem komputer N O R A D (Komando Pertahanan Amerika Utara) yang mengawasi rudal-rudal Rusia dan mengarahkan sistem rudal AS serta pesawat-pesawat pembom AS di seluruh dunia. Ia berhasil ditangkap setelah diburu selama 3 tahun (1992 – 1995) oleh para agen Federal dan sekelompok pakar komputer di bawah pimpinan pakar fisika komputasi di San Diego Computing Centre, Tsutonnu Shomomura.

2) Singkatan CIA yang terpampang dalam website lembaga rahasia ini diganti, sehingga berbunyi *Central Stupidity Agency* , sementara itu, Departemen Pertahanan AS, Pentagon mengaku menerima gangguan hacker *250.000* kali setiap tahunnya.

3) Remaja Kanada yang dikenal dengan *Mafia Boy*, didakwa telah melakukan kejahatan dituding menghalangi akses ke situs *CNN.com* selama empat jam pada Februari 2000, bukan Cuma CNN bocah ingusan itu juga didakwa melakukan hal yang sama pada situs *Yahoo!*, *e-Bay*, *Buy.com*, dan sejumlah situs lainnya dengan total kerugian mencapai US $ 1.2 milyar (12 triliun rupiah).

4) Microsoft *mendeteksi* di jaringan komputernya ada penyusup. Ia rupanya sudah ada disana selama paling kurang dua belas hari (sebelumnya dilaporkan sampai lima pekan), rupanya ada kode *blueprint* yang diduga lenyap. Sampai-sampai Microsoft sempat mengundang FBI untuk menyelidiki kasus tersebut. ini salah satu *contoh dari spionase industri*.Setelah dilakukan pelacakan terungkap ada keterlibatan orang dalam, sebab ada pengiriman informasi dari dalam perusahaan ke *account e'mail* di Saint Petersburg, Rusia.

5) Pada bulan Juni pada saat liburan sekolah di Amerika Serikat CNN melaporkan sebagai berikut : " It is June, the children are out of school and as highway and airports fill with vacationers, rolling power outages hit sections of Los Angeles, Chicago, Washington and New York. An airliner is mysteriously knocked off the fight control system and crashes in Kansas."[44]

---

44. CNN dotcom. ***Bracing for Guerrilla Warfare in Cyberspace.*** [Online]. Hal.1. Tersedia : http://cnn.com/TECH/specials/hackers/cyberterror/ . [15 Februari 2000].

Hal tersebut diatas diakibatkan oleh ulahnya para Kraker, sangat fatal dampaknya karena menyebabkan padamnya aliran listrik di Los Angeles, Chicago, Washington dan New York. Lebih parah lagi menyebabkan rusaknya sistem kontrol penerbangan, secara misterius di kota Kansas Amerika Serikat.

Ada beberapa kemungkinan yang dapat dilakukan para Kraker atau teroris yang menggunakan cara-cara Haking, untuk melaksanakan maksud (misinya) antara lain sebagai berikut :

1) Melumpuhkan dan merusak jaringan komputer dari sistem pertahanan / keamanan suatu negara, berikut ini adalah *contoh simulasi serangan* sebagaimana yang dilaporkan Senator Jon Kyl (Kepala bagian teknologi Senat negara bagian Arizona Amerika Serikat) dalam suatu dengar pendapat pada bulan Nopember 1997, sebagai berikut :

> "Eligible Receiver," as the exercise was called, achieved "root level" access in 36 of the Department of Defense's 40,000 networks. The simulated attack also "turned off" sections of the U.S. power grid, "shut down" parts of the 911 network in Washington, D.C., and other cities and gained access to systems aboard a Navy cruiser at sea. At a hearing in November 1997, Sen. Jon Kyl, R-Arizona, chairman of a Senate technology."[45]

Patut disukuri karena peristiwa diatas tersebut hanya merupakan simulasi serangan !. Terbukti bahwa dalam simulasi tersebut para Haker dapat masuk pada : *36 Root Level akses* dari 40.000 network Departemen Pertahanan Amerika Serikat, mematikan beberapa sektor sistem tenaga listrik, mematikan beberapa bagian sistem *telepon 911* (panggilan darurat Polisi) di Washington D.C dan beberapa kota lainnya, serta mampu *mengakses* ke sistem kendali *Kapal-kapal penjelajah* Angkatan Laut Amerika di lautan.

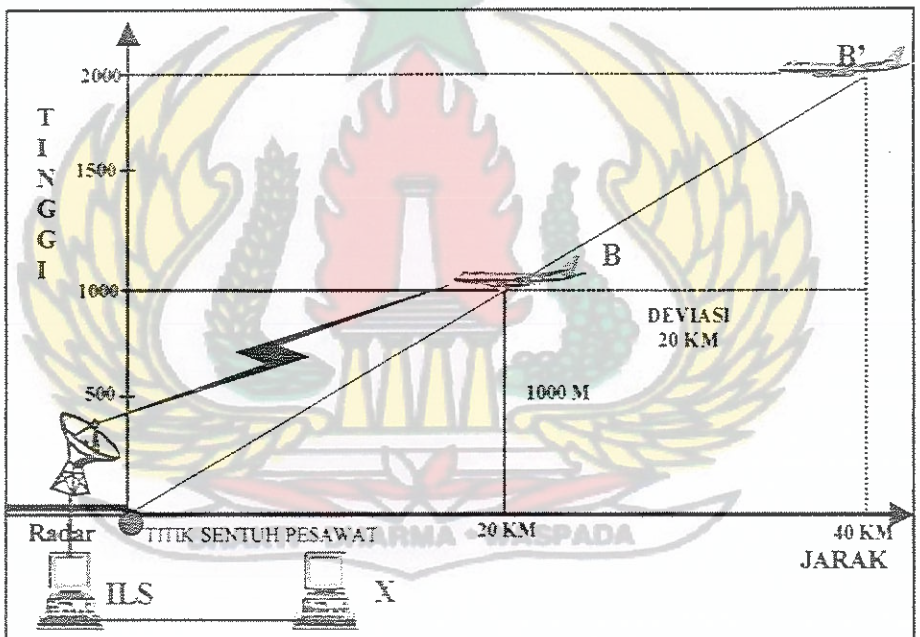
---

45. Ibid. Hal 2.

Kemungkinan lainnya adalah bila para Kraker / Teroris *mengganggu ILS* (Instrument Landing System), yaitu alat pemandu pendaratan pesawat terbang yang digunakan saat pesawat terbang akan mendarat pada suatu Bandara pada malam hari dan cuacanya sangat buruk / berkabut. Apabila benar-benar terjadi akibatnya sangat fatal, karena bila satu pesawat Boing 747 jatuh paling tidak 500 orang meninggal dunia, serta bukan *hanya satu* pesawat saja yang bisa jatuh, tetapi bisa lebih dari itu.

Gambar . 10

Gangguan Haker terhadap ILS



Keterangan gambar :

Seorang *Haker (X)* berhasil menembus sistem komputer ILS (Instrument Landing System) kemudian merubah programnya sehingga telemetrinya berubah. telemetri yang sudah dirubah tersebut dipancarkan oleh radar dan diterima oleh pilot di pesawat B. posisi *sesungguhnya* berada pada ketinggian 1000 Meter namun instrumen di pesawat *menunjukkan* pada angka 2000 Meter.

Pilot pesawat B menganggap masih berada pada ketinggian 2000 Meter (posisi B'). Apabila pilot menurunkan ketinggiannya sebanyak 1000 Meter, ia menganggap masih 1000 Meter lagi dari tanah padahal kenyataannya sudah menabrak tanah. Seluruh pesawat yang jaraknya masih dalam jangkauan ILS tersebut sama gejalanya, jadi pesawat yang jatuh bisa lebih dari satu

Apabila pesawat yang jatuh bisa lebih dari satu dan korban sangat banyak akan terjadi kepanikan masa yang luar biasa (geger), sangat sulit dibayangkan bila benar-benar terjadi di Bandara Sukarno Hatta - Cengkareng , Polri akan dibuat repot dan kewalahan serta *dimaki-maki* bila tidak bisa mengungkap pelakunya. Artinya fenomanena Haking / Kraking kelihatannya biasa saja namun mengandung suatau ancaman yang sangat fatal, serta apapun yang terjadi di luar negri dapat terjadi pula di Indonesia. Sangat perlu dan berguna apabila Polri dari sejak awal mengantisipasinya.

15. Perkembangan dan dampak Haking Komputer di Indonesia.

Perkembangan haking komputer di Indonesia tidak beda jauh dengan perkembangan haking komputer yang ada di luar negeri, kecanggihan *metoda* dan *program* pendukung yang terbaru dan beredar di luar negeri hanya dalam hitungan jam atau hari sudah beredar di Indonesia. Berikut ini perkembangan dan dampaknya yang terjadi di Indonesia :

a. Perkembangan haking komputer di Indonesia.

Perkembangan haking (kraking) dan preking yang ada di Indonesia *nuansanya* saja yang sedikit berbeda dimana di Indonesia *sangat mencerminkan* situasi kondisi keamanan dan politik yang masih belum stabil di negeri ini. Dalam BBS's yang ditayangkan oleh situs-situs resmi banyak menyangkut masalah pertikaian politik, HAM, kerusuhaan dan ekonomi, demikian juga para Haker apabila membobol suatu Web site hampir sama namun lebih kasar lagi.

Sedangkan para Kraker mencuri dan menipu korbannya dengan cara paling mudah, yaitu memanfaatkan *kartu kredit* dan *dotcommers*. para Preker juga meningkat pesat dalam menyerang perusahaan Telepon, sejalan dengan meningkatnya perusahaan-perusahaan yang melayani jasa komunikasi.

b. Profil para pelaku.

Profil para Haker di Indonesia hampir tidak ada bedanya dengan profil para Haker di luar negeri, mereka adalah memuja kesenangan, manusia-manusia yang ulet dan kreatif, tidak pembosan serta menginginkan kebebasan yang absolut. Hal yang terakhir ini sangat memungkinkan karena didukung oleh situasi *euphoria demokratisasi*. Mayoritas mereka hampir sama juga yaitu remaja dan para pelajar, dari segi umur hampir sama antara umur 13 sampai dengan 65 tahun (yang berumur tua biasanya orang-orang kampus).

c. Budaya para Haker.

Aturan-aturan yang berlaku, strata sosial para Haker sangat sama, mempunyai bahasa yang khusus dan sebagian menggunakan bahasa Indonesia khas bahasanya mereka, bahasa Haker lokal yang menggunakan bahasa Indonesia belum secara formal dibukukan dan disebarkan pada BBS`s atau Text file.

d. Jaringan para Haker

Hampir seluruh fasilitas jaringan internasional para Haker dimanfaatkan, namun belum ada jaringan yang khusus di Indonesia baru terbatas pada jaringan kampus-kampus tertentu, antara lain jaringan Haker dari kampus ITB, Universitas GAMA, Universitas Indonesia serta Sekolah khusus yang dikelola Departemen Telekomunikasi.

e. Modus Operandi dan Akibat-akibatnya.

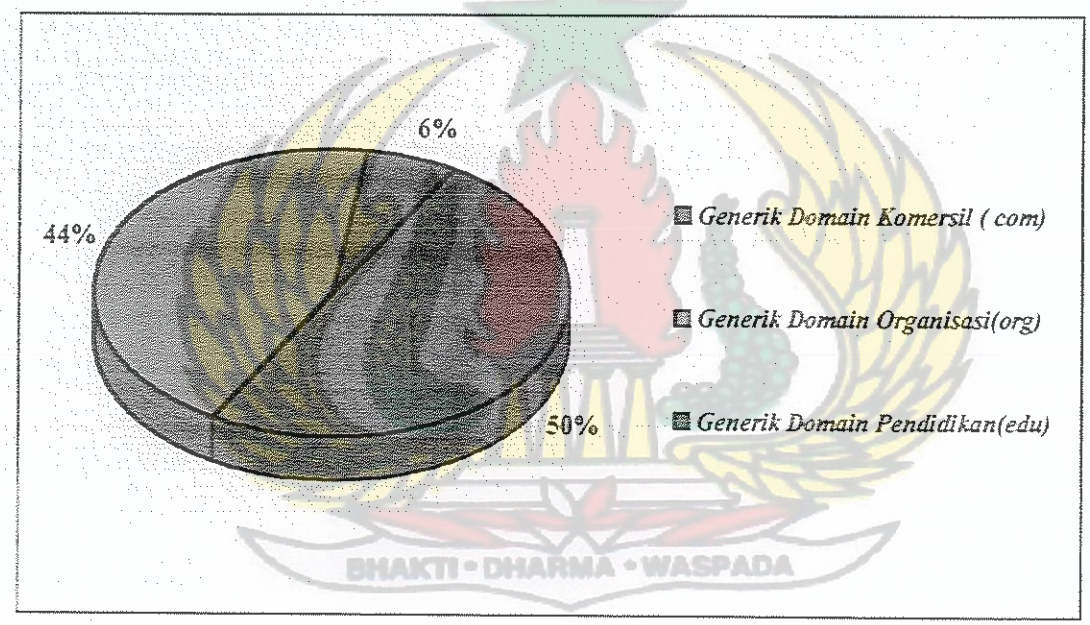
Modus operandi para Haker local hampir sama dengan Haker-haker di luar negeri, dari *segi motivasi* sedikit berbeda yaitu ; Benci terhadap pemerintah (termasuk TNI dan Polri), kesal (bencian) terhadap situasi Indonesia yang tidak

stabil. Kraker yang motivasinya finansial (mencuri) lebih banyak menggunakan sarana *creditcard* dengan menggunakan fasilitas e-commerce namun belum ada yang mencuri informasi untuk kepentingan industri (spionase bisnis) .

Dibawah ini grafik korban Haker di Indonesia berdasarkan Domainnya yang terdata dari tahun 1986 sampai dengan tahun 2000 . jumlahnya : 16 kasus . Jumlah ini tidak menunjukan situasi yang sebenarnya karena banyak yang tidak terdata atau dark number. Polri juga belum ada data yang khusus untuk mencatat kasus ini

Grafik / tabel . 5

Korban Haker di Indonesia (Th. 1986 – 2000).



Sumber : http://www.attrition.org

Berikut ini adalah data tanggal penyerangan. nama-nama situs yang menjadi korban di Indonesia serta nama Haker yang melakukannya . dengan bebarapa contoh Website yang menjadi korban dan akibat-akibat yang ditimbulkannya. Data inipun belum mencerminkan kejadian yang sesungguhnya (lebih banyak) . serta belum terdatakan kerugian finansial / ekonomi. .

Grafik / tabel . 6

Website di Indonesia korban Haking (Th. 1986 – 2000).

TANGGAL	NAMA SITUS KORBAN	NAMA HACKER
28 Okt 2000	Planetdata.co.id	Troya
27 Okt 2000	Matahari.co.id	Antihackerlink
26 Okt 2000	Asaba.co.id	Reboot
25 Okt 2000	Kabelvisionco.id	-
24 Okt 2000	Commerce.net.id	Stolen
07 Okt 2000	Astek.co.id	Hitler Crew
14 Juli 2000	Deka.co.id	SuBZeRo
14 Juli 2000	Trisakti.ac.id	SuBZeRo
24 Mei 2000	Rad.net.id	Antihackerlink
12 Sept 1999	Webprimus.iptek.net.id	HPT
24 Ags 1999	Redhat.or.id	Stroomtrooper
21 Ags 1999	Satelindo.co.id	Mozy
01 Ags 1998	Bit.net.id	KaoTik Team
19 Jan 1998	Polri.mil.id	Kecoak E
18 Jan 1998	Abri.mil.id	Kecoak E
23 Des 1996	Bppt.go.id	Phait

Sumber : http://www.attrition.org

Sangat memprihatinkan dari data tersebut terlihat bahwa pada tanggal *18 dan 19 Januari 1998* situs Polri dan ABRI menjadi korban namun tidak berdaya untuk mengungkap tersangkanya, adapun Haker yang sering melakukannya dan berasal dari Indonesia adalah : *Kecoak E*, *Phait* dan *Antihackerlink*, sedangkan yang lainnya sulit untuk diidentifikasi kemungkinan besar Hacker tersebut dari luar negeri.

Akibat yang ditimbulkan dari ulah para Haker (Kraker) tersebut adalah sebagai berikut :

1) *Planetdata.co.id* penampilannya tertutup habis, yang muncul cuma tulisan *Hacked!!!! Troya Rule*, Ferizal yang membobol situs ini juga memberi pesan-pesan. Ferizal misalnya menulis, *I knew I loved you before I met you* (Dedicated For Datu). Situs aslinya sendiri hingga akhir Oktober 2000 belum pulih.

2) *Situs Matahari* tiba-tiba berubah menjadi *Khaterina*, di bawahnya tertera tulisan *I really love you so much*. Haker tersebut menuliskan nama Iwan dan Kaht dan gambar hati. Mengaku sebagai *Chikebum*, salah seorang dari kelompok Antihackerlink, membobol situs Matahari karena frustasi akibat putus cinta.

Gambar . 11

Website e'commerce : Matahari Dept Store dirubah Haker

Sebelumnya, situs milik perusahaan terkait dengan Grup Lippo, Kabelvision juga diserang, tidak teridentifikasi siapa yang melakukannya. Di halaman Web hanya tertera : Sorry, http://www.kabelvision.co.id still under heavy attack.

3) *Situs astek co.id* milik PT Jamsostek pada 6 Oktober 2000 berubah tampilannya, tertera gambar *Adolf Hitler* lengkap dengan logo Nazi dan tulisan HC. Kraker ini menamakan dirinya *Hitler Crew*. dibagian bawah situs ada teks tentang Yahudi juga link ke www.hitler.org .

4) *Situs Universitas Trisakti* (*trisakti.ac.id*) pada pertengahan Juli tahun 2000 berubah wajah. seseorang yang menamakan dirinya *SubZeRo* menyusup

dan mengubah halaman tersebut. Halaman web berwarna hitam itu diisi oleh tulisan *SuBZeRo Owns You* dan ketikan besar berbunyi *Hacked by SuBZeRo*. Ia juga meninggalkan e-mail atas nama Ch4m313.on@hotmail.com.

5) ***Situs Rad.net***, perusahaan Internet service provider (ISP) juga kebobolan terjadi pada 24 Mei 2000 pelakunya *Antihackerlink*, mereka mengubah tampilan situs dengan menuliskan nama Antihackerlink besar-besar, di bawah tertera tulisan : *exist without skin colour, without nationally, with out religions bias.* Pelakunya juga meninggalkan e-mail, antihackerlink @antionline.org.

6) ***Satelindo.co.id***, dibubuhi sebuah gambar dengan tulisan di bawahnya, *I call that one… "The Last War."* pelakunya Mozy pada Agustus tahun lalu selain teks singkat juga meninggalkan e-mail di mozy@usa.com.

7) ***Polri.mil.id dan Abri.mil.id*** . Situs milik Kepolisian Republik Indonesia disusupi kecoak elektronik terjadi pada 19 Januari 1998, Si kecoak mengubah halaman depan situs, dengan tulisan Tritura 98. Isinya tuntutan agar meturunkan harga, rombak kabinet, dan bebaskan tapol. Juga disertakan hujatan kepada pemerintah.

Bersamaan dengan itu situs Polri dirubah tampilan tapi tidak merusak server, situs milik *TNI, abri.mil.id*. Di bagian atas tertulis, *The Cruel, Violent* and *Corrupted.*

8) ***Situs BPPT***, dirusak diserang oleh mereka yang menamakan dirinya *Portuguese Hackers Against Indonesia Tiranny* (Phait) melakukan mass hack ke situs Badan Pengkajian dan Penerapan Teknologi (BPPT), pada 23 Desember 1996. Pelakunya mengatakan bahwa serangan itu bukan melawan rakyat Indonesia, melainkan pemerintah Indonesia.

Berikut ini adalah data para Kraker yang bermotifkan ekonomi atau sengaja mencuri (sebagian tertangkap oleh Reserse Polda Jawa Tengah) , berdasarkan laporan dari *MasterCard International Security & Risk Management* tanggal 13 November 2000 yang berpusat di Singapura. Dasar laporan tersebut dari keluhan perusahaan komputer *Greywolf Computer Services* yang berada di kota Weirton negara bagian West Virginia Amerika Serikat, pemiliknya Mr. Mark Bunner pada tanggal 17 November 2000 melaporkan ke Master Crad telah ditipu oleh orang Indonesia sebanyak 14.644,41 US S. Dari laporan ini dapat diketahui siapa pelakunya di Indonesia dan dari kota mana transaksi dilakukan ;

Grafik / tabel . 7

Tersangka yang paling sering melakukan transaksi

NO	NAMA TERSANGKA	JUMLAH TRANSAKSI	KERUGIAN (US $)	KOTA
1	Beny Sum	4	3500	Salatiga
2	Aryanto Surya	2	2010	Ungaran
3	Banu Pradipto	3	1500	Ungaran
4	Adhenico. A	2	4000	Semarang
5	Kurniawan	3	840	Salatiga
6	Suriapuspa	2	600	Salatiga
7	Ferdinan Kesi	1	300	Salatiga
8	Januar Maulana Joko Haryanto	1	280	Salatiga
	JUMLAH	18	13010	

(Sumber data : *MasterCard International Security & Risk Management*)

Penyidikan terhadap para tersangka tersebut dan modus operandi yang mereka lakukan adalah sebagai berikut ; Pada tanggal 15 November 2000 tersangka Adhenico A. Kurniawan (Nico), umur 20 tahun seorang mahasiswa UNIKA – Salatiga ditangkap oleh Reserse Polda Jawa Tengah, dalam laporan Polisi No : A/133 /XI/2000/Serse tanggal 15 November 2000, ia dituduh melakukan tindak pidana sebagaimana dalam pasal 378 KUHP, 363 KUHP.

Reserse Polda Jawa Tengah, bekerja sama dengan Master Card Internasional berhasil mengembangkan kasus ini dan menangkap beberapa tersangka lainnya yaitu : Winardi, Akhmad Lastya, Banu Pradipto, Januar Maulana, Beny Sumarsivin (Beny Sum) dan Aldhy Suria Puspayana. Mereka adalah mahasiswa pada Universitas yang sama namun tempat tinggal (domisilinya) berlainan ada yang di Semarang, Salatiga dan Ungaran. Mereka telah menimbulkan kerugian ± 15.000 US $ sesuai dengan laporan dari Mr. Mark Bunner pemilik perusahaan retail Greywolf Computer Service yang beralamat di 80 Liberty Av. Weirton, West Virginia 26062 – 2124 – USA dengan alamat Dot Commerce : http://www.grewolfcomputer.com .

Adapun modus operandinya adalah sebagai berikut : tersangka Nico dan kawan-kawan melakukan chating dengan internet di Warung Internet Yahoo dan Dimensia Jl. Drs. Cipto – Semarang. dari rekannya (Anonim) di Amerika mendapatkan *data nomor kartu kredit* yang valid dan dijamin dapat digunakan untuk melakukan transaksi.

Mulai bulan Mei 2000 mereka memesan barang-barang melalui situs komersiil di Internet diantaranya *Greywolf Computer*, dengan cara :

a. Membuka situs komersiil (Dot Commerce) yang dituju.

b. Memesan barang-barang yang dikehendaki setelah ditulis, kemudian kolom BUY ditekan (Enter) selanjutnya salah satu nomor kartu kredit milik seorang dengan nomor Master Card : 5313 – 5520 – 0003 – 9280 dimasukkan, kemudian pada kolom User : dimasukkan nama tersangka, alamat rumah dan nomor telepon.

c. Setelah itu barang dikirim ± 2 minggu lewat perusahaan Cargo Fedex, diambil oleh tersangka ke perusahaan tersebut.

Perbuatan tersebut dilakukan dari bulan Mei 2000 sampai dengan awal November 2000, adapun barang-barang yang dapat diambil antara lain 12 kaca mata, 4 unit komputer Palmtop III a, 2 unit VCA Crad, Sandal, Kaos, Jaket dan lain-lain. Setiap transaksi berkisar

dari 198 US $ sampai dengan 2000 US $ sehingga seluruhnya mencapai ± 15.000 US $.

Dari data-data tersebut sangat nyata bahwa perkembangan haking komputer di Indonesia selaras dengan perkembangan haking komputer di luar negeri, demikian juga dengan akibat-akibat yang ditimbulkannya. Ada hal yang sangat *memprihatinkan* yaitu ; apabila seseorang menghendaki untuk melakukan Kraking / Preking, mereka dengan sangat mudah melakukannya serta sulit untuk dicegah seperti yang dikatakan oleh Fred B. Scneider seorang profesor ahli komputer pada Cornell University :"If somebody wanted to launch an attack, it would not be at all difficult."46

Fenomena ini perlu mendapatkan *perhatian yang serius* karena tidak sebuah komputerpun yang tersambung dengan jaringan komputer benar-benar aman dari serangan para Haker, selain itu haking, kraking dan preking akan terus ada dan berkembang. Seorang Haker sejati akan selalu melakukannya setiap saat ada kesempatan, mereka mengatakan melakukan haking sama dengan bernafas menghirup udara pada saat tidurpun mereka bila bermimpi perspektifnya tetap sebagai seorang Haker. Seperti yang dikatakan oleh Emanuel Goldstein : That's like asking how much time you spend breathing. It's always with you, you do more of it at certain times, but it's always something that's going on in your head. Even when I sleep, I dream from a hacker perspective."47

Fenomena Haker perlu dimengerti secara menyeluruh dan utuh, profil mereka secara utuh terlihat dalam manifestonya. Dalam manifesto para Haker akan terlihat bahwa mereka mempunyai alasan dan motivasi yang kuat untuk terus menerus melakukan haking, mereka menganggap dirinya bukanlah penjahat atau menganggap sebagai penjahat tetapi tidak sejahat penjahat lainnya yang menciptakan perang dan membuat senjata pembunuh masal.

---

46. CNN dotcom. Ibid. Hal 2.

47. Emanuel Goldstein. Ibid. Hal 4

Kotak dialog : 2

Manifesto para Haker

Inilah dunia kami sekarang ... dunia yang penuh dengan electron-elektron dan tombol , yang cantik. Kami berbuat dan melayani sehingga sempurna dan menarik tanpa dibayar tidak seperti orang-orang murahan yang kotor , tidak serakah dan loba,. tapi kalian menyebut aku penjahat. Kami hanya menggali dan mencari ... dan kalian menyebutnya kejahatan. Kami eksis tanpa perbedaan warna kulit, kebangsaan dan bias agama.

Panggillah kami penjahat. Tapi kalianlah yang membuat bom atom, memulai perang, membunuh, menipu dan membohongi kami serta membuat kami percaya bahwa untuk kebaikan yang kami buat sementara ini, kami dianggap sebagai penjahat . Benar, saya penjahat. Keingin tahuan yang tinggi adalah kejahatanku. Aku jadi penjahat karena dihakimi oleh kata –kata kalian yang tanpa dipikir dan tanpa dengan melihat seperti apa aku yang sebenarnya. Kejahatanku adalah karena aku lebih pintar dari kamu dan kamu tidak memaafkanku karena hal tersebut. Ya aku adalah Haker dan inilah manifestoku. Kalian boleh mempunyai pendapat pribadi, tapi tidak akan bisa menghentikan kami, karena sebenarnya kita adalah sama (penjahat juga).

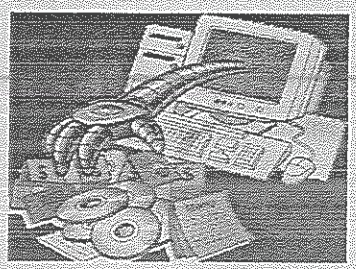
Sang Begawan

Sumber :
Hacker's Manifesto., http://www.hackers.com/texts/startbak.txt ,(Terjemahan).

Kevin Mitnick

MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

Bab. V



BAB V

KONSEPSI IDEAL KEMAMPUAN PENYIDIKAN DAN DUKUNGAN KOMPUTER FORENSIK SERTA PERANGKAT HUKUMNYA

16. Kemampuan penyidikan kasus haking komputer.

Penyidikan kasus haking komputer memerlukan suatu kemampuan khusus dari segi tehnis penyidikan serta profil penyidiknya, penyidik yang disiapkan untuk menangani kasus ini sebaiknya yang sudah cukup berpengalaman (bukan penyidik pemula), perlu menguasai tehnis penyidikan sekaligus penyelidikan juga menguasai administrasi penyidikan, serta menguasai dasar-dasar pengetahuan dibidang komputer dan profil Haker. Adapun *profil penyidik* dan *konsepsi tehnis penyidikan* yang diperlukan adalah sebagai berikut :

a. Profil dan latar belakang pendidikan penyidik.

Profil penyidik yang diutamakan antara lain penyidik yang sudah berpengalaman paling tidak 3 tahun sebagai penyidik dibidang tertentu (tindak pidana ekonomi), ulet dan berdedikasi tinggi, sedangkan kemampuan-kemampuan khusus yang diperlukan lainnya adalah sebagai berikut :

1) Latar belakang pendidikan.

Telah melaksanakan pendidikan kejuruan lanjutan dibidang Reserse, dan telah melaksanakan pendidikan dalam bidang komputer pada tingkat programer.

2) Pengetahuan dan kemampuan mengoperasikan komputer.

a) Dapat mengoperasikan komputer pada tingkat lanjutan atau bukan pemula, terbiasa menggunakan komputer untuk mengolah data dan menganalisa tidak hanya mengetik saja.

b) Mampu mengoperasikan program - program pengolahan data antara lain Foxpro, Dbase, LINUX, UNIX serta Python, atau program-program yang *biasa digunakan* oleh para Haker.

c) Sering menggunakan Internet dan mengerti prosedur penggunaan Internet serta seluk beluknya , diutamakan yang telah lama *berlangganan* pada salah satu ISP atau telah mempunyai *User ID*.

3) Mengetahui dan memahami kejahatan-kejahatan komputer secara umum.

Adapun kejahatan komputer secara umum tersebut, yang harus dipahami adalah sebagai berikut :

a) Kejahatan komputer yang menyerang *keamanan fisik komputer*, antara lain Dumpster Diving (Menyelami sampah), Wire Tapping (Penyadapan kawat telepon) dan Eavedropping on Emanations (Menampung pancaran Emisi).

b) Kejahatan komputer yang menyerang *keamanan personil*, antara lain Masquerading (Barisan topeng), Harassment (Gangguan / penghinaan) dan Software piracy (Pembajakan piranti lunak).

c) Kejahatan komputer yang menyerang *komunikasi dan keamanan data*, antara lain serangan terhadap data / pencurian data atau *Data attack* (Mengkopi data secara tidak sah, menganalisa lalu lintas data secara tidak sah dan membuat saluran rahasia) dan serangan terhadap piranti lunak atau *Software attack* (Trap doors, Session hijacking, Tunneling, Timing attack dan Trojan horse *termasuk* Virus / Worm, Salami attack dan Logic Bom).

d) Kejahatan komputer yang menyerang *keamanan operasional*,

antara lain Data didling (Penipuan data), IP Spoofing (Membohongi Internet protocol), Password Sniffing (Mengintip password) dan Scanning (Memindai).

b. Tehnis penyidikan / penyelidikan.

Penyelidikan dilakukan sebelum upaya penyidikan, *titik berat* penyelidikan haking komputer adalah pada *profiling tersangka* (Haker, Kraker dan Preker), serta saksi-saksi. *Tahap selanjutnya* adalah penyidikan dengan titik berat pada *modus operandi* dan *tehnis* haking dan preking dilakukan.

1) Kemampuan penyelidikan .

Ada beberapa kriteria yang perlu dikuasai agar dalam penyelidikan (termasuk under cover) optimal dilakukan, antara lain sebagai berikut :

a) Penyelidik *menguasai profil* para Haker dari segi umur, pekerjaan, motivasi, serta hal-hal yang menarik minta para Haker.

b) Penyelidik *memahami budaya* para Haker, antara lain aturan-aturan yang berlaku dikalangan mereka, bahasa khusus yang digunakan para Haker dan strata sosial para Haker.

c) Penyelidik *mengetahui jaringan-jaringan* para Haker agar dalam melaksanakan under cover tidak terputus komunikasi, serta dapat diterima oleh mereka dengan baik. Jaringan yang harus dikuasi tersebut antara lain : Website, Text file, Majalah, Gopher site dan Buletin Board System (BBS`s) para Haker dan Preker serta tempat-tempat mereka biasa mengadakan pertemuan.

Kemampuan-kemampuan tersebut diperlukan karena fenomena haking komputer *tidak bisa langsung* dilakukan penyidikan sesaat setelah ada seseorang yang menjadi korban dan membuat laporan Polisi, *jauh sebelum hal*

tersebut terjadi harus sudah dimulai pengumpulan data dan informasi mengenai para pelakunya. Penyamaran dilakukan dengan *intensif* sehingga penyelidik dapat masuk ke dalam jaringan mereka, apabila sewaktu-waktu penyidik memerlukan informasi yang akan digunakan dalam proses penyidikan diharapkan informasinya optimal dan target sasaran (tersangka) dapat dilokalisir secara tajam. Selain itu *perkembangan* modus operandi, piranti lunak-piranti lunak yang mereka kembangkan dan seluruh dinamika para Haker dapat dikuasai dengan baik.

2) Kemampuan penyidikan.

Penyidik diharapkan mempunyai pengetahuan serta kemampuan untuk mengetahui program-program jahat komputer dan modus operandi para Haker juga tehnis melakukan haking komputer, sekaligus dengan program-program yang digunakannya. Hal tersebut antara lain ;

a) Penyidik mengetahui *program-program jahat* komputer seperti Virus, Worm dan Trojan horse secara spesifik.

b) Memahami *modus-modus operandi* antara lain ; menyerang situs, menyerang net work dan melakukan transaksi palsu. Serta *akibatnya* antara lain ; tidak berfungsinya situs, informasi yang disalahgunakan dan kerugian finansial serta akibat-akibat lainnya yang lebih fatal.

c) Mengetahui *tehnis-tehnis haking komputer* secara kronologis antara lain ; Scanning, Router to Bridge, Cloaking, Probing, Weakness Identification, Pissing Daemon, Exploiting dan Clean up operation.

d) Mengetahui *tehnis melakukan preking*, yang menggunakan

Kontruksi Box dan COCOT / ANAC.

e) Mengetahui program-program komputer *yang digunakan* untuk melakukan haking dan preking antara lain ; Listing Metaclass Function, Aggressive SNMP scanner, program Sniffer, fungsi-fungsi Telenet Commands, Password shadowing dan sebagainya.

Pengetahuan dan kemampuan itu adalah dasar bagi para penyidik untuk melakukan tindakan pertama di TKP, pengolahan TKP dan barang bukti serta bahan untuk melakukan pemeriksaan terhadap tersangka. Sehingga dapat dipastikan motif dan statusnya apakah ia Haker, Kraker atau Preker dan *dilakukan* karena iseng atau untuk motif ekonomi. Selain itu agar pemeriksaan terhadap saksi tajam dapat mengungkap fakta *kapan terjadi, apa yang terjadi* dan *akibat* yang ditimbulkannya serta kerugian yang diderita, dan terhadap tersangka dapat dengan tajam *mengungkap* fakta-fakta sebagai berikut :

a) *Kapan (waktu)* dilakukan ;

(1) Tersangka masuk ke dalam jaringan .

(2) Sistem jaringan dirubah atau dirusak informasi yang ada diakses.

(3) Tersangka keluar dari jaringan.

b) *Bagaimana* melakukan ;

(1) Masuk ke dalam jaringan dan program yang digunakannya.

(2) Cara merusak data atau mengakses data.

(3) Menutup dan menghilangkan jejak sebelum keluar dari network.

c) *Lokasi / tempat* yang berkaitan :

(1) Terminal yang dia gunakan dan ISP yang menjadi medium atau perantara melakukan haking.

(2) Jaringan komputer (network) yang menjadi target sasaran atau korban.

Kemampuan-kemampuan tersebut *perlu dilengkapi* dengan dukungan komputer forensik serta saksi ahli, sehingga pada akhirnya penyidik mampu untuk menyimpulkan secara tepat delik-delik pidana yang akan digunakan. Karena itu diperlukan juga Undang-Undang yang mendukung proses penyidikan tersebut, berikut ini dibahas forensik pendukung penyidikan yang diharapkan, saksi ahli dan Undang-Undang yang diperlukan agar penyidikan haking komputer optimal.

17. **Komputer forensik pendukung penyidikan haking komputer.**

Istilah komputer forensic lebih tepat disebut dengan *computing forensic* karena yang menjadi sasaran dan bahan analisa adalah *operasionalnya* (penghitungan-penghitungan) bukan bendanya, sebagaimana dijelaskan oleh Vogon : "Forensic Computing is the science of capturing, processing and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law." [48], maksudnya adalah ilmu pengetahuan untuk mendapatkan, memproses dan menyidik data dari komputer-komputer yang digunakan dengan menggunakan metodologi tertentu agar seluruh bukti yang didapat dapat digunakan dalam proses peradilan.

Forensik computing ini diperlukan karena penanganan bukti-bukti yang berhubungan dengan data / program komputer tidak bisa disamakan dengan yang lainnya, serta ada beberapa masalah yang dialami sebelumnya oleh para penyidik antara lain :

---

48. Vogon. . *About Forensic Computing* [Online]. Tersedia : http://www.vogon-computer-evidence.com/forensic_services-01.htm [16 April 2000]. Hal. 1.

a. Waktu dan tanda penanggalan yang berhubungan arsip-arsip kritis mudah berubah, ketika dilakukan Booting pada mesin (komputer).

b. Informasi dalam Free space (area bebas) dari disk yang ditulis ulang atau ditindas saat dilakukan Booting dalam rangka investigasi. Virusnya berkembang memperbanyak diri dan merubah data-data yang ada pada sistem, menyebabkan para penyidik disalahkan karena dianggap telah mengakibatkan kerusakan-kerusakan.

c. Basis sistem dari suatu server tidak mampu lagi dikembalikan agar hidup seperti semula, setelah dimatikan secara gegabah oleh penyidik (tidak sesuai prosedur). Hal ini menyebabkan sengketa dan kecaman terhadap kesatuan penyidik, sebagai konsekwensi logis dari kerusakan-kerusakan yang ditimbulkannya.

d. Pada saat melakukan penyidikan terhadap mesin (komputer), Virus ditemukan dan dipindahkan dari piranti lunak terinfeksi yang sedang dilakukan atau jadi target penyidikan. Upaya pemindahan Virus ini merubah data, tanda waktu atau penanggalan yang ada pada komputer, tentu saja hal ini merubah isi dari arsip yang berisi Virus tadi (barang bukti sudah berubah).

Hal tersebut diatas dialami oleh para penyidik dari Kepolisian Inggris yang menjadikan *Vogon* sebagai mitra kerja dalam melakukan penyidikan kejahatan komputer, sebagaimana dijelaskan oleh Vogon sebagai berikut :

"Some of the problems that our customers have experienced in the past include:

* Time and date stamps relating to critical files changed when booting the machine
* Information in the 'free space' of the disk over written during the boot up During an investigation a virus was spread corrupting many files on the system, resulting in a claim for damages being brought against the investigator
* A server-based system was unable to be brought back to life after being in appropriately turned off. This resulted in a law suit and a claim for consequential damages against the firm of investigators

* Whilst investigating a machine, a virus was found and then removed to prevent infection of the investigating software. The act of removing the virus changed many time and date stamps on the machine and, of course, changed the contents of the file containing the virus."[49]

Vogon adalah suatu perusahaan swasta yang berdiri di Inggris sejak tahun 1985 mempunyai cabang di Amerika dan Jerman. khusus memberikan jasa pelayanan untuk mendapatkan, memproses bukti-bukti yang berhubungan dengan kejahatan komputer secara ilmiah, serta membantu penyidikan juga menjadi saksi ahli terhadap Kepolisian Inggris, Jerman dan Amerika dalam proses peradilan di negara-negara tersebut.

Cara kerja dan program-program Vogon ini patut dijadikan *konsepsi* untuk kegiatan komputer forensik yang akan dilakukan oleh Polri. secara umum ada tiga bagian besar operasional komputer forensik yaitu *Evidence collection* (pengumpulan dan penanganan bukti), *Forensic analysis* (analisa forensik) dan *Expert Witness* (kesaksian ahli). Adapun konsepsi –konsepsi tersebut adalah sebagai berikut :

a. Pengumpulan dan penanganan bukti.

Kegiatan pengumpulan dan penanganan bukti termasuk pengamanan terhadap barang bukti itu sendiri karena banyak berupa alat-alat elektronik yang sangat rentan terhadap suhu, cuaca dan pengaruh magnetik. Tujuannya adalah agar :

1) Tidak merubah waktu dan penanggalan standar yang terdapat pada media komputer.

2) Data-data yang ada tidak berubah.

3) Langkah-langkah pengambilan barang bukti dan data serta pengamanan barang bukti sudah sesuai prosedur, sehingga tidak ditolak pengadilan.

---

49. Vogon. *Risk and Pitfalls*. [Online]. Tersedia : http://www.vogon-computer-evidence.com /forensic_services-02.htm . [16 April 2000]. Hal. 1.

4) Mengetahui secara pasti operasi apa yang terjadi, bila komputer target diaktifkan.

Adapun tindakan-tindakan yang dilakukan agar tujuan tersebut diatas tercapai, adalah sebagai berikut

1) Mengambil secara tepat apa-apa yang perlu di salin (copy) yang ada dalam komputer, dapat menentukan arsip mana yang perlu disalin atau diabaikan.

2) Memelihara secara terus menerus tindakan-tindakan yang dilakukan sehingga proses penyidikan selanjutnya tidak terganggu.

3) Melakukan verifikasi terhadap tindakan yang diambil pada setiap tahap-tahap penyidikan.

4) Mampu secara cepat untuk mengidentifikasi informasi-informasi dan bukti-bukti yang diperlukan dalam suatu komputer dan perangkat-perangkat lainnya, agar tidak salah dalam mengambil barang bukti. *Contohnya* : apabila sasarannya suatu *main frame computer*, penyidik harus dapat menentukan dengan tepat apakah seluruh main frame diambil atau cukup harddisknya saja.

Keyboard dan layar monitor tidak perlu diambil karena di Laboratorium forensik sudah ada.

5) Dapat menentukan apakah data-data yang sudah dihapus, dapat ditimbulkan kembali, dan menyita medium yang menyimpan data tersebut.

6) Dapat mencari informasi-informasi yang disembunyikan pada tempat-tempat penyimpanan data yang berada diluar area.

7) Dapat menentukan untuk mengambil data-data lama yang sudah ditulis ulang atau dirubah (over writte).

Apabila prosedur-prosedur tersebut sudah dilakukan dengan baik selanjutnya

dilakukan prosedur-prosedur untuk menganalisanya yang disebut analisa forensik, prosedur analisa ini memerlukan *piranti keras analisa* dan *piranti lunak analisa*.

b. Analisa forensik.

Dalam melakukan analisa forensik, ada *dua hal utama* yang sangat prinsipil dalam menangani media komputer yang sangat beragam pembuktiannya yaitu :

1) Memastikan bahwa semua tindakan Polisi dan para penyidik tidak merubah data pada komputer atau media lainnya, sehingga selanjutnya dapat mendukung selama dalam persidangan.

2) Harus diciptakan dan disiapkan sebelumnya apabila mengaudit jejak-jejak atau rekaman lainnya terhadap seluruh proses yang digunakan dalam dasar-dasar pembuktian komputer, sehingga *proses kedua* (selanjutnya) yang dilakukan oleh orang lain secara terpisah akan dapat mengulangi seluruh proses dengan cara yang sama dan menghasilkan hasil yang sama pula.

Artinya proses pembuktian ulang yang dilakukan dalam persidangan sangat penting dan harus sama dengan proses sebelumnya, sehingga hasil analisa dapat diterima sebagai bukti otentik. Dijelaskan oleh Vogon sebagai berikut :

> in addition, there are several documented central principles for the handling of computer media in an evidentially sound manner. Two of the most important are:
>
> No action taken by Police or their agents should change data held on acomputer or other media which may subsequently be relied upon in Court.
>
> An audit trail or other record of all processes applied to computer based evidence should be created and preserved. An independent third party should be able to repeat those processes and achieve the same result."[50]

---

50. Vogon *Good Practice Guidlines*. [Online]. Tersedia : http://www.vogon-computer-evidence.com /forensic_services-03.htm . [16 April 2000]. Hal. 1.

Adapun *Piranti keras yang diperlukan* dalam analisa forensic adalah : DAT Imager, Diskette Imager, Covert Imager, Mobile Forensic Workstation dan Enterprise Imaging System. Penjelasan dari piranti keras tersebut adalah sebagai berikut :

1) DAT Imager (Pencitra DAT).

DAT Imager didesain khusus untuk dapat secara cepat menggambarkan dua *set drive* yang terdiri dari pita berukuran standar 4 mm, alat ini mampu untuk mengumpulkan barang bukti data komputer dalam jumlah yang banyak secara jelas, cepat dan efisien. Kegunaan- kegunaan antara lain :

a) Melakukan Imaging (pencitraan) terhadap disk yang berkapsitas besar sampai dengan 25 Giga byte

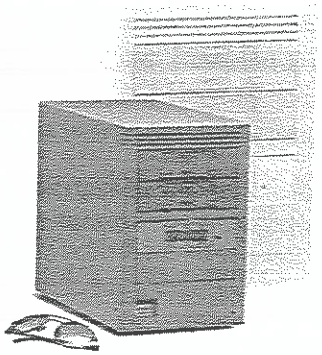
b) Secara otomatis mengkompres data dan disiapkan untuk menangani data yang lebih besar.

c) Apabila pita DAT diisi selama proses imaging, secara cepat unit khusus lainnya memasukkan ke pita-pita yang lain sehingga proses dapat berjalan secara mulus.

d) Dilengkapi dengan perlindungan diri pada seluruh piranti lunak dan piranti kerasnya agar tidak terganggu pada saat pengambilan citra.

Gambar . 12

DAT Imager

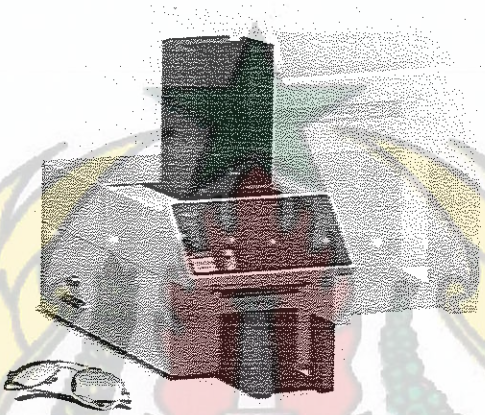


2) Diskette Imager (Pencitra Disket).

Alat ini digunakan apabila situasinya sering menjumpai floppy disks yang sangat banyak yang harus dilakukan proses imaging, alat ini mampu melakukan pencitraan puluhan floppy disks secara otomatis dan tidak perlu membutuhkan banyak operator sehingga menghemat waktu dan dana.

Gambar . 13

Diskette Imager



3) Disk Emulator (Emulator piringan data).

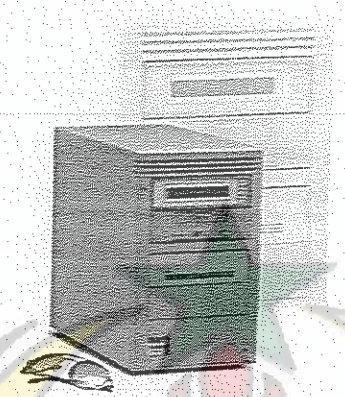
Alat ini membuat tampilan data-data hasil pencitraan menjadi sederhana dan efisien prosesnya sehingga memudahkan para penyidik. *mula-mula* data citra yang telah ditangkap oleh sistem DAT imager dan terekam pada pitanya kemudian dimasukkan ke dalam DAT Emulator dengan menggunakan display LCD yang simpel, untuk *selanjutnya* ditransfer pada emulator. Data-data atau gambar tersebut merupakan pantulan (emulasi) kemudian secara lengkap emulasi tersebut dipindahkan pada disk emulator dan datanya disimpan dalam harddisknya.

Gunanya untuk menduplikasi data dari komputer yang menjadi sasaran penyidikan dengan tidak berubah data-data yang ada pada komputer sasaran

tersebut, demikan juga data yang diduplikasi 100 % sama karena cara kerja alat ini model " Write protect" . Kapasitasnya sangat beragam dari 18 Giga byte sampai dengan 36 Giga byte. dapat ditingkatkan lagi menjadi lebih besar.

Gambar . 14

Disk Emulator

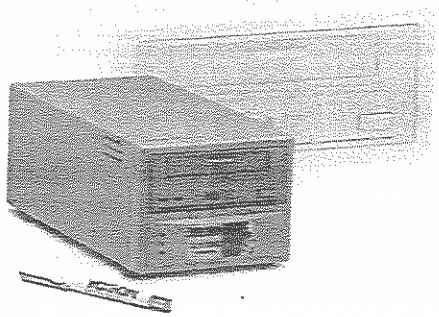


4) Covert Imager (Pelindung hasil pencitraan).

Alat ini dipergunakan untuk *melindungi bukti-bukti* yang diambil oleh para penyidik untuk digunakan dalam peradilan secara sempurna, sehingga hasil-hasilnya akan diterima dalam proses peradilan. Selain itu memungkinkan untuk melakukan pencitraan yang lengkap dari *harddisk* komputer-komputer yang menjadi sasaran.

Gambar . 15

Covert Imager



5) Mobile Forensic Workstation (Labolatorium forensik lapangan).

Penyidikan haking dan preking perlu tindakan yang secepat-cepatnya maka diperlukan laboratorium forensik komputer mini yang lengkap dan dapat dipindah-pindah (mobile) atau labolatorium lapangan. Perlengkapannya terdiri dari DAT Imager, Diskette Imager, Disk Emulator ditambah dengan komputer-komputer lainnya untuk *analisa grafis, analisa angka* dan *word processor* juga *transponder* untuk berhubungan dengan laboratorium pusat serta dilengkapi dengan kendaraan pengangkutnya.

Gambar . 16

Mobile Forensic Workstation

Konfigurasi dasar dan kemampuan dari laboratorium lapangan tersebut . adalah sebagai berikut :

a) Otomatis dapat memproses data-data dalam kapasitas yang besar.

b) Mencerminkan kemampuan dan dapat memenuhi kebutuhan seperti laboratorium proses yang lebih besar.

c) Display layar yang jelas dan akurat untuk mengontrol informasi-informasi yang tampak.

d) Dilengkapi dengan alat yang mampu memberitahukan kesalahan-kesalahan prosedur, sehingga terhindar dari kesalahan operatornya.

e) Dilengkapi dengan piranti-piranti lunak skala besar dari Bus interfaces termasuk SCSI, LVD SCSI, USB, EIDE, IrDA, Ethernet dan CSM.

f) Tampilan seperti yang dikehendaki (sebagaimana aslinya) sehingga tidak memungkinkan dilakukan intervensi dan perubahan-perubahan oleh penggunanya, memungkinkan penyidik yang terampil untuk bekerja dengan baik dan menyukai prosesnya karena sangat sederhana.

6) Enterprise Imaging System.

Alat ini didesain untuk digunakan oleh penyidik-penyidik yang sangat berpengalaman (operator ahli) karena *menangani* Network komputer yang sedang operasional, digunakan untuk kegiatan *pencitraan* dalam skala besar. System ini dilengkapi kabel-kabel untuk masuk / berhubungan dengan infra struktur jaringan komputer, dan dapat dijalankan berdasarkan basis software UNIX yang sangat kuat dapat berkomunikasi dengan berbagai tingkat program-program UNIX.

Gambar . 17

Enterprise Imaging System

Selain itu dirancang untuk menyimpan *citra* dalam skala besar dari program operasional suatu jaringan-jaringan komputer yang jadi *target penyidikan*, dan dapat dikendalikan dengan komputer dari jarak jauh dengan kecepatan pita-pita pelindung (backup tapes) yang sangat tinggi sehingga sangat aman. Adapun komponen pendukung dari sistem ini adalah sebagai berikut :

a) Berbasis program UNIX yang luas dan fleksibel, dapat beradaptasi dengan bahasa atau program komputer lainnya

b) Dapat menangkap data / citra secara cepat , pada berbagai tingkat (level) secara bersamaan.

c) Tampilan pada layar sangat jelas dan sangat akurat dalam mengontrol informasi.

d) Mencatat dan memelihara jejak-jejak / prosedur kerja, sehingga terhindar dari kesalahan.

e) Sistim keamanan password yang menggunakan metode *enkripsi*, sehingga terjamin keamanannya.

Sedangkan *piranti lunak yang diperlukan* dalam melakukan analisa forensik adalah : *GenX / Gen Text* untuk memproses disk, pita data dan arsip-arsip serta *Gen Tree* untuk meneliti arsip-arsip dalam *file manager application* (aplikasi pengaturan arsip), penjelasan dari piranti lunak tersebut adalah sebagai berikut :

1) GenX dan Gen Text

Piranti lunak ini selalu berpasangan karena GenX beroperasi pada Gen Text , guna dari piranti lunak ini adalah untuk memudahkan para penyidik melokalisir informasi-informasi yang tersimpan dalam berbagai piranti lunak yang sangat beragam dalam komputer, secara otomatis mengkompres data-data yang diperlukan juga mengidentifikasi data-data yang telah terkompres secara

cepat. Ada *dua kemampuan yang paling penting* dari piranti lunak ini yaitu secara otomatis menimbulkan kembali arsip-arsip yang sudah dihapus, dan secara otomatis mengidentifikasi jenis-jenis arsip yang tersembunyi.

Cara beroperasinya ada dua macam ; *Pertama* adalah Extraction Mode, yaitu mengambil data-data penting dari seluruh bagian-bagian data yang terkandung dalam barang bukti sasaran pemeriksaan. yang beroperasi pada MS-DOS / Windows. *Kedua* Maping Mode, yaitu secara otomatis memetakan dan menandai arsip-arsip yang diperiksa dengan detil lokasi-lokasinya, serta secara otomatis menyusunnya sehingga memudahkan para penyidik untuk melihat dan menganalisanya.

Adapun *sasaran* yang di analisa oleh GenX dan Gen Text ini adalah sebagai berikut :

a) Seluruh file-file yang ada.

b) Free space (area bebas) pada sistem arsip yang tidak diperlukan untuk menyimpan data.

c) Area data yang hilang yang ada diluar sistem arsip.

d) Slack space yaitu area antara akhir dari arsip dan akhir dari lokasi-lokasi blok yang ditempati data-data yang dicurigai atau disembunyikan.

e) Sistem yang mengatur penempatan arsip cadangan, yang digunakan untuk pangkalan sistem operasi (host).

f) Area-area yang tidak digunakan untuk sistem operasi.

2) Gen Tree.

Gen Tree adalah aplikasi Windows sejenis dengan *file manager application* yaitu aplikasi yang fungsinya *menganur* penempatan arsip-arsip.

gunanya agar para penyidik dapat mengetahui dan menganalisa secara cepat data atau image dari berbagai target yang diperiksa walaupun sistem operasinya berbeda-beda. Piranti lunak ini mempunyai kemampuan untuk menganalisa arsip-arsip tulisan, grafik, gambar dengan tidak merubah objek aslinya.

c. Kesaksian ahli.

Komputer forensik pendukung penyidikan haking dan preking baru dapat sempurna apabila hasil-hasil laboratorium tersebut didukung oleh *opini* seorang saksi ahli, adapun para saksi ahli dapat digolongkan dalam 2 kategori berdasarkan pada fakta-fakta yang ditemukannya :

1) Seorang saksi ahli yang mampu menjelaskan fakta-fakta sebagaimana adanya berdasarkan pada pengetahuannya dan hasil pengujiannya dengan menggunakan *metoda-metoda tertentu*, yang berdasarkan pada urutan langkah kerja yang baku (pasti) dan sangat teliti. Sehingga fakta-fakta tersebut dapat dijelaskan sampai pada bagian-bagiannya terkecil.

2) Saksi ahli pemberi opini yang dijadikan sebagai bukti, para saksi ahli dapat memberikan pendapatnya yang berdasarkan pada pengalamannya terhadap suatu fakta atau kejadian, dengan *merinci* urutan atau kronologis kejadian tersebut serta *menentukan* apakah benar-benar hal tersebut berlangsung atau tidak. Pendapatnya ini dijadikan sebagai bukti.

Dijelaskan oleh Vogon mengenai posisi dari saksi ahli tersebut adalah sebagai berikut :

"Experts can fall into two categories :

- The specialist as Expert Witness of fact. Where a witness can state as a fact, from his own knowledge examination of a particular item, that a certain sequence of events always occurs and that this sequence followed in a particular instance.

- The specialist as Expert Witness who gives evidence of opinion. Where a witness can, from his own and experience, give an opinion as to why a certain sequence of events did or did not occur."51

Saksi ahli tersebut *tidak terbatas* hanya pada operator-operator laboratorium forensik tetapi lebih luas lagi melibatkan ahli-ahli dalam berbagai bidang antara lain ahli dalam tehnologi informasi, mendesain internet, program-program jaringan komputer serta ahli dalam bidang enkripsi / password atau pengamanan jaringan komputer. Posisi mereka berada diluar laboratorium, opini atau kesaksiannya perlu dipadukan dengan laporan-laporan formal dan fakta-fakta yang dihasilkan para operator laboratorium forensik.

Kombinasi dari fakta-fakta yang di dapat dari laboratorium forensic dan *opini para saksi ahli* diharapkan dapat membantu para penyidik dalam proses penyidikan, dimana produk penyidikan tersebut dapat diterima oleh Jaksa penuntut umum dan Hakim serta sangat berarti dalam proses peradilan. Karena kombinasi dari keduanya akan menghasilkan hal-hal sebagai berikut : *prosedur* penanganan bukti-bukti yang benar dan dapat diterima dalam proses peradilan, barang bukti *dijamin keasliannya* tidak rusak dan tidak berubah, *hasil analisa* dapat dipercaya dan akurat.

Selain itu dapat diketahui dengan pasti *sejauh mana* kerusakan atau perbedaan yang terjadi pada suatu sistem jaringan komputer, *program-program* apa yang digunakan untuk merusak, *kapan dan bagaimana* hal tersebut bisa terjadi serta dapat *diprediksi* sejauh mana hal tersebut telah mengakibatkan kerusakan atau akan dapat menimbulkan kerugian serta sejauh mana fatalitas yang akan terjadi.

---

51. Vogon. *Expert Witnesses* [Online]. Tersedia : http://www.vogon-computer-evidence.com forensic services-04.htm . [16 April 2000]. Hal. 1.

18. **Perangkat hukum khusus untuk bidang haking komputer.**

Undang-undang atau perangkat hukum positif adalah instrumen terakhir dalam menentukan berhasil atau tidak suatu penyidikan, karena penerapan delik-delik hukum yang salah akan *mementahkan* penyidikan yang telah dilakukan. Walaupun penyidiknya sudah mampu dan memahami profil dan budaya para Haker / Preker, tehnis-tehnis serta modus operandi para Haker / Preker, serta sudah didukung dengan laboratorium forensik yang canggih sekalipun.

Namun fakta–fakta yang ada menunjukkan bahwa hukum selalu ketinggalan dibandingkan dengan teknologi sebagaimana dikatakan Pandji R Hadinoto :

> "Hukum sebagai produk perkembangan sosial budaya (termasuk teknologi) disadari mau tidak mau selalu tertinggal paradigma adalah Technology Driven yang dominan, Hukum lokal menjadi semakin jauh tidak berdaya, sementara kesadaran Ahli Hukum akan Hukum Teknologi Maju seperti cyberLaw masih saja sebatas wacana melalui seminar ..."[52]

hukum berkembang secara *gradual* (deret tambah) tidak seimbang dengan teknologi yang berkembang secara *ekponensial* (deret kali), akibatnya terjadi kesenjangan dan hukum tidak mampu menjangkau fenomena yang ada.

a. Hukum positif kurang sempurna.

Beberapa fakta berikut ini menunjukkan bahwa hukum positif di Indonesia belum mampu menjawab kemajuan teknologi yang berkembang , berikut ini adalah beberapa contoh kasusnya ;

Kasus *pertama* , Indosat dan Satelindo dirugikan akibat dibobol dua perusahaan di Surabaya yang mengakses SLI dari dua operator tersebut tanpa bayar. PT Net Phone

---

52. Hadinoto Pandji R, Ir, PE, MBL, PhD. *Supremasi Teknologi Eksponensial.* [Online]. Tersedia : http://www.polri.mil.id/cyberlawboard_no2.htm . [29 Desember 2000]. Hal. 1.

Call (NPC) dan PT Ciptavisi Universal (CU) dimana pemilik perusahaan hanya membayar pulsa lokal ke Telkom, sehingga Indosat dan Satelindo tidak menikmati hasil pulsa tersebut karena alat yang disebut sebagai *Gate Way* (GW) memungkinkan mengakses ke nomor telpon di luar negeri dengan mendapat potongan biaya pulsa antara 50 % sampai dengan 65 % dari tarif internasional.

Kasus kedua , piranti lunak baru FIRETALK beredar di Indonesia untuk berbicara global tetapi membayar lokal yang merupakan inovasi teknologi penggabungan suara terintegrasi ke dalam jaringan komunikasi audio Internet, melalui : http://www.firetalk.com yang bermutu *full duplex* memungkinkan dua orang atau lebih berbicara secara simultan. Akibatnya banyak yang menghindari berbicara keluar negeri melalui fasilitas SLJJ dan SLI Telkom, sehingga pendapatan perusahaan ini menurun drastis.

Kasus ketiga , piranti lunak baru lainnya VOIP (Voice over Internet Protocol) yang memungkinkan dua orang berbicara melintasi batas negara, didepan kamera dan mike yang terpasang pada komputer. Cara ini dianggap *solusi teknologi* bukan membobol telekomunikasi SLJJ dan SLI, walaupun mengakibatkan penurunan pendapatan pada perusahaan penyedia SLJJ dan SLI

Dari ketiga contoh kasus diatas *membuktikan* bahwa perangkat hukum di Indonesia belum mampu menjangkau kecanggihan teknologi yang telah banyak digunakan Indonesia, walaupun banyak perusahaan jasa telekomunikasi yang dirugikan mereka tidak bisa menuntutnya dengan alasan ; hukum yang ada *belum* bisa menjangkau, cara-cara tersebut diatas *bukan kejahatan* tapi dianggap solusi teknologi atau pada saat dilakukan perjanjian kerja sama (pada kasus pertama diatas) perjanjiannya *tidak merinci* sampai pada penggunaan teknologi mana yang diperbolehkan atau yang dilarang.

Beberapa contoh lainnya dalam upaya menangani kasus-kasus yang terjadi dan merupakan tindak pidana, para penyidik *melakukan analogi* terhadap pasal-pasal dalam KUHP yang paralel dengan tindak pidana yang terjadi tersebut. Upaya ini mengandung banyak kelemahan antara lain sebagai berikut :

Kelemahan pertama , banyak terjadi kasus yang melanggar kesusilaan umum (violate public decency) dalam internet, pada KUHP diatur dalam pasal 282 ayat (1) yang berbunyi sebagai berikut : barang siapa menyiarkan, mempertunjukkan atau menempelkan *di muka umum* tulisan, gambar atau benda yang telah diketahui isinya melanggar kesusilaan ... dan seterusnya. Perkataan *di muka umum* dalam pasal ini sulit dikenakan terhadap layar komputer, memasukkan layar komputer termasuk ke dalam pengertian di muka umum sulit untuk diterima meskipun dengan menggunakan berbagai interprestasi. Akibatnya satu unsur perbuatan pidana yang dirumuskan dalam pasal 282 KUHP dapat gugur apabila diterapkan untuk delik susila di *cyberspace*, manakala salah satu unsur perbuatan pidana tidak terpenuhi maka perbuatan pidana tersebut *tidak dapat* dituntut sehingga tersangka bisa bebas dari jerat hukum.

Kelemahan kedua , karena di Indonesia menganut prinsip ***testimonium de auditum*** yaitu mendengar, melihat dan mengalami sendiri sebagaimana dirumuskan pasal 1 ayat (27) KUHAP. Prinsip ini menyulitkan apabila digunakan untuk kasus *cybercrime* (kejahatan di Mayantara) karena perbuatan pidana yang dilakukan oleh pelaku cybercrime biasanya dilaksanakan dalam ruangan-ruangan tersembunyi, bersifat privat dan jauh dari keramaian atau *tidak ada kontak fisik* dengan orang lain. Karakter modus operandi semacam inilah menyebabkan Kraker dan Preker sulit dilacak, tidak seperti dalam tindak pidana umum lainnya yang realtif mudah menghadirkan saksi-saksinya. Menurut pasal 184 KUHP keterangan saksi menempati urutan pertama, namun untuk perkara cybercrime hal tersebut sulit untuk dipenuhi.

Fakta-fakta diatas tersebut menunjukkan hukum positif di Indonesia tidak mampu atau lemah dalam menghadapi cybercrime seperti kreking dan preking, sehingga diperlukan hukum yang bersifat khusus dan mampu untuk menghadapinya. Indonesia perlu merujuk pada negara-negara yang sudah cukup maju instrumen hukum positifnya, seperti negara Inggris. Amerika juga dari negara tetangga Asean.

b. Hukum positif pembanding.

Negara-negara maju di dunia Inggris dan Amerika serta dari negara tetangga yaitu Singapura dan Malaysia, telah mempunyai *Cyberlaw* untuk menghadapi *Cybercrime*. Sebagian sudah cukup sempurna untuk menjerat para pelakunya namun ada juga yang belum sempurna. Contoh-contoh dari hukum positif tersebut adalah sebagai berikut :

1) Hukum positif yang digunakan di negara Inggris

Negara ini sudah cukup maju dalam menjerat tindak pidana kreking atau preking serta cybercrime lainnya sudah ada Undang-undang yang sangat khusus seperti Undang-undang penyalahgunaan komputer, Undang-undang perlindungan data, Undang-undang gangguan komunikasi serta Undang-undang lainnya yang bersifat umum tapi mendukung penyelidikan cybercrime. Undang-undang tersebut adalah sebagai berikut :

> "The Police and Criminal Evidence Act 1984 – Section 19, 20, 21, 22 and 78
> Computer Misuse Act 1990 – Section 1, 2, 3, 10 and 17
> Copyright Designs and Patents Act 1988 – Section 107,108 and 109
> Telecommunications Act 1984 – Section 42, 42A, 43, 44 and 45
> Post Office Act 1953 – Section 11
> Data Protection Act 1984
> Interception of Communications Act 1985
> Health and Safety Act 1986."[53]

---

53. Vogon. **Good Practice Guidelines** [Online]. Tersedia : http://www.vogon-computer-evidence.com/forensic_services-03.htm. [16 April 2000]. Hal. 1.

Inggris walaupun sudah lebih maju dari Indonesia namun tetap saja belum sempurna, masih ada seorang Haker disana lolos dari jerat hukum, sebagaimana dalam contoh kasus dibawah ini :

> "Salah seorang diantaranya telah berhasil mengakses file-file pribadi milik Duke of Edinburgh dan mempermainkannya dengan meninggalkan pesan "selamat siang HRH Duke of Edinburgh" tertuduh diadili berdasarkan *Forgery and Counterfeiting Act* dengan dasar melakukan *false instrument* yaitu pemalsuan dengan maksud agar digunakan oleh orang lain sebagai suatu instrumen atau informasi sebenarnya yang mengakibatkan kerugian bagi orang lain."[54]

Pada pengadilan tingkat pertama Haker tersebut dinyatakan bersalah mereka didenda 750 pounds dan yang lainnya didenda 600 pounds, tetapi putusan ini *dibatalkan* oleh Court of Appeal dan dikukuhkan oleh House of Lord yang menyatakan bahwa tindakan para pelaku itu bukanlah tindak pidana, tetapi lebih merupakan sebagai penyalahgunaan komputer atau pengacauan instalasi elektronik.

2) Hukum positif yang digunakan di negara Amerika.

Amerika Serikat merupakan negara cikal bakal internet, telah maju dalam bidang hukum yang mengatur *teknologi informasi*, *internet* dan *cybercrime*, salah satu Undang-undangnya adalah Communication Assistance for Law Enforcement Act dan Telecommunication Service tahun 1996. Undang-undang ini terpisah sama sekali dengan produk hukum yang sudah ada, dengan pertimbangan bahwa pemaksaan terhadap perlakuan suatu hukum terhadap cybercrime akan tidak optimal.

3) Hukum positif yang digunakan di negara Singapura.

---

54. Komar Mieke, Prof. DR. SH. MCL. CN dan Ahmad M Ramli, SH, MH. *Sistem Informasi Sebagai Fenomena Hukum Baru di Indonesia*, Lembaga Afiliasi Penelitian dan Industri (LAPI) – ITB , Bandung, 1998. Hal. 8.

Singapura adalah negara tetangga yang sudah cukup maju dalam perangkat hukumnya bahkan mempunyai pengalaman menyidik seorang Kraker berasal dari Indonesia (masih berumur 15 tahun) yang melakukan kegiatan kraking pada tanggal 2 Juni tahun 2000, sebagaimana dijelaskan oleh R.M. Suryo : ".Singapura telah memiliki The Electronic Act 1998 (Undang-undang tentang transaksi secara elektronik), serta Electronic Communication Privacy Act (ECPA), seperti Communication Assistance for Law Enforcement Act, Telecommunication Service 96 yang telah dijalankan di Amerika."[55]

Singapura juga sudah mempunyai *Computer Misuse Act* (Undang-undang Penyalahgunaan Komputer) yang di Singapura disebut *Cyberlaw* menurut *Inspektur Tan Chee Kiong* pejabat Kepala Cabang Kriminalitas Komputer CID (Criminal Investigation Department) Singapore, dengan Undang-undang inilah Kraker Indonesia yang tertangkap tersebut dijerat.

Adapun pasal-pasal yang dikenakan adalah pasal sektor 3 tentang *Unauthorized Access of Computer Material* dengan denda maksimal SGD$ 5000 / penjara maksimal 3 tahun, dan sektor 5 tentang *Unauthorized Modification of Computer Material* dengan denda maksimal SGD$ 10000 / penjara maksimal 3 tahun. Namun tidak terbukti karena Pengacara *Muni Oh* di persidangan berhasil melakukan pembelaan dari 16 dakwaan Jaksa Penuntut yang diajukan, dengan menangkis 11 dakwaan sehingga hanya didenda SIN$ 30,505 atas kejadian haking tersebut. Hal ini juga menunjukkan bahwasanya perangkat Cyberlaw di Singapura saat ini masih belum sempurna, atau

---

55. Suryo R.M. *Mendesak CyberLaw untuk Indonesia.* [Online]. Tersedia : http://www .polri .mil.id cyberlaw board no2.htm [16 April 2000]. Hal. 2.

memiliki ruang gerak untuk terjadinya perbedaan pendapat yang memberikan advantage (keberuntungan) bagi pelaku Cybercrime.

4) Hukum positif yang digunakan di negara Malaysia.

Negara Malaysia sudah mempunyai hukum yang bersifat lex spesialis untuk cybercrime atau Malaysia sudah mempunyai cyberlaw Undang-undang tersebut adalah Digital Signature Act Tahun 1997 dan Digital Mellinnium Copyright Act. 1998.

Hukum positif di negara lain tersebut yang telah lebih baik dari Indonesia, serta berpengalaman dalam menyidik *cybercrime* termasuk haking, kraking dan preking perlu dijadikan *bahan konsepsi* perangkat hukum yang khusus untuk bidang haking komputer atau kejahatan komputer lainnya di Indonesia. Dengan kata lain patut dijadikan bahan acuan untuk *konsep cyberlaw*, yang akan diberlakukan di Indonesia sebagai *hukum positif*.

c. Cyberlaw yang diperlukan di Indonesia.

Undang-undang ini maksudnya adalah hukum yang mengatur segala sesuatu yang berhubungan dengan cyberspace atau *ruang mayantara* , yaitu objek yang seolah-olah ada atau riil yang tercipta karena adanya internet, namun sebetulnya objek-objek tersebut maya yang nampak hanyalah tampilan hasil-hasil program komputer yang seolah-olah nyata (virtual realty). Sedangkan objek dari pada Undang-undang ini adalah segala sesuatu yang berhubungan dengan penggunaan komputer, jaringan komputer , teknologi informasi serta kejahatan-kejahatan yang menggunakan hal-hal tadi sebagai alat atau media untuk melakukan kejahatan, termasuk kejahatan komputer secara umum serta haking, kraking dan preking.

Menurut Atip Latifulhayat : "Istilah *cyberspace* untuk pertama kalinya diperkenalkan oleh William Gibson seorang penulis fiksi ilmiah (science fiction) dalam

novelnya yang berjudul Neuromancer. Istilah yang sama kemudian diulanginya dalam novelnya yang lain yang berjudul Virtual Light."[56] . Sedangkan fungsi dan posisi hukum ini adalah sebagai berikut : pada media *cyberspace* terdapat *cybercrime* yaitu pengguna media yang jahat melakukan tindak pidana yang melanggar *cyberlaw* dan disidik oleh *cybercop* atau *cyber police*.

Berdasarkan hal tersebut diatas cyberlaw memang harus *lex spesialis* untuk menangani hal-hal yang bersifat *serba cyber* juga harus dapat menunjang para penyidik atau penegak hukum yang khusus menangani bidang ini (cybercop) , sedangkan fenomena cybercrime termasuk haking, kraking dan preking bila *ditinjau* dari segi unsur pidana atau delik hukumnya : ada *unsur perbuatan* yang melanggar hukum serta ada *unsur akibat* dari perbuatan tersebut. Sehingga konsepsi cyberlaw yang diperlukan di Indonesia harus lengkap untuk menjerat unsur-unsur dimaksud, adapun konsepsi cyberlaw tersebut adalah sebagai berikut :

1) Konsepsi cyberlaw bersifat lex spesialis (pokok / inti), yaitu yang khusus untuk menjerat *unsur-unsur perbuatan* pelaku cybercrime.

a) Undang-undang penyalahgunaan komputer (Computer Misuse Act).

Maksudnya untuk menjerat para cybercrime apabila memodifikasi perangkat *keras komputer* (modem, kabel-kabel coaxial) atau memodifikasi *program-program* komputer menjadi program jahat (membuat virus, worm serta Trojan horse), serta agar masyarakat mengetahui bahwa perbuatan tersebut melanggar hukum.

---

56. Latifulhayat Atip, SH, LLM. ***Cyberlaw dan Urgensinya bagi Indonesia.*** [Online]. Tersedia : http://www.polri.mil.id/Cyber_pol/CYBERLAW_URGEN.HTM [29 Desember 2000]. Hal. 1.

b) Undang-undang perlindungan data (Data Protection Act).

Maksudnya untuk melindungi data-data yang dimiliki oleh individu atau suatu organisasi, serta menghukum apabila ada seseorang yang mengambil data secara tidak sah walaupun belum menggunakannya. Contohnya : seseorang mencatat nomor telepon, nomor kartu kredit bahkan Nrp anggota Polisi atau password komputer dengan tanpa seijinnya, atau tanpa seijin pemilik yang sah memberikan data dimaksud kepada orang lain akan dianggap melanggar hukum.

c) Undang-undang gangguan komunikasi (Interception of Communication Act).

Maksud Undang-undang ini lebih menitik beratkan untuk melindungi materi atau informasi yang dikomunikasikan bukan alat komunikasinya. Dalam mengirim e'mail bisa saja materi atau data di dalamnya dirubah. diharapkan orang yang melakukan tersebut perbuatannya dapat dijerat oleh Undang-undang dimaksud.

d) Undang-undang perlindungan kerahasiaan komunikasi elektronik (Electronic Communication Privacy Act / ECA).

Maksudnya untuk melindungi komunikasi elektronik yang biasanya datanya di *enkripsi* agar tidak bisa dibaca atau dilihat oleh yang tidak berhak. namun para cybercrime bisa memecah kode enkripsi tersebut . Perbuatan ini dapat dianggap melanggar hukum walaupun tidak atau belum menimbulkan kerugian.

e) Undang-undang keabsahan data dan tanda tangan digital (Digital Signature Act).

Pada saat sekarang ini data digital atau tanda tangan seseorang

yang berupa kode-kode digital *belum dianggap* sah atau diterima sebagai alat bukti demikian juga log file pada server serta log file di chat room IRC (internet relay chat), diharapkan apabila Undang-undang ini telah ada maka hal tersebut dianggap sah dalam proses hukum atau dalam melakukan perjanjian-perjanjian bisnis yang menggunakan media elektronik. Selain itu apabila ada seseorang yang menyalahgunakannya, dapat dianggap melanggar hukum dan diajukan ke pengadilan.

f) Undang-undang perlindungan perniagaan secara elektronik (Electronic Commerce Protection Act).

Maksud Undang-undang ini untuk *melindungi* konsumen juga para pedagang yang melakukan transaksi menggunakan media e'commerce di internet, diharapkan dapat *menentukan* apakah transaksi tersebut sah / legal atau batal, apakah *pembayaran* sudah dilaksanakan atau belum, apakah *produk/barang atau jasa* dianggap sudah diterima atau belum oleh yang berhak. Selain itu diharapkan dapat *menjerat* para pelaku yang melanggar ketentuan-ketentuan tersebut, atau bila melakukan penipuan / wanprestasi (perdata).

g) Undang-undang hak cipta media digital (Digital Copyright Act).

Maksudnya untuk melindungi hak cipta yang dibuat berdasarkan pada *program-program komputer* serta ditayangkan dengan secara digital *pada media internet*, belum berupa brosur-brosur hasil cetakan atau terekam pada CD, pita magnetic. Contohnya antara lain ; *citra* yang terlihat pada suatu website, *animasi-animasi*, produk yang berupa *video* ataupun *audio* (terutama musik) yang ditayangkan di internet.

h) Undang-undang telekomunikasi dan teknologi informasi (Telekomunication and Information Technology Act).

Maksudnya untuk mengatur *tata cara* menyelenggarakan pelayanan telekomunikasi dan mengatur *penggunaan* teknologi informasi antara lain internet, selain mengatur bidang telekomunikasi juga harus mampu mengatur *prosedur-prosedur* penggunaan internet, *hak dan kewajiban* penyelenggara juga pengguna internet serta *perlindungan* terhadap website atau domain-domain yang ada di internet.

Selain itu untuk *menjerat secara hukum* apabila penyelenggara atau pengguna menyalahgunakannya serta tidak melakukan kewajiban-kewajibannya , juga secara langsung / tidak langsung menimbulkan kerugian dan gangguan keamanan bagi masyarakat diluar pengguna jasa telekomunikasi dan internet tersebut (sudah ada Undang-undang No. 3 tahun 1989 tentang Telekomunikasi namun belum mengatur penggunaan teknologi informasi khususnya internet).

2) Konsepsi cyberlaw yang bersifat pendukung.

Konsepsi cyberlaw yang bersifat pendukung, yaitu yang khusus untuk menjerat *unsur-unsur akibat*, dari pelaku cybercrime melakukan tindak pidana Kraking ataupun Preking. Undang-undang ini bukanlah Undang-undang yang khusus untuk menangani fenomena-fenomena yang ada di cyberspace, tetapi perlu dijadikan konsepsi sebagai *pendukung* cyberlaw karena fenomena cybercrime juga akibat-akibat yang ditimbulkannya melanggar Undang-undang seperti yang tersebut dibawah ini (sebagian sudah ada dan menjadi hukum positif, sebagian masih dalam proses untuk diundangkan) :

a) Undang-undang No. 3 tahun 1971 tentang Pemberantasan tindak pidana korupsi.

b) Undang-undang No. 6 tahun 1984 tentang Pos.

c) Undang-undang No. 4 tahun 1990 tentang Serah simpan karya cetak dan karya rekam.

d) Undang-undang No. 7 tahun 1992 tentang Perbangkan.

e) Undang-undang No. 8 tahun 1995 tentang Pasar modal.

f) Undang-undang No. 12 tahun 1997 tentang Hak cipta.

g) Undang-undang No. 13 tahun 1997 tentang Paten.

h) Undang-undang No. 14 tahun 1997 tentang Merek.

i) Undang-undang Keselamatan dan perlindungan negara.

Undang-undang ini masih dalam proses dan masih diperdebatkan oleh masyarakat belum diundangkan sampai sekarang, dulu disebut *Undang-undang anti subversif*. Di negara manapun di dunia Undang-undang ini selalu ada untuk mencegah negara tersebut dari tindakan-tindakan subversi atau tindakan yang akan memecah belah negara tersebut, juga untuk mencegah infiltrasi dan invasi dari negara asing atau musuh negara. Kreking dan Preking dapat dijadikan *senjata ampuh* untuk sabotase, propaganda yang bersifat subversif atau tindakan-tindakan lainnya yang dapat menyerang keselamatan dan keutuhan suatu negara.

3) Konsepsi Cyberlaw dari KUHP.

Sebagian kecil unsur-unsur *perbuatan* cybercrime khususnya Kraking dan Preking memenuhi *delik-delik* pidana dalam KUHP, dan unsur-unsur *akibat dari perbuatan* cybercrime tersebut sebagian besar

memenuhi delik-delik pidana dalam KUHP. Penerapannya diperlukan analogi dan interpretasi lebih lanjut, yang memberikan peluang pada para penegak hukum berbeda pendapat (kepastian hukum diragukan). Adapun pasal-pasal tersebut adalah sebagai berikut :

1) Tindak pidana yang berkaitan dengan kepentingan negara dan pertahanan keamanan, pasal 112 – 118 KUHP.

2) Menyebarkan kebencian terhadap pemerintah, pasal 154-155 KUHP.

3) Informasi / pernyataan permusuhan atau penghinaan terhadap golongan-golongan rakyat Indonesia, pasal 157 KUHP.

4) Informasi untuk menghasut masyarakat, pasal 160-161 KUHP.

5) Informasi terhadap sarana kriminalitas, pasal 163-163-163 bis KUHP.

6) Kejahatan terhadap kesopanan / susila, pasal 282 - 283 KUHP.

7) Pencurian, pasal 362 KUHP.

8) Penggelapan, pasal 372 KUHP.

9) Penipuan, pasal 378 KUHP.

Konsepsi cyberlaw tersebut yang diperlukan untuk menangani cybercrime (Haking, Kraking dan Preking), juga *harus menjangkau* kejahatan komputer lainnya diluar cybercrime. Konsep cyberlaw ini perlu *mencontoh* dari negara-negara yang sudah mempunyainya dan berpengalaman menggunakan Undang - undang tersebut , sehingga dapat diketahui secara pasti kelebihan dan kekurangan Undang-undang tersebut.

Konsep penerapan Undang-undang ini (cyberlaw) yang ideal, adalah mengutamakan Undang-undang yang bersifat lex spesialis, selanjutnya Undang-

undang lain yang mendukung cyberlaw, kemudian terakhir KUHP diterapkan. Tidak terbalik seperti sekarang justru KUHP yang dikedepankan. Dengan kata lain, *tuduhan primernya* menggunakan cyberlaw yang bersifat lex spesialis (contoh : UU Penyalahgunaan komputer), *tuduhan subsider* menggunakan Undang-undang pendukung cyberlaw (contoh : UU No. 7 tahun 1992 tentang Perbangkan), *tuduhan lebih subsider* menggunakan KUHP (Contoh : pasal 372 jo 378 KUHP).

Secara umum *konsepsi ideal* kemampuan penyidikan dan konsepsi komputer forensik serta perangkat hukumnya adalah ; bagaimana mewujudkan profil para penyidik yang berpengalaman lebih dari 3 tahun sebagai penyidik lanjutan, berpendidikan programer komputer mampu menggunakan program LINUX, UNIX biasa digunakan oleh Haker, sehingga mengetahui budaya para Haker, tehnis melakukan haking / modus operandinya. Didukung oleh laboratorium forensik khusus kejahatan komputer, juga didukung saksi-saksi ahli di bidang komputer. Kemudian penyidiknya mampu menerapkan cyberlaw yang bersifat lex spesialis, tidak terbatas pada pasal-pasal dalam KUHP saja.

Kotak dialog . 3

Dari Citizen ke Netizen

Fenomena cyberspace ternyata komplek terutama masalah hukum yang menyangkut perniagaan dan kejahatan, contohnya ; seseorang melakukan transaksi dari negara Indonesia ke Australia. Bagaimanakah pajaknya ? Australia menganut *e'commerce* harus bebas pajak tapi Indonesia tidak setuju . Uang yang digunakanpun menjadi masalah walaupun menggunakan kartu kredit harus dikonversi ke dollar Amerika kemudian ke Australia.

Contoh lain A (warga negara Amerika) melakukan kraking dari New York mencuri dana dari Bank Bali di Jakarta milik B (warga negara Indonesia), lalu mentrasfernya ke rekening C (warga negara Swiss) di Swiss. Walaupun cyberlaw di Indonesia sudah lengkap, persoalannya adalah Bagaimana penyidikannya karena A dan C adalah WNA dan berada di negaranya masing-masing. Mampukah Undang-undang yang ada di Indonesia menjangkau mereka.

Jalan keluarnya *Citizen* ditingkatkan menjadi *Netizen*. Undang-undang yang berlaku terhadap A , B dan C sama karena mereka *satu netizen* (contoh : Amazon.com netizen), mata uangnya sama *Electron*. *Cybercop dari Mabes Polri* harus menguasai *Netizen Law* yang berlaku dan melakukan penyelidikan atas dasar Undang-undang ini, ia mampu melakukan penyidikan dengan *tidak mengenal batas-batas negara* asalkan masih dalam netizen yang sama. *netizen law* yang berlaku di Indonesia bisa bermacam -macam (Amazon.com Law, Yahoo.com Law, dsb). Seorang citizen Indonesia bisa menjadi netizen di berbagai dot com, begitupun cybercop Mabes Polri dapat menyidik diberbagai dot com. dunia tanpa negara terwujud.

MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

Bab. VI

BAB VI

PEMAHAMAN / KEMAMPUAN PARA PENYIDIK POLRI

MENYIDIK HAKING KOMPUTER

Dalam melakukan penyidikan haking komputer diperlukan penyidik Polri yang memahami fenomena haking komputer secara menyeluruh dan utuh serta mampu dan menguasai tehnik-tehnik penyelidikan dan penyidikan sebagaimana lazimnya para penyidik atau penyidik pembantu Polri, untuk mengetahui kondisi para penyidik Polri terhadap hal tersebut dilakukan wawancara dengan para penyidik Polri. Responden diambil dari personil Direktorat Reserse Mabes Polri Bagian Reserse Ekonomi sebanyak 25 orang (100 %), dan responden dari Direktorat Reserse Polda Jawa Tengah sebanyak 10 responden (100 %).

Tidak seluruh anggota Reserse dijadikan responden hanya pada Subdit Reserse Ekonomi dengan pertimbangan bagian tersebut biasanya menangani kasus-kasus *tindak pidana ekonomi* yang berlatar belakang komputer, ataupun kasus diluar bidang tindak pidana ekonomi namun menggunakan komputer sebagai sarana kejahatannya. Responden-responden tersebut diwawancarai untuk mengetahui sejauh mana penguasaan mengoperasikan komputer, pemahaman terhadap Haking komputer dan kemampuan menyidiknya serta faktor-faktor yang sangat berpengaruh (Determinant).

19. Penguasaan Operasional komputer.

a. Data, status dan pendidikan responden.

Jumlah responden seluruhnya 35 orang (Mabes Polri 25 responden dan Polda Jawa Tengah 10 responden), pengalaman dan lama mereka bertugas di Reserse serta pendidikannya adalah sebagai berikut :

1) Lama bertugas sebagai penyidik dibidang Reserse Ekonomi.

a) Dibawah 3 tahun : 20 orang (57,14 %).

b). Diatas 3 tahun : 15 orang (42,85 %).

2) Lama bertugas sebagai penyidik diluar bidang Reserse Ekonomi.

a) Dibawah 3 tahun : 25 orang (71,42 %).

b). Diatas 3 tahun : 10 orang (28,57 %).

Dari data tersebut menunjukkan bahwa responden cukup berpengalaman sebagai penyidik dan bekerja di satuan Reserse Polri. 42,85 % responden cukup berpengalaman dibidang Reserse Ekonomi. Adapun dari segi pendidikannya yang telah melaksanakan Dikjur lanjutan Reserse dan pendidikan formal dibidang komputer baik sebagai operator ataupun programmer, adalah sebagai berikut :

1) Pendidikan Kejuruan Reserse.

a) Pendidikan kejuruan lanjutan : 21 orang (60 %).

b). Pendidikan kejuruan dasar (tidak Dikjur) : 14 orang (40 %).

2) Pendidikan / kursus komputer.

a) Pernah pendidikan kursus komputer : 8 orang (22,85 %).

b). Belum pernah pendidikan komputer : 27 orang (77,14 %).

Dari data tersebut penyidik yang telah mengikuti pendidikan kejuruan lanjutan 60 % sedangkan yang pernah mengikuti pendidikan komputer sangat minim hanya 22,85 %. dari yang pernah dididik komputer tersebut hanya *1 responden* (2,85 %) berkualifikasi sebagai *programer*, sisanya *7 responden* (20 %) sebagai *operator*.

b. <u>Pengetahuan dan kemampuan mengoperasikan komputer.</u>

Haking komputer penyidikannya perlu dilakukan oleh para penyidik yang

mengetahui pengetahuan dan kemampuan mengoperasikan komputer, untuk mengetahui hal ini kepada responden ditanyakan pertanyaan-pertanyaan sebagai berikut :

1) Menanyakan apakah bisa mengoperasikan komputer, responden diminta memperagakan dari *mulai start*, *menggunakan* salah satu aplikasi sampai dengan prosedur *shut down*.

2) Menanyakan apabila menggunakan komputer, apakah hanya untuk mengetik atau digunakan untuk *mengolah* data serta *menganalisanya*.

3) Menanyakan program aplikasi (software) apa saja yang sering ia gunakan, diharapkan responden mampu menggunakan software *text file* (Microsoft word, dll), software *pengolahan data / program* (Foxpro, Dbase dan lain-lain) , dan diharapkan mengerti serta bisa menggunakan software seperti *LINUX, UNIX* serta *Python*.

4) Menanyakan apakah sering menggunakan Internet dan mempunyai *user ID* di salah satu ISP (Internet Service Provider), diharapkan paling tidak responden telah berlangganan selama 6 bulan.

Berdasarkan jawaban-jawaban responden terhadap pertanyaan tersebut, dapat diketahui *pengetahuan* dan *kemampuan* mengoperasikan komputer para responden sebagai berikut :

1) Kemampuan mengoperasikan komputer dan menggunakan program aplikasi.

a) Dapat mengoperasikan komputer : 30 responden (85,71 %).

b) Tidak dapat mengoperasikan komputer : 5 responden (14,28 %)

dari data tersebut menunjukkan bahwa walaupun responden yang mempunyai pendidikan komputer hanya 8 responden (22,85 %), namun yang mampu

mengoperasikan komputer 30 responden (83,71 %). Artinya sebagian responden mampu mengoperasikan komputer secara otodidak, atau karena komputer tersedia mereka mencoba memanfaatkan dan menggunakannya.

2) Penggunaan / pemanfaatan komputer, dari jawaban responden ternyata hampir seluruh komputer-komputer yang ada dikantor mereka hanya dipergunakan untuk *mengetik* bukan untuk mengolah dan menganalisa data, mereka gunakan untuk mengetik berita acara pemeriksaan, pemberkasan dan membuat laporan-laporan lainnya. Artinya walaupun ada diantara mereka yang berpendidikan sebagai programer namun kenyataannya hanya mengerjakan pekerjaan-pekerjaan sebagai operator komputer.

3) Program aplikasi yang sering dipergunakan, sebagaimana data diatas komputer digunakan hanya digunakan untuk pengetikan, hampir seluruh responden menjawab sering menggunakan *software text file* Microsoft word dan *software Grafis* Microsoft Power point, seluruhnya belum pernah ada yang menggunakan *software pengolahan data / program* (Foxpro, Dbase dll) demikian juga belum pernah menggunakan software LINUX, UNIX serta Python (tidak ada komputer yang diinstal software ini).

4) Pengetahuan mengenai Internet, seluruh responden (100 %) belum mempunyai user ID atau tidak berlangganan Internet di ISP, hanya 2 responden (5,71 %) yang pernah menggunakan fasilitas Internet meminjam dari orang lain. Yang lainnya hanya mendengar ada Internet namun tidak tahu wujudnya seperti apa dan tidak pernah menggunakannya.

Dari data tersebut para responden atau para penyidik di bagian Reserse Ekonomi sangat terbatas pengetahuan dan kemampuannya dalam mengoperasikan komputer, walaupun ada yang berpendidikan *sebagai programer* namun hanya mengerjakan pekerjaan-pekerjaan

sebagai operator jadi bisa dikatakan 100 % responden terbatas kemampuan hanya sebagai operator. Sedangkan penggunaan komputer 100 % hanya digunakan *untuk pengetikan* dan hanya menggunakan *software text file*, belum pernah menggunakan software pengolahan data / program bahkan tidak ada komputer mereka yang diinstal software tersebut.

20. **Pemahaman terhadap Haking komputer dan kemampuan menyidiknya.**

Untuk mengetahui sejauh mana para responden memahami Haking komputer dan mengetahui sejauh mana kemampuan penyidikannya, kepada para responden ditanyakan pertanyaan mengenai hal-hal sebagai berikut :

a. Pengetahuan mengenai program jahat komputer (Virus, Worm, Trojan horse, dsb) serta fenomena haking komputer, dengan pertanyaan-pertanyaan spesifik sebagaimana dibawah ini :

1) Menanyakan apakah mengerti yang dimaksud dengan *program–program jahat* komputer.

2) Menanyakan apa perbedaan *Virus* dan *Worm* serta apa program jahat *Trojan horse*

3) Menanyakan apakah mengerti fenomena *Haking komputer*, bila mengerti selanjutnya ditanyakan apa bedanya *Haker*, *Kraker* dan *Preker*.

b. Pengetahuan mengenai modus operandi para Haker, dan program-program Haking komputer, dengan pertanyaan-pertanyaan spesifik sebagaimana dibawah ini :.

1) Menanyakan apakah seluruh Haker jahat ?. dan bagaimana *profil* mereka ?.

2) Menanyakan *program-program* apa yang digunakan untuk melakukan Haking komputer.

3) Menanyakan bagaimana *kronologis* seorang Haker memasuki suatu jaringan komputer.

4) Menanyakan *kejahatan-kejahatan* apa dan *gangguan* yang bisa dilakukan para Kraker dan Preker , pada Internet, jaringan komputer lainnya dan jaringan telepon.

5) Menanyakan *pasal-pasal* apa yang bisa diterapkan, siapa yang menjadi kemungkinan *tersangka / saksi / korban*, barang bukti apa yang *harus disita*.

c. Pengalaman melakukan penyidikan terhadap tindak pidana yang menggunakan komputer dan program komputer sebagai alat kejahatan.

Sebagaimana dalam Pasal 1 ayat 2 KUHP penyidikan adalah "serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumnpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya."[57] , dengan tindakan-tindakan seperti penangkapan, penahanan, penggeledahan dan penyitaan serta mendatangkan saksi ahli.

Adapun pertanyaan-pertanyaan spesifik untuk mengetahui kondisi responden terhadap hal tersebut, adalah sebagai berikut :

1) Meminta agar responden *menceritakan* pengalamannya secara kronologis dan singkat.

---

67. Nusantara Abdul Hakim G. SH. LLM dkk. *KUHAP*. Djambatan. Jakarta. 1986. Hal. 5.

2) Menanyakan *pasal-pasal* apa yang telah diterapkan, siapa yang menjadi *tersangka / saksi / korban*, *barang bukti* apa yang telah disita.

3) Menanyakan apakah berkas perkara *dikirim* atau *tidak* kepada Jaksa penuntut umum, apakah perkara tersebut *sudah* divonis atau belum.

4) Menanyakan apa *kendala-kendala* dalam menyidik kasus tersebut, apakah *saksi ahli* digunakan atau tidak.

Berdasarkan pertanyaan-pertanyaan tersebut diatas *pengetahuan / pemahaman* para responden dapat diketahui, (setelah dilakukan wawancara) adapun hasilnya adalah sebagai berikut :

a. Pengetahuan / pemahaman program jahat komputer dan fenomena haking komputer.

1) Pengetahuan / pemahaman terhadap program jahat komputer (Virus, Worm, Trojan horse dsb) sebagai berikut :

a) 8 responden (22,85 .%) mengetahui Virus komputer dan akibat yang ditimbulkannya.

b) 1 responden (2,85 %) mengerti program Worm dan Trojan horse serta cara kerjanya.

2) Kemampuan membedakan antara Virus dan Worm serta program jahat Trojan horse, hanya 1 responden (2,85 %) yang mengetahui dan bisa membedakan hal tersebut.

3) Pengetahuan / pemahaman mengenai fenomena haking komputer dan kemampuan membedakan antara Haker, Kraker dan Preker

a) 8 responden (22,85 %) mengerti fenomena haking komputer umumnya tidak mengetahui bedanya antara Haker, Kraker dan Preker.

b) 1 responden (2,85 %) mengerti perbedaan antara Haker, Kraker dan Preker.

Dari data tersebut dapat diketahui bahwa pengetahuan / pemahaman para responden terhadap program jahat komputer dan haking komputer sangat minim, artinya pengetahuan para penyidik Polri terhadap hal tersebut hanya terbatas pada Virus komputer dan akibat yang ditimbulkannya, tidak mengetahui program Worm dan Trojan horse apalagi membedakannya. Hampir seluruhnya para penyidik Polri tidak mengetahui perbedaan antara Haker, Kraker dan Preker (hanya 1 responden yang mengetahui hal tersebut).

b. Pengetahuan / pemahaman modus operandi para Haker dan program-program haking komputer.

1) Pengetahuan / pemahaman motivasi para Haker dan profil mereka.

a) 1 responden (2,85 %) mengetahui bahwa tidak semua Haker jahat, ada yang hanya untuk iseng atau karena keingin tahuan yang tinggi dari pelakunya.

b) Hampir seluruh responden tidak mengetahui secara pasti bagaimana profil para Haker.

2) Pengetahuan / pemahaman program-program yang digunakan untuk melakukan haking komputer.

a) Hanya 1 responden (2,85 %) yang mengetahui program-program komputer diantaranya menyebutkan program LINUX, UNIX dan Window NT.

b) Responden lainnya tidak mengetahui sama sekali hal tersebut.

3) Pengetahuan / pemahaman kronologis seorang Haker memasuki jaringan

komputer. Tidak ada seorang respondenpun yang mampu untuk menggambarkan bagaimana seorang Haker secara illegal memasuki suatu jaringan komputer yang menjadi sasarannya, pengetahuan mereka hanya *sebatas* bahwa Haker mampu mengganggu suatu jaringan komputer.

4) Pengetahuan / pemahaman *kejahatan-kejahatan* apa dan *gangguan* yang biasa dilakukan para Kraker dan Preker, pada Internet, jaringan komputer lainnya dan jaringan telepon.

a) Hanya 1 responden (2,85 %) yang mengetahui kejahatan dan gangguan yang bisa ditimbulkan oleh para Haker, Kraker dan Preker, sedangkan responden yang lainnya tidak mengetahui hal tersebut.

b) Responden yang satu itu (berpendidikan programer) dapat memprediksi kejahatan-kejahatan para Kraker / Preker antara lain ; pencurian, sabotase dan mengganggu Webiste yang ada di Internet serta mencuri pulsa telepon.

5) Pengetahuan / pemahaman *pasal-pasal* apa yang bisa diterapkan, siapa yang dapat, menjadi *tersangka / saksi / korban*, serta *barang bukti* apa yang bisa disita.

a) 4 responden (11,42 %) menyebutkan bisa diterapkan pasal : 362 KUHP (Pencurian), 372 KUHP (Penggelapan), 378 KUHP (Penipuan) dan 335 KUHP (Perbuatan tidak menyenangkan) serta pengrusakan (KUHP).

b) 1 responden (2,85 %) dapat menyebutkan pasal-pasal tersebut diatas ditambah dengan 263 KUHP (Memalsukan surat-surat), 282 dan 283 KUHP (Kejahatan terhadap kesopanan) serta 154 KUHP (Menyebarkan kebencian terhadap pemerintah).

Dari data tersebut dapat diketahui bahwa pengetahuan / pemahaman para responden terhadap *modus operandi para Haker* dan *program-program haking komputer* juga sangat minim, artinya hampir semua penyidik Polri yang menjadi responden tidak mengetahui motivasi para Haker dan profilnya mereka tidak bisa membedakan antara Haker, Kraker dan Preker. Hampir semuanya tidak mengetahui program-program komputer yang biasa digunakan oleh para Haker (hanya 1 responden yang tahu).

Tidak ada seorangpun responden yang mengetahui bagaimana seorang Haker memasuki suatu jaringan komputer secara tidak sah, artinya mereka tidak tahu sama sekali modus - modus operandi para Haker, Kraker dan Preker dalam melakukan aksinya, hanya *1 responden* yang mengetahui kejahatan dan gangguan apa saja bisa ditimbulkan para Haker, Kraker dan Preker. Pengetahuan para responden mengenai penerapan pasal-pasal KUHP untuk menjerat para Kraker dan Preker sangat minim, hanya terbatas pada pasal-pasal dalam KUHP saja.

c. Pengalaman melakukan penyidikan terhadap tindak pidana yang menggunakan komputer dan program komputer sebagai alat kejahatan.

1) 3 responden (8.57 %) mempunyai pengalaman menyidik penipuan kartu kredit yang menggunakan fasilitas dot commerce di Internet yaitu para penyidik dari *Dit Serse Umum Polda Jawa Tengah*, sedangkan sisanya termasuk para penyidik dari Subdit Reserse Ekonomi Mabes Polri tidak ada yang berpengalaman terhadap hal tersebut. Beberapa penyidik yang mempunyai pengalaman mengenai kasus ini telah dimutasikan, terhadap ketiga responden dari *Dit Serse Umum Polda Jawa Tengah* dilakukan wawancara pada tanggal *20 Januari 2001* bertempat di Markas Polda Jawa Tengah. Nama

dan jabatan para penyidik tersebut adalah sebagai berikut :

a) AKBP Drs Arif Darmawan (Kabag Serse Umum).

b) AIPDA Gigih Tjahyono (Penyidik).

c) BRIPKA Suryanto Dananjaya (Penyidik pembantu).

2) Para penyidik tersebut menjerat tersangka *Adhenico Agusta dkk* dengan pasal 378 KUHP junto 363 KUHP, adapun yang menjadi *saksi* adalah petugas jasa kurir Federal Expres (Fedex). Sedangkan *barang bukti* yang disita adalah : komputer-komputer yang digunakan oleh para tersangka dan barang-barang hasil dari kejahatan.

3) Berkas perkara belum bisa dikirim ke Jaksa penuntut umum dan para tersangka ditangguhkan karena alat-alat bukti belum lengkap.

4) Kendala-kendala utama yang mereka hadapi adalah tehnis pembuktian, saksi-saksi yang ada di luar negeri, saksi ahli yang belum ada serta belum adanya fasilitas komputer forensik.

Dari data responden tersebut dapat diketahui bahwa pengalaman menyidik kasus atau tindak pidana yang menggunakan komputer dan program komputer sebagai alat kejahatan sangat minim, hanya 3 responden yang mempunyai pengalaman hal tersebut. Ketiga responden ini *bukan termasuk* responden yang memahami modus-modus operandi para Haker dan program-program yang digunakan oleh para Haker, untuk melakukan aksinya.

Pengalaman para responden tersebut dalam menyidik tersangka *Adhenico dkk* masih terbatas menggunakan pasal 378 KUHP junto 363 KUHP, mereka menemukan *kendala* dalam penyidikannya terutama dalam *pembuktian* , kesaksian serta sarana komputer forensik yang belum ada. Sehingga kasus yang ditanganinya belum bisa diajukan ke Jaksa penuntut umum, dan para tersangka terpaksa ditangguhkan.

21. **Faktor-faktor yang sangat berpengaruh (Determinant).**

Secara umum penguasaan operasional komputer dan pemahaman terhadap haking komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus tersebut dari para penyidik Polri masih sangat minim. banyak faktor-faktor yang mempengaruhi hal tersebut namun dari beberapa faktor tersebut ada yang sangat *berpengaruh* (Determinant), adapun faktor-faktor *determinan* tersebut adalah sebagai berikut :

a. Faktor determinan yang mempengaruhi kemampuan mengoperasikan komputer.

Ada tiga faktor yang mempengaruhi hal tersebut diatas, dari ketiga faktor tersebut faktor pendidikan formal dibidang komputer lebih dominan dibandingkan faktor-faktor lainnya, adapun faktor-faktor tersebut adalah sebagai berikut :

1) Pendidikan formal komputer, antara lain kursus-kursus komputer dan pendidikan komputer di luar Polri atau pendidikan kejuruan komputer yang diselenggarakan Polri.

2) Sarana / prasarana komputer yang tersedia di lingkungan kerja para penyidik Polri, artinya walaupun para penyidik *tidak dididik secara formal* dalam bidang komputer namun apabila di lingkungan kerjanya *tersedia* sarana komputer sangat berpengaruh terhadap kemampuan dalam mengoperasionalkan komputer.

3) Program-program aplikasi yang sering digunakan, serta penggunaan komputer yang tak sesuai dengan fungsinya (mengolah data) atau hanya digunakan untuk mengetik.

b. Faktor determinan yang mempengaruhi kemampuan para penyidik dalam memahami modus operandi para Haker dan program-program haking komputer.

1) Tingkat pendidikan formal penyidik Polri dalam bidang komputer.

Hal tersebut diatas *sangat berpengaruh*, terutama apabila pendidikannya mencapai *level (tingkat) programer*, ia akan cukup mampu untuk memahami modus operandi para Haker dan program-program haking komputer bahkan *dapat memprediksi* kejahatan-kejahatan atau gangguan yang dapat dilakukan oleh para Kraker / Preker dengan baik.

Selain itu mampu menerapkan pasal-pasal dalam KUHP lebih baik, dibandingkan dengan pendidikannya hanya pada tingkat operator komputer.

2) Status para penyidik sebagai pengguna / pelanggan Internet.

Apabila ia telah menggunakan Internet atau menjadi pelanggan pada salah satu ISP (Internet Service Provider) juga sangat menentukan, apabila ia sebagai pelanggan akan lebih dapat memahami bagaimana Haker melakukan aksinya.

c. Faktor determinan yang mempengaruhi kemampuan melakukan penyidikan.

Ada empat faktor yang sangat berpengaruh terhadap kemampuan penyidik Polri dalam menyidik kasus-kasus yang berhubungan dengan Haker / Kraker dan Preker, diantara faktor-faktor tersebut yang *paling dominan* berpengaruh adalah *pengalaman* para penyidik menangani kasus-kasus dimaksud. Adapun faktor-faktor tersebut adalah sebagai berikut :

1) Faktor pengalaman penyidik.

Responden-responden dari Direktorat Reserse Polda Jawa Tengah walaupun pendidikan formal dibidang komputer hanya sebatas operator bahkan ada yang belum pernah mendapatkan pendidikan komputer, dan seluruhnya bukan pelanggan Internet. Karena mereka menangani kasus yang berhubungan dengan penipuan kartu kredit yang menggunakan fasilitas *dot commerce* di

Internet, akibatnya cukup menguasai / memahami masalah-masalah yang berhubungan dengan prosedur Internet, haking komputer dan preking.

2) Faktor sistem pembuktian.

Jaksa penuntut umum masih meminta keterangan saksi dalam bentuk berita acara pemeriksaan yang *formal*, sehingga diperlukan pemanggilan saksi / korban yang ada di luar untuk dibuatkan berita acaranya di Indonesia, belum bisa menerima *pernyataan korban atau saksi* dalam bentuk e-mail atau print out facximile sebagai alat bukti.

3) Fasilitas komputer forensik.

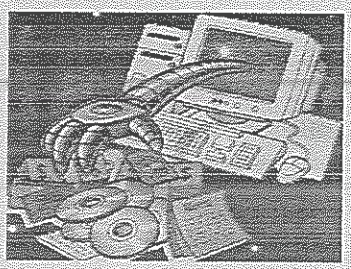
Untuk membuktikan jejak-jejak para Haker , Kraker dan Preker dalam melakukan aksinya terutama yang berhubungan dengan *program-program* komputer dan *data-data komputer* belum memadai karena belum ada komputer forensik.

4) Belum ada Undang-Undang yang bersifat *lex-spesialis* yang mengatur bidang Internet, dot commerce serta hal lainnya yang berhubungan dengan penggunaan komputer.

Berdasarkan uraian tersebut diatas dapat diketahui secara umum, *faktor-faktor determinan* tersebut adalah : tingkat pendidikan para penyidik dibidang komputer, status mereka sebagai pelanggan Internet, pengalaman mereka dalam melakukan penyidikan kasus-kasus tersebut, sistem pembuktian, sarana dan prasarana komputer forensik serta Undang-Undang yang bersifat lex-spesialis. Dari seluruh faktor-faktor tersebut yang perlu mendapatkan *perhatian serius* adalah faktor pendidikan para penyidik dan sarana komputer forensik.

MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

Bab. VII



BAB VII

AKTUALISASI PENEGAKAN HUKUM HAKING KOMPUTER

Untuk mengetahui *sejauh mana* aktualisasi penegakan hukum terhadap Haking komputer (Kraking dan Preking) atau cybercrime, perlu dianalisa kasus-kasus kejahatan komputer yang tergolong dalam cybercrime. Data-data yang ada pada kesatuan- kesatuan Polri (Mabes Polri ataupun di Polda-Polda) sangat minim, ada beberapa kasus yang pernah ditangani namun tidak berhubungan dengan jaringan komputer / Internet atau hanya kejahatan komputer biasa (bukan cybercrime).

Data-data adanya haking komputer di Indonesia *diperoleh* dari media masa dan dari jaringan internet (bukan dari instansi Polri), dari tahun 1986 sampai tahun 2000 ada *16 kasus* haking komputer (sebenarnya lebih banyak lagi). Namun *tidak satupun* yang ditangani oleh Polri walaupun pada tanggal 19 Januari 1988 Polri menjadi korban gangguan Kraker. Hanya ada satu kasus ditangani oleh Polda Jawa Tengah yang dilakukan oleh Kraker mahasiswa, namun *modus operandinya* cenderung ke penipuan dalam e'commerce, bukan modus operandi haking komputer yang sebenarnya (Haking yang paling sangat sederhana).

Sehingga bahan untuk menganalisa hanyalah dari kasus yang ditangani Polda Jawa Tengah, serta dari 16 kasus yang terjadi sejak tahun 1986 sampai dengan tahun 2000 atau selama 4 tahun. Dari hal tersebut akan dapat diketahui *bagaimana kemampuan* para penyidik menangani kasus haking komputer *paling sangat sederhana* yang terjadi di Jawa Tengah, dan selama 4 tahun ada 16 kasus yang terjadi namun *tidak satupun* yang diungkap oleh penyidik Polri. Hal ini menunjukkan bahwa para penyidik Polri *belum mempunyai kemampuan* menyidik kasus haking komputer yang sebenarnya atau modus operandinya canggih. Berikut ini adalah gambaran kemampuan penyidik Polri, melakukan penyidikan kasus haking komputer yang paling sederhana dan aktualisasi penegakan hukumnya.

22. **Penyelidikan Haking Komputer.**

a. Kronologis kasus yang ditangani penyidik.

Tersangka Adhenico dan kawan-kawan melakukan chating dengan internet di Warung Internet Yahoo dan Dimensia Jl. Drs. Cipto – Semarang, dari rekannya (Anonim) di Amerika mendapatkan *data nomor kartu kredit* yang valid dan dijamin dapat digunakan untuk melakukan transaksi. Mulai bulan Mei 2000 mereka memesan barang-barang melalui situs komersil di Internet diantaranya *Greywolf Computer*, dengan cara :

1) Membuka situs komersil (Dot Commerce) yang dituju.

2) Memesan barang-barang yang dikehendaki setelah ditulis, kemudian kolom BUY ditekan (Enter) selanjutnya salah satu nomor kartu kredit milik seseorang dengan nomor Master Card : 5313 – 5520 – 0003 – 9280 dimasukkan, kemudian pada kolom User : dimasukkan nama tersangka, alamat rumah dan nomor telepon.

3) Setelah itu barang dikirim ± 2 minggu lewat perusahaan Cargo Fedex, diambil oleh tersangka ke perusahaan tersebut.

Perbuatan tersebut dilakukan dari bulan Mei 2000 sampai dengan awal November 2000, adapun barang-barang yang dapat diambil antara lain 12 kaca mata, 4 unit komputer Palmtop III a, 2 unit VGA card, Sandal, Kaos, Jaket dan lain-lain. Setiap transaksi berkisar dari 198 US $ sampai dengan 2000 US $. Mereka telah menimbulkan kerugian ± 14.644,41 US $ sesuai dengan laporan dari Mr. Mark Bunner pemilik perusahaan retail Greywolf Computer Service yang beralamat di 80 Liberty Av .Weirton, West Virginia 26062– 2124 – USA dengan alamat Dot Commerce: http:// www. grewolfcomputer.com.

Mr. Mark Bunner pada tanggal 13 November 2000 melaporkan ke Mastercard telah ditipu oleh orang Indonesia, dari laporan ini dapat diketahui siapa pelakunya di Indonesia dan dari kota mana transaksi dilakukan. Kemudian *Mastercard International Security & Risk Management* yang berpusat di Singapura, menghubungi langsung Kabag Reserse umum Dit Serse Polda Jawa Tengah AKBP Drs. Arif Darmawan, bekerja sama dengan Mastercard Internasional berhasil mengembangkan kasus ini pada tanggal 15 November 2000 tersangka Adhenico A. Kurniawan (Nico), umur 20 tahun seorang mahasiswa UNIKA – Salatiga ditangkap oleh Reserse Polda Jawa Tengah.

Kemudian menangkap beberapa tersangka lainnya yaitu : Winardi, Akhmad Lastya, Banu Pradipto, Januar Maulana, Beny Sumarsivin (Beny Sum) dan Aldhy Suria Puspayana. Mereka adalah mahasiswa pada Universitas yang sama namun tempat tinggal (domisilinya) berlainan ada yang di Semarang, Salatiga dan Ungaran. Taktik yang digunakan adalah dengan memancing Adhenico untuk mengambil barang-barang pesanan di kantor Fedex Semarang, koordinasi antara Polisi Jawa Tengah dan Mastercard Internasional Security and Risk Management memutuskan barang-barang pesanan tetap dikirim ke Semarang dan pada saat diambil tersangka akan ditangkap, dari keterangan Adhenico inilah tersangka-tersangka lainnya dapat diketahui.

Penyidikan terhadap para tersangka tersebut dituangkan dalam laporan Polisi No : A/133 /XI/2000/Serse tanggal 15 November 2000, mereka dituduh melakukan tindak pidana sebagaimana dalam pasal 378 KUHP, 363 KUHP. Dalam beberapa hari ditahan namun karena kesulitan dalam pembuktian, tersangka ditangguhkan dan sampai sekarang kasus ini belum bisa di berkas.

b. <u>Penyelidikan dalam rangka deteksi dini</u>.

Beberapa bulan sebelumnya AKBP Drs . Arif Darmawan yang cukup

dikenal di kalangan Mastercard International Security and Risk Management, menerima informasi melalui telepon yang *bersifat peringatan* bahwa di kota Semarang dan Salatiga sering terjadi transaksi palsu yang merugikan perusahaan-perusahaan komersil mitra dari Mastercard tersebut. Informasi ini ditampung namun tidak ditindak lanjuti karena para penyidik pada bagian Reserse umum Polda Jawa Tengah, karena tidak ada yang mengerti profil para Haker dan budaya para Haker sehingga tidak mempunyai *petunjuk atau arah* untuk melakukan penyelidikan.

Akibatnya tindak pidana terus berlangsung dan menyebabkan kerugian yang cukup besar terhadap pengusaha di Amerika sehingga pihak Mastercard menghubungi kembali Reserse umum Polda Jawa Tengah dengan surat resmi, berikut data print out transaksi yang berisi informasi nama-nama pemesan barang, lokasi pemesanan serta alamat dari Internet Provider (IP address) yaitu nomor : *202.159.33.210* dan *203.230.214.174*. IP address tersebut menunjukkan dari Indonesia, seharusnya para penyidik *melacak IP address* tersebut dan melihat ke log servernya sehingga dapat diketahui *user ID* atau *warung Internet* tempat dilakukan transaksi.

Dilain pihak Mastercard masih menunggu jawaban perkembangannya, mereka memperkirakan bahwa dengan melokalisir IP address dapat diketahui tersangkanya, namun hal ini tidak dimengerti oleh para penyidik Direktorat Reserse Polda Jawa Tengah.

c. Penyelidikan untuk mendalami fenomena Haking komputer.

Pihak Mastercard menyadari para penyidik di Polda Jawa Tengah *tidak bisa melacak* berdasarkan IP address, penyidik Mastercard mengetahui dengan pasti bagaimana modus operandi para Haker tersebut. Biasanya para Haker mencantumkan

nama dan alamat palsu untuk pengiriman barang, namun dari *manifes* yang ada terlihat bahwa barang-barang tersebut diambil langsung ke kantor perusahaan jasa kurir / kargo Federal Expres (Fedex) yang ada di kota Semarang. Mereka mengarahkan para penyidik dimaksud untuk melokalisir kantor Fedex.

Situasi menguntungkan pihak penyidik karena Adhenico menggunakan *nama aslinya* dan barang diambil dengan cara *langsung* ke kantor Fedex, sehingga dapat diintip dan pada saat datang mengambil barang ditangkap. Penangkapan tersebut tidak akan terjadi apabila tersangka menggunakan nama palsu dan alamat palsu serta *tidak langsung* mengambil barang kiriman ke kantor Fedex. apabila seperti ini *cara satu-satunya* adalah melokalisir IP address dan Warnet yang digunakan.

Dari fakta tersebut dapat diketahui bahwa para penyidik dapat sampai mengarah pada para tersangka *bukan dengan cara* menyelidiki prosedur kerja Internet, melihat ke log file di server IP, tetapi berdasarkan pada *petunjuk Mastercard* untuk melokalisir kantor jasa Ekspidisi Fedex. Menunjukkan bahwa para penyidik belum mengetahui seluk beluk masalah Internet, serta belum mengenal modus-modus operandi yang biasa dilakukan para Kraker. Petunjuk-petunjuk dari penyidik Mastercard (*Mr. K.C. Cheng* dan *Mr. Melvin Chew)* dan faktor keteledoran tersangka Adhenico memakai identitas asli, *memungkinkan* para penyidik menangkapnya.

23. **Penyidikan Haking komputer.**

a. Pengelolahan dan penanganan TKP.

Dalam kasus tersebut ada tiga TKP yaitu warnet atau tempat tersangka *Login* ke jaringan Internet / Internet provider service (IPS) yang melayani Warnet tersebut, tempat barang *hasil kejahatan* diambil yaitu kantor Fedex di Semarang serta

rumah tersangka. TKP utamanya adalah warung Internet tempat tersangka login ke Internet, selanjutnya melakukan pemesanan barang pada dot commerce yang menjadi sasaran / korbannya. Adapun pengolahan dan penanganan TKP-TKP tersebut adalah sebagai berikut :

1) Pengolahan TKP di kantor Fedex.

TKP ini merupakan tempat dimana tersangka mengambil barang-barang pesanan dari Amerika (barang hasil kejahatan) juga tempat dimana tersangka ditangkap. Di TKP ini penyidik melakukan penangkapan terhadap tersangka menyita barang bukti hasil kejahatan dan hanya *sebatas* menyita menifes-manifes yang berhubungan dengan pengiriman barang-barang dimaksud. Tidak ada pengolahan TKP lebih lanjut karena memang tidak begitu diperlukan, sedangkan dari barang bukti yang ada hanya dapat *menunjukkan* bahwa tersangka Adhenico terbukti sebagai penerima barang hasil kejahatan, belum bisa membuktikan dirinya yang melakukan pemesanan atau transaksi di Internet.

2) Pengolahan TKP di rumah tersangka.

Dari rumah tersangka ini ditemukan barang-barang lainnya hasil dari kejahatan (transaksi) sebelumnya, tidak ditemukan catatan-catatan program dalam bentuk hard copy (tulisan-tulisan di buku atau di kertas). atau soft copy (data / tulisan dalam disket atau hardisk). penyidik belum mengarah pada usaha mendapatkan bukti koleksi nomor-nomor kartu kredit yang akan atau telah digunakan. Apabila mendapatkan barang bukti koleksi nomor-nomor kartu kredit, akan berguna untuk *membuktikan* bahwa Adhenico merupakan pelaku yang melakukan transaksi dengan menggunakan nomor kartu kredit milik orang lain.

Tampaknya para penyidik di rumah tersangka lebih terfokus mencari dan menyita barang-barang bukti hasil kejahatan seperti komputer Palmtop III, asesoris komputer liannya serta pakaian-pakaian. belum mengarah pada bukti-bukti untuk mengungkap tehnis-tehnis melakukan kraking dan modus operandinya.

3) Pengolahan TKP Warnet / IP service.

Ditempat inilah merupakan TKP utamanya . apabila dalam kasus pembunuhan sama dengan tempat dimana tersangka membacok / menusuk korbannya atau menembak korbannya sampai tewas. Dari pengakuan tersangka mereka melakukannya di Warnet Yahoo serta warnet Dimensia Jl. Drs Tjipto Semarang dari tempat inilah tersangka menghubungi *Greywolf computer service* dengan alamat : http:// www.greywolfcomputer.com , memesan barang dan melakukan penipuan seolah-olah dirinya pemilik kartu kredit yang syah dan menggunakan untuk membayar barang-barang yang dipesannya tersebut.

Penyidik memang mendatangi TKP ini namun *hanya menanyakan* kepada operator-oprator yang ada disana apakah pernah melihat Adhenico menggunakan Internet di tempat tersebut, seharusnya *meminta* kepada operator untuk *mencetak log file* pada server komputer di warung internet tersebut. Untuk diketahui kapan Adhenico melakukan login dan kapan menghubungi korbannya. serta mencari arsip tanda pembayaran dari Adhenico.

Tindakan lainnya adalah mengkopi image / citra yang ada pada hardisk di server internet tersebut dan menanyakan *IP service* yang digunakan oleh warung Internet tersebut. untuk selanjutnya mendatangi IP service untuk mengumpulkan bukti-bukti lainnya agar lebih lengkap. TKP inilah yang paling penting dan harus diolah lebih teliti dibandingkan TKP-TKP lainnya. namun

yang terjadi penyidik malah lebih serius menangani / memeriksa rumah tersangka.

b. Pemeriksaan saksi/ saksi ahli dan tersangka.

Pada tahap pemeriksaan para saksi dan tersangka dari kasus tersebut , apabila para penyidik sudah memahami penyidikan haking komputer maka mereka akan memeriksa (konsep ideal pemeriksaan saksi tersangka) ; saksi operator warnet, saksi ahli dari asosiasi kartu kredit , saksi ahli tehnologi informasi serta dari laboratorium forensik Polri. tersangka pemberi nomor-nomor kartu. Ternyata para penyidik bagian Reserse Ekonomi Direktorat Reserse Polda Jawa Tengah, tindakannya tidak demikian.

1) ***Pemeriksaan saksi operator warnet,*** para penyidik tidak melakukannya padahal pemeriksaan saksi ini *sangat penting* untuk membuktikan bahwa tersangka melakukan pembelian secara ilegal dari tempatnya, posisi saksi ini adalah sebagai *saksi utama yang berada di TKP* namun tidak dilakukan pemeriksaan dan tidak dibuatkan berita acaranya.

Seharusnya yang dilakukan adalah memeriksa saksi operator yang sedang piket pada waktu itu, dengan beberapa *pertanyaan pokok* antara lain : a) apakah ada tanda bukti pembayaran menyewa fasilitas Internet di perusahaannya ; b) meminta supaya file di log server di *print out* untuk mengetahui kapan tersangka *log in* (masuk ke jaringan Internet) dan kapan tersangka *log out* (keluar dari jaringanan Internet) ; c) alamat mana saja yang dituju oleh tersangka selama dia menggunakan Internet (Data ini pasti akan ada pada warnet karena berdasarkan perbedaan waktu log in dan log out warnet tersebut *menagih uang sewa* kepada tersangka). ; d) menanyakan dan

meminta kepada operator tersebut untuk meminta print out dari file *Temp* dan *File cockies*, yang akan membuktikan alamat-alamat mana yang dituju oleh tersangka.

2) ***Pemeriksaan saksi ahli kartu kredit,*** para penyidik tidak memanggil dan memeriksa saksi ahli kartu kredit dari asosiasi kartu kredit (AKKI), padahal ditemukan *40 nomor-nomor kartu kredit* digunakan para tersangka. Seharusnya mereka dipanggil dan ditanyakan : a) siapa saja pemilik sah dari kartu kredit tersebut ; b) Bank mana dan negara mana yang menerbitkan kartu tersebut ; c) meminta pertanyaan tertulis dari pemilik yang sah bahwa mereka tidak pernah melakukan transaksi (kartunya telah disalahgunakan oleh orang lain).

Salah satu nomor kartu kredit Mastercard yang digunakan tersangka Adhenico adalah ***5313 5520 0003 9280*** hasil konfirmasi (tanggal 18 April 2001) dengan Boedi Setiawan, SE dari Collection and Risk Management Consummer Finance Group Bank Niaga yang merangkap sebagai saksi ahli dari Asosiasi Kartu Kredit Indonesia (AKKI). dapat diketahui bahwa nomor ICA (Interbank Card Associate) adalah : 1528, artinya kartu kredit yang disalah gunakan tersebut dikeluarkan oleh National Australian Bank Limited di Sydney Australia.

Seharusnya para penyidik tersebut meminta data ICA diatas melalui saksi ahli AKKI kemudian hasilnya ditindak lanjuti dengan meminta keterangan dari Bank yang mengeluarkan kartu tersebut di Australia, kemudian meminta keterangan atas nama nasabah siapa kartu kredit tersebut disertai pernyataan bahwa dirinya tidak pernah ke Indonesia dan tidak pernah memesan barang dari sebuah warnet di Semarang.

3) ***Pemeriksaan saksi ahli dari teknologi informasi dan laboratorium forensik,*** tindakan para penyidik sama (tidak memanggil dan memeriksa), seharusnya mereka dipanggil dan diperiksa untuk memberikan keterangan keahliannya (opini), untuk membenarkan bahwa print out dari file di log server warnet, otentik serta citra (image) yang disalin dari server di warnet juga otentik.

Dari fakta tersebut dapat diketahui bahwa para penyidik tidak memeriksa saksi-saksi kunci yang sangat diperlukan, yang dapat membuktikan perbuatan tersangka dalam persidangan atau pengadilan. Hal ini terjadi karena para penyidik belum memahami prosedur penggunaan dan operasional internet, juga belum mengetahui bagaimana chating pada suatu chat room.

4) ***Pemeriksaan tersangka,*** para penyidik dalam tahap ini selayaknya mendapatkan bukti dan keterangan mengenai ; cara-cara pelaku melakukan perbuatannya, akibat yang ditimbulkan, informasi jaringan Haker / Preker dan motivasinya. Adapun yang dilakukan para penyidik dari Direktorat Reserse Polda Jawa Timur, adalah sebagai berikut :

a) Mengetahui cara-cara melakukan dan jaringan Haker.

Salah satu pertanyaan penyidik Aipda Gigih Tjahyono dalam Berita Acara Pemeriksaan tanggal 15 Desember 2000 terhadap tersangka Adhenico, menanyakan bagaimana cara memesan barang atau melakukan transaksi melalui Internet, tersangka menerangkan mula-mula mencari nomor-nomor kartu kredit orang luar negeri dengan cara chating , namun ia tidak tahu siapa yang diajak chating tersebut.

Setelah mendapat nomor-nomor kartu kredit kemudian ia mencari e`commerce domain di luar negeri serta meminta yang dipesan

dikirimkan melalui perusahaan kargo Fedex.

Seharusnya penyidik menanyakan lebih detil dengan pertanyaan-pertanyaan sebagai berikut : (1) Chating room apa yang digunakan ? ; (2) Kapan mulai dilakukan chating room serta kapan selesainya sehingga dapat diketahui beberapa lama melakukan chating ; (3) Data-data nomor kartu kredit yang di dapat disimpan atau direkam dimana ? (rekaman inilah yang dicari penyidik dan dijadikan barang bukti) : (4) Menanyakan user ID lawan chatingnya atau tersangka yang memberikan nomor-nomor kartu kredit.

Tersangka menjawab tidak tahu nama atau lawan chatingnya, dapat *dipastikan* ia berbohong kepada penyidik, karena paling tidak *mengetahui user ID* atau nama panggilannya di Internet, tidak mungkin seseorang memberikan nomor-nomor kartu kredit kepada orang yang tidak dikenalnya. Keterbatasan pengetahuan para penyidik dalam melakukan chating dan fasilitas chating room, menyebabkan para penyidik tidak mampu mengungkap jaringan tersangka yang menyebarkan nomor-nomor kartu kredit.

b) Mengetahui akibat dan perbuatan pelaku.

Dalam upaya untuk mengetahui akibat yang ditimbulkan oleh para pelaku para penyidik sudah cukup baik, telah mempunyai pernyataan dari pengusaha yang dirugikan (Mr. Mark Bunner pemilik Greywolf Computer Service) senilai 14.644,41 US $. Di dukung dengan barangbukti-barang bukti berupa barang-barang pesanan yang disita dari tersangka.

c) Mengetahui motivasi pelaku.

Para penyidik dalam upaya untuk mengetahui motivasi tersangka juga sudah cukup baik, dapat dibuktikan dasarnya adalah motif ekonomi serta ingin dipuji oleh rekan-rekannya. Contohnya ; Adhenico menjual barang-barang hasil transaksi ilegal tersebut dan mendapatkan uang sebanyak Rp.15.000.000,- , selain itu supaya dipuji teman-temannya maka ia membagikan barang–barang berupa jaket, sepatu dan kaca mata. Mereka bukan penjahat profesional tapi lebih cenderung karena iseng dalam memanfaatkan Internet, tanpa berpikir lebih jauh bahwa perbuatan sangat merugikan orang lain.

Dapat diketahui bahwa para penyidik dalam mengungkap motivasi pelaku, akibat-akibat dari perbuatan pelaku sudah dapat melakukannya dengan baik. Namun belum bisa untuk mengungkap bagaimana cara-cara pelaku mendapatkan informasi kartu kredit yang akan digunakan, cara-cara melakukan transaksi serta belum mampu mengungkap jaringannya. Kelemahan ini disebabkan karena belum menguasai penggunaan Internet, khususnya media chating room.

c. Penanganan bukti- bukti dan komputer forensik.

Seperti hal dalam memeriksa para saksi dan tersangka, dalam penanganan dan pengolahan bukti-bukti, dengan dukungan komputer forensik. Harus mampu membuktikan telah terjadi suatu perbuatan dan membuktikan akibat perbuatan tersebut, adapun penanganan / pengolahan barang bukti tersebut adalah sebagai berikut :

1) ***Bukti terjadinya suatu perbuatan,*** harus di dapat yaitu untuk membuktikan barang bukti utama telah terjadi suatu perbuatan antara lain :

a) image (citra) dari server di warnet ; b) print out file dari log server warnet ; c) catatan nomor-nomor kartu kredit yang di dapat tersangka (pada kertas atau disket). Barang bukti tersebut harusnya didapat oleh penyidik untuk dilakukan pemeriksaan di laboratorium forensik guna membuktikan otentifikasinya, namun tidak bisa didapat.

2) ***Bukti terjadinya suatu akibat dari perbuatan,*** akibat dari perbuatan para tersangka korban telah dirugikan karena mengirimkan barang-barang kepada tersangka tetapi tidak ada pembayaran untuk hal tersebut. bukti barang hasil kejahatan *dapat disita* oleh penyidik antara lain sebagai berikut : a) kaca mata kurang lebih sebanyak dua belas buah ; b) dua baju kaos ; c) empat unit komputer dan dua unit Asesori komputer berupa VGA CARD ; d) sepasang sandal ; e) dua buah tas ; f) satu jacket Sky.

Dari tindakan-tindakan penyidik tersebut dapat diketahui bahwa mereka lebih mengutamakan penanganan barang bukti untuk membuktikan terjadinya suatu akibat dari perbuatan. seharusnya *lebih terfokus* pada barang bukti untuk membuktikan terjadinya suatu perbuatan. Karena tindak pidana yang terjadi dalam lingkup cyberspace, yang justru *bukti bagaimana berbuat* harus lebih dulu dibuktikan.

Dari fakta tersebut dapat diketahui bahwa *kemampuan para penyidik* dalam menangani kasus tersebut, dari segi pengolahan dan penanganan TKP, pemeriksaan saksi-saksi ahli dan tersangka masih belum seperti yang diharapkan. Dalam mengolah dan menangani TKP justru warnet sebagai TKP pertama tidak ditangani dengan baik sehingga, print out log file di server tidak bisa didapat demikian juga citra (image) pada harddisk servernya. Dalam pemeriksaan

saksi belum terfokus pada pemeriksaan saksi operator warnet dan saksi-saksi ahli, masih terfokus pada pemeriksaan saksi mahkota. Dalam pemeriksaan tersangka belum mampu mengarahkan pada cara tersangka berbuat dan jaringan para pelaku, baru mampu mengungkap motivasi para pelaku dan akibat dari perbuatan pelaku tersebut.

24. Penerapan pasal-pasal dan pemberkasan.

Tahap akhir yang dilakukan penyidik adalah menentukan pasal yang tepat pada resume berkas perkara pemeriksaan (untuk selanjutnya diserahkan ke Jaksa Penuntut Umum), penerapan pasal sangat vital apabila salah dapat mengakibatkan tersangka bebas dalam sidang pengadilan. Penerapan pasal-pasal ini ditentukan oleh hasil penyidikan para penyidik dalam menggali *unsur obyektif* dan *unsur subyektif* dari suatu tindak pidana dan bukti-bukti yang di dapat serta pengetahuan para penyidik terhadap hukum positif.

Berikut ini adalah penerapan pasal-pasal dan pemberkasan, yang dilakukan oleh penyidik Direktorat Reserse Polda Jawa Tengah terhadap kasus tersangka Adhenico :

a. Penerapan pasal-pasal.

Dalam kasus tersebut diterapkan pasal *363 KUHP* (pencurian dengan pemberatan) dan *378 KUHP* (penipuan), secara lengkap pasal tersebut adalah sebagai berikut :

"Pasal 363 : Dengan hukuman penjara selama-lamanya tujuh tahun, dihukum :
1e. Pencurian hewan.
2e. pencurian pada waktu kebakaran, letusan, banjir, gempa bumi atau gempa laut, letusan gunung api, kapal karam, kapal terdampar, kecelakaan kereta api, huru hara, pemberontakan atau kesengsaraan dimasa perang.
3e. pencurian pada waktu malam dalam sebuah rumah atau pekarangan yang tertutup yang ada rumahnya, dilakukan oleh orang yang ada disitu tiada dengan setahunya atau bertentangan dengan kemauannya orang yang berhak (yang punya).
4e. pencurian dilakukan oleh dua orang bersama-sama atau lebih.

5e. pencurian yang dilakukan oleh tersalah dengan masuk ke tempat kejahatan itu atau dapat mencapai barang untuk diambilnya, dengan jalan membongkar, memecah atau memanjat atau dengan jalan memakai kunci palsu, perintah palsu atau pakaian jabatan palsu."[68]

Penerapan pasal 363 ini tidak tepat karena tersangka melakukan perbuatan *transaksi* bukan pencurian , juga di warung internet tidak bisa dikatakan mencuri dalam sebuah rumah karena tidak ada barang yang diambil di warnet tersebut. Demikian juga tersangka tidak mengambil barang secara langsung ke Greywolf Computer Service di Negara Amerika Serikat, barang-barang ada pada tersangka dengan sukarela dikirimkan oleh pemiliknya, sehingga unsur mengambilpun tidak dapat dikenakan. Dijelaskan oleh R. Susilo sebagai berikut ; "Mengambil" = mengambil untuk dikuasainya, maksudnya waktu pencuri mengambil barang itu, barang tersebut belum ada dalam kekuasaannya, apabila waktu memiliki itu itu barangnya sudah ada ditangannya, maka perbuatan ini bukan pencurian, tetapi penggelapan (pasal 372)."[69]

Namun penerapan pasal 372 KUHP juga kurang tepat, karena barang *sebelumnya* belum ada dalam kekuasaannya, yang lebih tepat adalah pasal 378 KUHP sebagai berikut :

> "Barang siapa dengan maksud hendak menguntungkan diri sendiri atau orang lain dengan melawan hak, baik dengan memakai nama palsu atau keadaan palsu, baik dengan akal dan tipu muslihat, maupun dengan karangan perkataan-perkataan bohong, membujuk orang supaya memberikan sesuatu barang membuat utang atau menghapuskan piutang, dihukum karena penipuan , dengan hukuman penjara selama –lamanya empat tahun."[70]

perbuatan tersangka memenuhi unsur memakai *keadaan palsu*, dengan *akal atau tipu*

---

68. Soesilo R. ***Kitab Undang-Undang Hukum Pidana (KUHP).*** Politeia, Bogor, 1990. Hal. 250.

69. Ibid. Hal. 258.

70. Ibid. Hal. 260.

muslihat, *membujuk* seseorang supaya memberikan suatu barang, dalam hal ini tersangka seolah-olah sebagai pemilik kartu kredit yang sah membuat pemilik barang percaya sehingga mengirimkan barangnya.

Kemampuan penyidik dalam menerapkan pasal belum seperti yang diharapkan, belum mampu menguraikan unsur -unsur perbuatan para tersangka untuk diterapkan pada delik-delik pasal suatu Undang-undang. Apabila para penyidik telah mampu menguraikan unsur-unsur para tersangka maka akan terlihat perbuatan sebagai berikut : 1) menyalah gunakan komputer ; 2) mengambil data tanpa seijin pemiliknya ; 3) menggunakan data untuk kepentingan dirinya sendiri ; 4) melakukan tindakan seolah-olah dirinya pemilik kartu kredit yang sah ; 5) membujuk atau mengelabui sehingga pemilik barang mengirimkan barang-barang kepada tersangka (tersangka Memiliki barang milik orang lain dengan melawan hukum).

Unsur-unsur pada huruf "4) " dan "5)" dapat dipenuhi oleh pasal 378 KUHP bukan pasal 363 KUHP, unsur-unsur lainnya belum merupakan tindak pidana karena belum ada Undang-undang lex spesialis yang mengatur hal tersebut. Konsepsi hukum pidana untuk menjerat hal tersebut adalah sebagai berikut :

1) Menyalah gunakan komputer, akan menjadi delik pidana apabila ada Undang-undang penyalahgunaan komputer (Computer Misuse Act) .

2) Mengambil data tanpa seijin pemiliknya dan menggunakan untuk kepentingan dirinya sendiri akan menjadi delik pidana apabila ada Undang-undang perlindungan data (Data Protection Act) seperti yang ada di Inggris.

Dapat diketahui bahwa para penyidik belum mampu menguraikan unsur-unsur perbuatan yang dilakukan oleh para tersangka, sehingga salah dalam menerapkan pasal dan masih terpaku pada pasal-pasal dalam KUHP. Kemampuan

yang diharapkan adalah mampu menguraikan unsur-unsur perbuatan yang dilakukan oleh tersangka, kemudian menerapkannya dalam pasal-pasal yang ada di KUHP secara tepat , serta pasal-pasal dalam Undang-undang yang bersifat lex spesialis untuk cybercrime apabila nanti sudah ada dan diberlakukan sebagai hukum positif di Indonesia.

b. Pemberkasan berkas perkara.

Pemberkasan berkas perkara merupakan langkah terakhir dari suatu penyidikan, kasus tersebut ternyata belum dilakukan pemberkasan berkas perkara dan para tersangka ditangguhkan penahanannya, salah satu pertimbangan untuk menangguhkan karena perkara sulit untuk sampai pada tahap pemberkasan apalagi diserahkan ke Jaksa Penuntut Umum. Apabila diserahkan ke Jaksa Penuntut Umum dapat dipastikan akan dikembalikan ke penyidik. Dijelaskan oleh Kepala Bagian Reserse Umum AKBP Drs. Arif Darmawan Kabag Serse Umum Dit Serse Polda Jawa Tengah sebagai berikut :

> "Sudah dilakukan koordinasi dengan Jaksa namun mereka tetap meminta saksi / korban yang ada di luar negeri harus diambil kesaksiannya dan dituangkan dalam berita acara, juga pemilik sah kartu kredit yang di salah gunakan. Pernyataan tertulis dari korban belum cukup, sedangkan pernyataan dari pemilik kartu bahwa dirinya tidak pernah menggunakan kartu untuk berbelanja di warung Internet Semarang juga belum ada. Nampaknya Jaksa Penuntut Umum belum mengerti ada modus-modus tindak pidana yang baru dan tidak mungkin dilakukan dengan prosedur hukum seperti biasanya, memang kelemahannya tidak ada hukum yang mengatur khusus serta para penyidik yang belum mengerti fenomena haking komputer demikian juga dengan para Jaksa."[71]

Dapat diketahui bahwa kendala utama penyidikan adalah kemampuan dan pengetahuan para penyidik bahkan Jaksa Penuntut Umum terhadap haking komputer serta hukum positif yang belum memadai, sehingga aktualisasi penegakan hukumnya

---

71. Wawancara dengan Kepala bagian *Serse Umum Dit Serse Polda Jawa Tengah*, 20 Januari 2001.

belum seperti yang diharapkan. Harapannya kasus tersebut dapat ditangani oleh para penyidik dengan baik mulai dari tahap penyelidikan, penyidikan sampai dengan pemberkasan dan penyerahan berita acara ke Jaksa penuntut Umum bahkan sampai dengan adanya vonis, namun kenyataannya pemberkasan perkaranya belum dapat dilakukan. Dalam wawancara dengan Kasubdit Fiskal Moneter dan Devisa (Fismondev) Direktorat Tipiter Korps Reserse Mabes Polri yaitu AKBP Drs. Desman Sinaga menyatakan hal yang senada , yaitu : " Baru-baru ini ada surat keluhan dari Kedutaan besar Inggris karena banyak kartu kredit warga Inggris yang ada di Indonesia di salah gunakan dengan modus memesan barang melalui Internet, selain itu kasus-kasus haking komputer belum ada dan disidik sampai sekarang."[72]

Hipotesa awal (Ho1) bahwa : kemampuan / pemahaman penyidik Polri terhadap haking komputer belum seperti yang diharapkan, *sehingga* aktualisasi penegakan hukumnya belum optimal *ternyata terbukti.* Hal tersebut tercermin dalam fakta-fakta yang telah diuraikan diatas, selain itu dikuatkan oleh pakar tehnologi informasi yang menyatakan : "sumber daya manusia pihak Kepolisian dan aparat keamanan Indonesia amat sangat lemah dan *menyedihkan* di bidang tehnologi informasi dan Internet Apa boleh buat, cybersquad, cyber patrol swasta barang kali perlu dibudayakan untuk survival dotcommers Indonesia di Internet." [73]

Masyarakat sudah menghendaki aparat penegak hukum mampu menangani cybercrime, namun kemampuan para penyidik Polri sangat jauh dari harapan. Penyebabnya karena mereka belum dididik untuk mengetahui program komputer yang biasa digunakan para Haker, pengalaman kurang, dan sistem pembuktian yang belum didukung oleh fasilitas komputer Undang-undang serta bersifat lex spesialis.

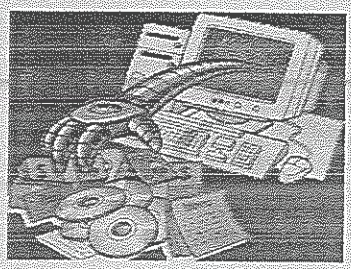
---

72. Wawancara dengan Kepala Sub bagian *Direktorat Fiskal Moneter dan Devisa Direktorat Tipiter Reserse Mabes Polri*, 6 April 2001.

73. Purbo W. Onno. *Belajar menjadi Hacker*, Kompas, 6 Maret 2001. Hal. 38.

MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

Bab. VIII



BAB VIII

PENUTUP

25. **Kesimpulan.**

a. Perkembangan haking komputer di Indonesia selaras dengan perkembangan haking komputer di luar negeri demikian juga dengan akibat-akibat yang ditimbulkannya. Fenomena ini perlu mendapatkan *perhatian yang serius* karena tidak sebuah komputerpun yang tersambung dengan jaringan komputer benar-benar aman dari serangan para Haker, selain itu haking, kraking dan preking akan terus ada dan berkembang. Seorang Haker sejati akan selalu melakukannya setiap saat ada kesempatan,

Umumnya modus operandi para Haker (Kraker) , adalah menyerang Website, kemudian disusul dengan perusakan-perusakan sarana / instalasi-instalasi yang dikendalikan melalui jaringan komputer, modus para Haker (Kraker) tersebut dikategorikan sebagai berikut :

1) Menyerang mengganggu situs-situs (Website) dengan tujuan : a) Menghalangi akses masuk ke situs ; b) Merubah tampilan situs dan fungsinya ; c) Merusak situs dan membuat tidak berfungsi.

2) Menyerang pada suatu komputer Network (Internet, Intranet, WAN serta LAN), untuk melakukan hal-hal sebagai berikut : a) Mencuri informasi untuk kepentingan industri (Spionase bisnis) ; b) Merubah program / piranti lunak agar tidak berfungsi secara normal.

3) Melakukan transaksi palsu pada perusahaan-perusahaan *Dotcom* (.Commerce) , atau website komersil lainnya.

Akibat dari hal tersebut telah banyak perusahaan e'commerce di Indonesia dirugikan dan telah banyak gangguan yang disebabkan oleh para Haker, yang sangat merugikan domain-domain Internet yang ada di Indonesia bahkan Polri sendiri menjadi korbannya.

Para Haker mempunyai budaya dan aturan tertentu, strata sosialnya tidak mengenal adanya pemimpin, mereka hanya mengenal idola dan pahlawannya, serta para penutur hikayat (historian) dan sebagai anggota kelompok namun status mereka sama atau sejajar. Apabila ingin diterima oleh mereka, diakui dan dijadikan kelompoknya perlu mengadaptasi karakter tertentu dan hobi mereka.

b. Secara umum *konsepsi ideal* kemampuan penyidikan dan konsepsi komputer forensik serta perangkat hukumnya adalah : bagaimana mewujudkan profil para penyidik yang berpengalaman lebih dari 3 tahun sebagai penyidik lanjutan, berpendidikan programer komputer mampu menggunakan program LINUX, UNIX biasa digunakan oleh Haker, sehingga mengetahui budaya para Haker, tehnis melakukan haking / modus operandinya. Didukung oleh laboratorium forensik khusus kejahatan komputer, juga didukung saksi-saksi ahli di bidang komputer. Kemudian penyidiknya mampu menerapkan cyberlaw yang bersifat lex spesialis, tidak terbatas pada pasal-pasal dalam KUHP saja.

Vogon adalah suatu perusahaan swasta yang berdiri di Inggris sejak tahun 1985 mempunyai cabang di Amerika dan Jerman, khusus memberikan jasa pelayanan untuk mendapatkan, memproses bukti-bukti yang berhubungan dengan kejahatan komputer secara ilmiah, serta membantu penyidikan juga menjadi saksi ahli terhadap Kepolisian Inggris, Jerman dan Amerika dalam proses peradilan di negara-negara tersebut. Cara kerja dan program - program Vogon ini patut dijadikan *konsepsi* untuk kegiatan

komputer forensik yang akan dilakukan oleh Polri, secara umum ada tiga bagian besar operasional komputer forensik yaitu *Evidence collection* (pengumpulan dan penanganan bukti), *Forensic analysis* (analisa forensik) dan *Expert Witness* (kesaksian ahli).

Konsepsi cyberlaw diperlukan untuk menangani cybercrime (Haking, Kraking dan Preking), juga *harus menjangkau* kejahatan komputer lainnya diluar cybercrime. *Konsep cyberlaw* ini antara lain : 1) Undang-undang penyalahgunaan komputer (Computer Misuse Act) ; 2) Undang-undang perlindungan data (Data Protection Act) ; 3) Undang- undang gangguan komunikasi (Interception of Communication Act) ; 4) Undang - undang perlindungan kerahasiaan komunikasi elektronik (Electronic Communication Privacy Act / ECA) ; 5) Undang-undang keabsahan data dan tanda tangan digital (Digital Signature Act) ; 6) Undang-undang perlindungan perniagaan secara elektronik (Electronic Commerce Protection Act) ; 7) Undang-undang hak cipta media digital (Digital Copyright Act) ; 8) Undang-undang telekomunikasi dan teknologi informasi (Telekomunication and Information Technology Act).

Konsep *penerapan Undang-undang* ini (cyberlaw) yang ideal, adalah mengutamakan Undang-undang yang bersifat lex spesialis, selanjutnya Undang-undang lain yang mendukung cyberlaw, kemudian terakhir KUHP diterapkan. Tidak terbalik seperti sekarang justru KUHP yang dikedepankan.

c. Pengetahuan / pemahaman para responden penyidik Polri terhadap *modus operandi para Haker* dan *program-program haking komputer* juga sangat minim, artinya hampir semua penyidik Polri yang menjadi responden tidak mengetahui motivasi para Haker dan profilnya mereka tidak bisa membedakan antara Haker, Kraker dan Preker. Hampir semuanya tidak mengetahui program-program komputer

yang biasa digunakan oleh para Haker (hanya 1 responden yang tahu). Pengetahuan para penyidik Polri hanya terbatas pada Virus komputer dan akibat yang ditimbulkannya, tidak mengetahui program Worm dan Trojan horse apalagi membedakannya.

Tidak ada seorangpun responden yang mengetahui bagaimana seorang Haker memasuki suatu jaringan komputer secara tidak sah, artinya mereka tidak tahu sama sekali modus - modus operandi para Haker, Kraker dan Preker dalam melakukan aksinya, hanya *1 responden* yang mengetahui kejahatan dan gangguan apa saja bisa ditimbulkan para Haker, Kraker dan Preker. Pengetahuan para responden mengenai penerapan pasal-pasal KUHP untuk menjerat para Kraker dan Preker sangat minim, hanya terbatas pada pasal-pasal dalam KUHP saja.

Banyak faktor yang mempengaruhi hal tersebut diatas namun diantaranya ada yang sangat berpengaruh *(faktor determinan)*, yaitu : 1) tingkat pendidikan para penyidik dibidang komputer ; 2) status mereka sebagai pelanggan Internet ; 3) pengalaman mereka dalam melakukan penyidikan kasus-kasus tersebut ; 4) sistem pembuktian ; 5) sarana dan prasarana komputer forensik ; 6) Undang-Undang yang bersifat lex-spesialis dari seluruh faktor-faktor tersebut yang perlu mendapatkan *perhatian serius* adalah faktor pendidikan para penyidik dan sarana komputer forensik.

d. Dari hasil analisa kasus kraker yang ditangani Polda Jawa Tengah dapat diketahui *bagaimana kemampuan* para penyidik menangani kasus haking komputer *paling sangat sederhana* , namun tidak mampu untuk diajukan ke Jaksa Penuntut Umum. Dari fakta-fakta bahwa selama 4 tahun ada 16 kasus Haking yang terjadi namun *tidak satupun* yang diungkap oleh penyidik Polri. Hal ini menunjukkan bahwa para penyidik Polri *belum mampu* menyidik kasus haking komputer yang sebenarnya.

Para penyidik dapat sampai mengarah pada para tersangka *bukan dengan cara* menyelidiki prosedur kerja Internet, melihat ke log file di server IP, tetapi berdasarkan pada *petunjuk Mastercard* untuk melokalisir kantor jasa Ekspidisi Fedex. Menunjukkan bahwa para penyidik belum mengetahui seluk beluk masalah Internet, serta belum mengenal modus-modus operandi yang biasa dilakukan para Kraker.

Kemampuan para penyidik dalam pengolahan dan penanganan TKP, pemeriksaan saksi-saksi ahli dan tersangka masih belum seperti yang diharapkan. Dalam mengolah dan menangani TKP justru warnet sebagai TKP pertama tidak ditangani dengan baik sehingga, print out log file di server tidak bisa didapat demikian juga citra (image) pada harddisk servernya.

Dalam pemeriksaan saksi belum terfokus pada pemeriksaan saksi operator warnet dan saksi-saksi ahli, masih terfokus pada pemeriksaan saksi mahkota. Dalam pemeriksaan tersangka belum mampu mengarahkan pada cara tersangka berbuat dan jaringan para pelaku, baru mampu mengungkap motivasi para pelaku dan akibat dari perbuatan pelaku tersebut. Cara mereka menerapkan pasal-pasal yang disangkakan juga masih belum optimal, hanya terfokus pada analogi pasal-pasal dalam KUHP.

e. *Hipotesa awal (Ho1)* bahwa : kemampuan / pemahaman penyidik Polri terhadap haking komputer belum seperti yang diharapkan, *sehingga* aktualisasi penegakan hukumnya belum optimal *ternyata terbukti*. Hal tersebut tercermin dalam fakta-fakta yang telah diuraikan diatas. Seorang pakar tehnologi informasi menyatakan bahwa, sumber daya manusia pihak Kepolisian dan aparat keamanan Indonesia amat sangat lemah di bidang tehnologi informasi dan Internet.

Masyarakat sudah menghendaki aparat penegak hukum mampu menangani

cybercrime, namun kemampuan para penyidik Polri sangat jauh dari harapan. Penyebabnya karena mereka belum dididik untuk mengetahui program komputer yang biasa digunakan para Haker, pengalaman kurang, dan sistem pembuktian yang belum didukung oleh fasilitas komputer Undang-undang serta bersifat lex spesialis. Sehingga maysrakat *mengisyaratkan perlunya* cybersquad, cyber patrol swasta diberdayakan agar dotcommers Indonesia di Internet tetap survive (bisa bertahan).

26. Saran-saran.

a. Mempersiapkan personil (Brainware), antara lain dengan cara :

1) Mendidik para penyidik Polri secara khusus dalam bidang komputer dengan fokus *materi pendidikan* untuk mengantisipasi cybercrime, serta mengirim calon-calon pendidik (Instruktur) ke perusahaan jasa pendidikan dan penyidikan Vogon di Inggris dengan alamat : ***Vogon International Limited***, Talisman Business Centre, Talisman Road, Bicester OX26 6HR, United Kingdom Telephone : – 44 (0) 1869 355255 / Fax : + 44 (0) 1869 355256.

2) Meningkatkan pengalaman para penyidik kasus-kasus cybercrime yang selama belum dilakukan penyidikan, agar *proaktif disidik* tanpa menunggu laporan dari masyarakat karena tindak pidana dalam cybercrime tersebut sebagian besar bukan delik aduan, selain itu *mensosialisasikan Internet* pada seluruh penyidik Polri dengan memanfaatkan Website Polri yang sudah ada (http://www.polri.mil.id).

b. Mempersiapkan piranti lunak (Software) dengan cara :

Mempelopori untuk mengkaji agar ada *hukum positif* yang bersifat lex spesialis untuk mengantisipasi aktivitas cyberspace sekaligus cybercrime dengan memanfaatkan

pakar-pakar hukum antara lain ; Atip Latifulhayat, SH, LLM (UNPAD), untuk bekerja sama dengan Dinas Hukum Mabes Polri yang berperan sebagai penjuru dalam pengkajian ini (Project Officer).

c. Mempersiapkan piranti keras (Hardware) dengan cara :

Melakukan *pengkajian* untuk membentuk laboratorium forensik khusus bidang Forensic Computing, berikut awaknya yang mampu untuk mengoperasionalkan peralatan khusus untuk hal tersebut antara lain : 1) DAT Imager (Pencitra DAT) ; 2) Diskette Imager (Pencitra Disket) : 3) Disk Emulator (Emulator piringan data) ; 4) Covert Imager (Pelindung hasil pencitraan) ; 5) Mobile Forensic Workstation (Labolatorium forensik lapangan) ; 6) Enterprise Imaging System.

Saran untuk pengkajian tersebut melakukan studi banding ke *Vogon International Limited*, karena perusahaan ini mempunyai laboratorium Komputer Forensik yang dianggap terbaik di dunia. Selain itu melakukan koordinasi dengan pakar-pakar IT (Information Technology) antara lain : Onno W. Purbo (ITB) dan Roy M. Suryo (GAMA), karena Polri sudah saatnya memberdayakan *Police sciencetific community* (Pakar-pakar dari berbagai disipin ilmu pengetahuan) untuk membantu penyidikan-penyidikan yang dilakukan oleh Polri.

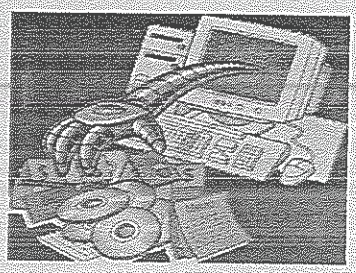
Demikian kesimpulan dan saran sebagai konklusi dari Taskap ; ***Tinjauan terhadap kemampuan penyidik Polri dalam menyidik Haking komputer serta aktualisasi penegakan hukumnya*** , semoga bermanfaat serta semoga Sespim Polri dapat melahirkan pemimpin-pemimpin Polri yang intelektual dan handal.

Lembang, 21 April 2001.

P e n u l i s

MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

Daftar Pustaka



DAFTAR – PUSTAKA

Abdussalam, R. Drs, SH, MH. ***Pencegahan Hukum di lapangan oleh Polri.*** Perpustakaan Nasional, Jakarta, 1997.

Gaffar Mohammad Fakry , H. Prof. Dr. M.Ed, dkk. ***Pedoman Penulisan Karya Ilmiah (Laporan Buku, Makalah, Skripsi, Tesis, Disertasi).*** Universitas Pendidikan Indonesia, Bandung, 2000.

Hartono Jogiyanto, MBA, Ph.D. *Pengenalan Komputer.* Andi, Yogyakarta, 1999.

Iskandar Widi. ***Pemanfaatan Jaringan Komputer Global Internet untuk Pemerolehan Karya Ilmiah.*** Majalah Sanyata sumanasa wira, Sespim Polri, Lembang, 1997.

Jogiyanto Hartono, MBA, Ph.D. ***Pengenalan Komputer.*** ANDI, Yogyakarta, 1999.

Koentjaraningrat. ***Metode-metode Penelitian Masyarakat.*** Gramedia, Jakarta, 1989.

Komar Mieke, Prof, DR, SH, MCL, CN dan Ahmad M Ramli, SH, MH. ***Sistem Informasi Sebagai Fenomena Hukum Baru di Indonesia.*** Lembaga Afiliasi Penelitian dan Industri (LAPI) – ITB , Bandung, 1998.

Kumar Ranjit. ***Writing A Research Proposal (Some Guidelines for Beginners).*** Curtin University of Technology, Perth, Western Australia, 1993.

Nusantara Abdul Hakim G, SH, LLM, dkk. ***Kitab Undang-Undang Hukum Acara Pidana dan Peraturan-Peraturan Pelaksana.*** Djambatan, Jakarta, 1986.

Poerwadarminta W.J.S. ***Kamus Umum Bahasa Indonesia.*** Balai Pustaka, Jakarta, 1999.

Purbo W. Onno dan Wihardjito Tony. ***Keamanan Jaringan Internet.*** Elex Media Komputerindo, Jakarta, 2000.

Razali Norrizan. ***Higher Education Reform Towards Industrialization : A Malaysian File*** *(Re-engineering Education : Perspectives, Priorities and Issues)* dalam Laporan kedua UNESCO-ACEID International Conference. Asia-Pasific Centre of Educational Innovation (ACEID – UNESCO), Bangkok, 1996.

Sabadan Daan Drs. dan Drs. Kunarto. ***Kejahatan Berdimensi Baru.*** *Cipta Manunggal,* Jakarta, 1999.

Soesilo R. ***Kitab Undang-Undang Hukum Pidana (KUHP).*** Politeia, Bogor, 1990.

Toffler Alvin . ***Kejutan Masa Depan.*** Pantja Simpati, Jakarta , 1992.

Wojowasito, S. Prof. Drs. dan W.J.S. Poerwadarminta. *Kamus Lengkap.* Hasta, Bandung, 1980.

CNN dotcom. ***Bracing for Guerrilla Warfare in Cyberspace,*** [Online]. Tersedia : http://cnn.com/TECH/specials/hackers/cyberterror/ . [15 Februari 2000].

Goldstein Emmanuel. ***Q & A with Emmanuel Goldstein of 2600: The Hacker's Quarterly.*** [Online]. Tersedia : http://cnn.com/TECH /specials /hackers /qandas/ goldstein.html. [15 Februari 2000].

Hadinoto Pandji R, Ir, PE, MBL, PhD. ***Supremasi Teknologi Eksponensial.*** [Online]. Tersedia : http: www.polri.mil.id/cyberlawboard_no2.htm . [29 Desember 2000].

Icove David, dkk. ***Computer Crime A Crimefighter's Handbook.*** O'Reilly Online Catalog [Online] . Tersedia : http://www.oreilly.com/catalog/crime/chapter/cri_02.html. [23 April 2000].

Latifulhayat Atip, SH, LLM. ***Cyberlaw dan Urgensinya bagi Indonesia.*** [Online]. Tersedia : http://www.polri.mil.id Cyber_pol/CYBERLAW_URGEN.HTM [29 Desember 2000].

Linux Journal. ***Metaclass Function,*** [Online]. Tersedia : http://noframes.linuxjournal.com/lj-issues/issue73/388214.html . [24 Desember 2000].

Loa Ash Revelation. ***The Ultimate Beginner's Guide to Hacking and Phreacking.*** [Online]. Tersedia: http://www.hackers.com /texts/neos/starhak.txt.[23 April 2000].

NetMag. ***Hacking : An art in itself.*** [Online]. Tersedia : http://www.netmag.com.pk/new/hacking.htm. [26 Desember 2000].

Palmer. Charles C. Dr. ***Q & A with IBM's Charles Palmer*** . [Online]. Tersedia http://www. cnn.com / TECH / specials / hackers / qandas / palmer.html . [15 Februari 2000].

Raymond Eric Steven. ***How To Become A Hacker.*** [Online]. Tersedia : http://www.tuxedo.org/~esr/faqs/hacker-howto.html. [24 Desember 2000].

_____. ***Jargon File Resources.*** [Online]. Tersedia : http://www. tuxedu.org /~esr/jargon/jargon.html. [24 Desember 2000].

Suryo R.M. ***Mendesak CyberLaw untuk Indonesia.*** [Online]. Tersedia : http://www .polri .mil.id /cyberlawboard_no2.htm [16 April 2000].

Vogon. ***About Forensic Computing*** [Online]. Tersedia : http: www.vogon-computer-evidence.com forensic_services-01.htm [16 April 2000].

_____. ***Risk and Pitfalls.*** [Online]. Tersedia : http: www.vogon-computer-evidence.com forensic_services-02.htm . [16 April 2000].

_____. ***Good Practice Guidelines*** [Online]. Tersedia : http: www.vogon-computer-evidence .com forensic_services-03.htm. [16 April 2000].

_____. ***Good Practice Guidlines.*** [Online]. Tersedia : http://www.vogon-computer-evidence.com /forensic_services-03.htm . [16 April 2000].

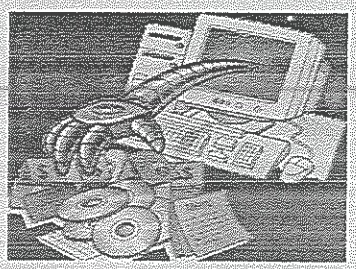
_____. ***Expert Witnesses*** [Online]. Tersedia : http://www.vogon-computer-evidence.com /forensic_services-04.htm . [16 April 2000].

Supriyatna Akhmad. ***Menyelusuri Jejak Para Penyusup.*** Majalah Panji No. 29 Tahun IV, Jakarta, 8 November 2000.

Purbo W. Onno. ***Belajar menjadi Hacker.*** Kompas, Jakarta, 6 Maret 2001.

MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

Lampiran



MARKAS BESAR
KEPOLISIAN NEGARA REPUBLIK INDONESIA
SEKOLAH STAF DAN PIMPINAN

PANDUAN WAWANCARA UNTUK RESPONDEN

(Penyidik Polri dibidang Reserse Ekonomi)

I. **Identitas , data dan status responden.**

1. Tanyakan lama bertugas di Reserse (sebagai penyidik), diharapkan lebih dari 3 tahun sebagai penyidik dibidang Reserse ekonomi atau bidang lainnya.

2. Tanyakan apakah pernah mengikuti Dikjur Reserse, diharapkan responden paling tidak pernah mengikuti Dikjur lanjutan Reserse.

3. Tanyakan apakah pernah *mengikuti* dan *lulus* pendidikan formal dibidang komputer, diharapkan responden tidak hanya dididik sebagai operator tetapi sebagai programer.

II. **Pengetahuan dan kemampuan mengoperasikan komputer.**

1. Tanyakan apakah bisa mengoperasikan komputer, responden diminta memperagakan dari *mulai start*, *menggunakan* salah satu aplikasi sampai dengan prosedur *shut down*.

2. Tanyakan apabila menggunakan komputer, apakah hanya untuk mengetik atau digunakan untuk *mengolah* data serta *menganalisanya*.

3. Tanyakan program aplikasi (software) apa saja yang sering ia gunakan, diharapkan responden mampu menggunakan software *text file* (Microsoft word, dll), software *pengolahan data / program* (Foxpro, Dbase dan lain-lain) , dan diharapkan mengerti serta bisa menggunakan software seperti *LINUX, UNIX* serta *Python*.

4. Tanyakan apakah sering menggunakan Internet dan mempunyai *user ID* di salah satu ISP (Internet Service Provider), diharapkan paling tidak responden telah berlangganan selama 6 bulan.

III. **Pengetahuan mengenai program jahat komputer (Virus, Worm, Trojan horse, dsb) serta fenomena haking komputer.**

(*Keterangan* : Pertanyaan dibawah ini ditujukan hanya pada responden yang *memenuhi kriteria* jawaban *bagian II nomor 3 dan 4*, apabila jawabannya negatif wawancara dihentikan).

1. Tanyakan apakah mengerti yang dimaksud dengan *program–program jahat* komputer.

2. Tanyakan apa perbedaan *Virus* dan *Worm* serta apa program jahat *Trojan horse*.

3. Tanyakan apakah mengerti fenomena *Haking komputer*, bila mengerti tanyakan apa bedanya *Haker*, *Kraker* dan *Preker*.

IV. **Pengetahuan mengenai modus operandi para Haker, dan program-program Haking komputer.**

(*Keterangan* : Pertanyaan dibawah ini ditujukan hanya pada responden yang *memenuhi kriteria* jawaban *bagian III nomor 3*, apabila jawabannya negatif wawancara dihentikan).

1. Tanyakan apakah seluruh Haker jahat, dan bagaimana *profil* mereka.

2. Tanyakan *program-program* apa yang digunakan untuk melakukan Haking komputer.

3. Tanyakan bagaimana *kronologis* seorang Haker memasuki suatu jaringan komputer.

4. Tanyakan *kejahatan-kejahatan* apa dan *gangguan* yasng biasa dilakukan para Kraker dan Preker , pada Internet, jaringan komputer lainnya dan jaringan telepon.

5. Tanyakan *pasal-pasal* apa yang bisa diterapkan, siapa yang menjadi kemungkinan *tersangka / saksi / korban*, barang bukti apa yang *harus disita*.

V. **Pengalaman melakukan penyidikan terhadap tindak pidana yang menggunakan komputer dan program komputer sebagai alat kejahatan.**

(*Keterangan :* Pertanyaan dibawah ini ditujukan hanya pada responden yang *berpengalaman* melakukan penyidikan terhadap tindak pidana yang menggunakan *komputer* dan *program komputer* sebagai alat kejahatan, apabila jawabannya negatif wawancara dihentikan).

1. Meminta agar responden *menceritakan* pengalamannya secara kronologis dan singkat.

2. Tanyakan *pasal-pasal* apa yang telah diterapkan, siapa yang menjadi *tersangka / saksi / korban*, *barang bukti* apa yang telah disita.

3. Tanyakan apakah berkas perkara *dikirim* atau *tidak* kepada Jaksa penuntut umum, apakah perkara tersebut *sudah* divonis atau belum.

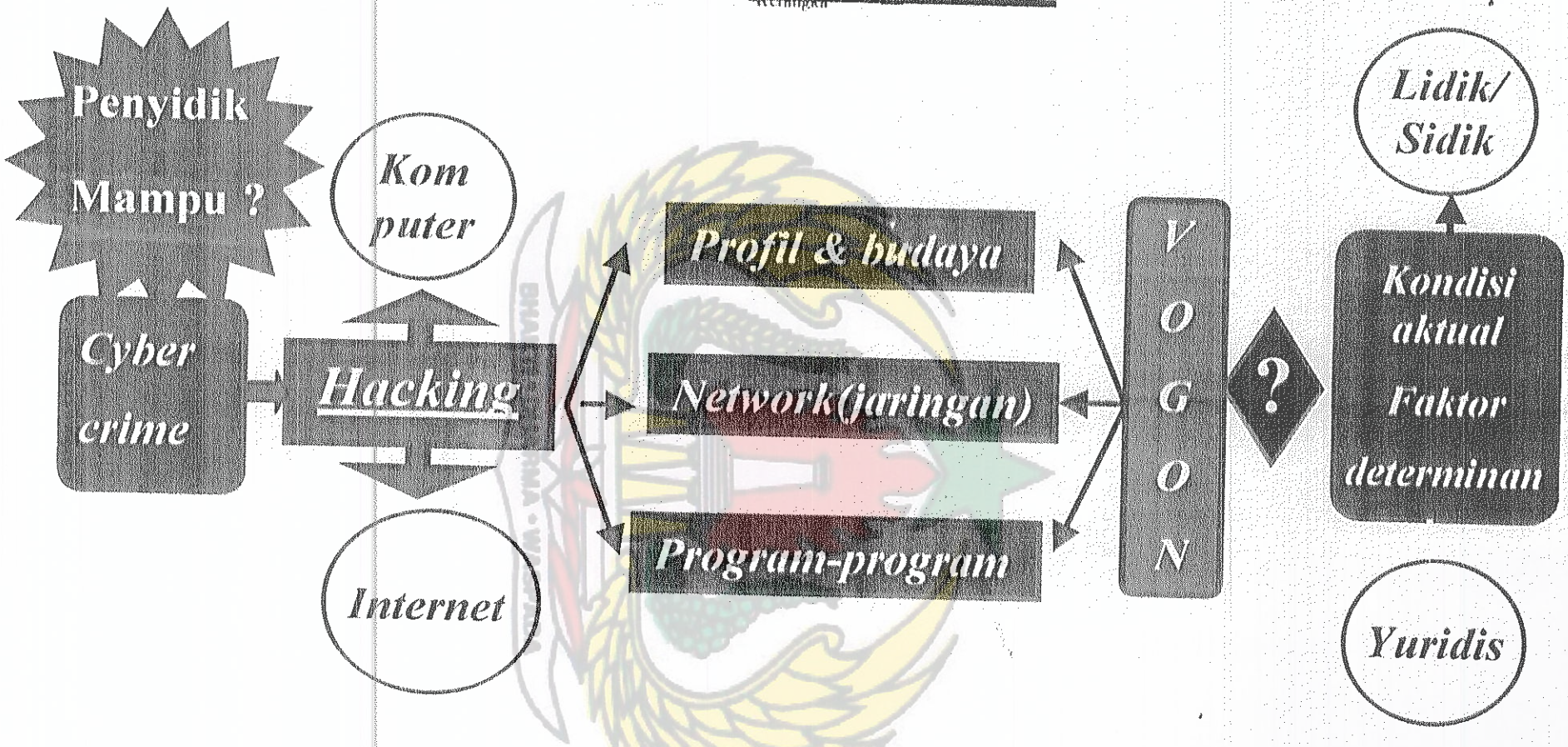
4. Tanyakan apa *kendala-kendala* dalam menyidik kasus tersebut, apakah *saksi ahli* digunakan atau tidak.

Catatan :

* Ucapan terima kasih kepada para responden setelah wawancara selesai.
* Responden yang berpengalaman atau menjawab seluruh pertanyaan dengan baik (positif), dilakukan pendalaman lebih lanjut.

----------oo0oo----------

Kerangka pikir



REKAP HASIL WAWANCARA

PERTANYAAN		RESPONDEN																																						JLH
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	
I	1	0	1	0	1	1	1	1	0	1	1	1	0	1	0	1	0	1	0	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	15
	2	1	1	0	1	1	1	1	1	1	1	1	0	1	0	1	0	1	0	1	1	1	0	1	1	0	1	1	0	0	0	0	1	0	0	0	21
	3	0	0	0	1	0	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8
II	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	30
	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	35
	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
III	1	0	0	0	1	0	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8
	2	0	0	0	1	0	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8
	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IV	1	1	0	0	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4
	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
	4	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
																																					3

Keterangan :
1 = jawaban positif.
0 = jawaban negatif.

KORPS RESERSE POLRI
DIREKTORAT PIDANA TERTENTU
Jl. Trunojoyo No. 3 Keb. Baru Jakarta Selatan

Jakarta, 6 April 2001

No. Pol. : B/ [illegible] -M/IV/2001/Ditpidter
Klasifikasi : BIASA
Lampiran : -
Perihal : Penghadapan Pasis Sespim Polri A.n. KOMPOL Drs. E. BRATA MANDALA

Kepada

Yth. KEPALA SEKOLAH STAF DAN PIMPINAN POLRI

di

Bandung

Up. Direktur Pendidikan dan Pengajaran

1. Rujukan surat Kepala Sekolah Staf dan Pimpinan Polri No. Pol : B./87/IV/2001/ Sespimpol tanggal 5 April 2001 tentang permohonan data dalam rangka pembuatan taskap dan penghadapan Pasis a.n. Komool Drs. E. BRATA MANDALA.

2. Sehubungan dengan hal tersebut di atas, bersama ini diberitahukan dengan hormat kepada KA bahwa Pasis Sespim Polri atas nama :

N a m a : Drs. E. BRATA MANDALA
Pangkat / Jabatan : Komisaris Polisi / Pasis Sespim Polri

Telah menghadap di Direktorat Pidana Tertentu Korps Reserse Polri dalam rangka pengumpulan data dan informasi guna penyusunan pembuatan Taskap yang bersangkutan.

3. Demikian untuk menjadi periksa.

A.n. DIREKTUR PIDANA TERTENTU
KASUBDIT FISMONDEV
U.b.
W A K A

Drs. DESMAN SINAGA
AJUN KOMISARIS BESAR POLISI NRP 52090083

usan :

ur Pidana Tertentu

13. Riwayat jabatan :

a. Kanit Lantas Res Tangerang.

b. Pamapta Res Tangerang.

c. Kaset Ops Puskodal Res Tangerang.

d. Kanit Reserse Res Tangerang.

e. Wakasat Sabhara Res Tangerang.

f. Mahasiswa PTIK XVII.

g. Paur Bagmin Set Deops Mabes Polri.

h. Paur Bag Ops Set Deops Mabes Polri.

i. Pjs Kasubbag Min Ops Set Deops Mabes Polri.

j. Kasat Lantas Wil Jakut Polda Metro.

k. Kasat Lantas Wil Jakpus Polda Metro.

l. Waka Polres Tangerang.

m. Waka Polres Jakarta Utara.

n. Kabag Rekayasa Dit Lantas Polri.

14. Data Penugasan Operasi :

a. KONGA XII/D UNTAG 1992 – Kamboja.

b. Creditcard Fraud Conference Tahun 1994 – Taiwan.

c. Studycase PUSAT LATIHAN POLIS Tahun 1994 – Malaysia.

15. Tanda jasa : :

a. The United Nations Medal – Police Commisioner UNTAG.

b. Santi Dharma.

c. Satya Lencana Kesetiaan Delapan Tahun.

d. Dwidyasistha.

----------oooOooo----------