

Komunikasi di dunia tidak akan berkembang demikian cepat tanpa adanya teknologi yang satu ini. Fiber optik memang tonggak sejarah baru dan juga masa depan bagi kemajuan teknologi komunikasi digital.

Hayri

Bagian 1 dari 2 Artikel



Seluk-beluk Fiber Optik

► Media komunikasi data menjadi topik yang cukup banyak dibicarakan beberapa dekade terakhir. Menjadi pembicaraan yang hangat, media komunikasi data memang selalu menyajikan yang baru, yang lebih hebat, yang lebih berguna untuk kehidupan manusia, dan mungkin juga membuat perubahan baru dalam kehidupan manusia.

Medianya komunikasi yang diperbincangkan pun tidak hanya terbatas pada media kabel tembaga saja. Mulai dari media udara dengan menggunakan frekuensi radio hingga media serat kaca, semuanya diperbincangkan karena mengalami perkembangan yang sangat luar biasa. Menggilanya penggunaan dan perkembangan ini dikarenakan meningkatnya kebutuhan komunikasi yang sangat tajam belakangan ini. Untuk melewati data berupa teks, suara, video, dan banyak lagi, semua kebutuhan tersebut akan semakin menuntut kemampuan media pembawanya lebih dan lebih lagi.

Media yang paling umum digunakan saat ini adalah media kabel tembaga. Media ini telah cukup lama digunakan karena memang media inilah yang

menjadi cikal-bakal sistem komunikasi data maupun suara. Kabel tembaga telah tertanam di mana-mana membentuk sebuah infrastruktur yang hebat di mana-mana.

Namun beberapa dekade belakangan ini, penggunaan kabel tembaga mulai mengalami penurunan. Penurunan tersebut bukan karena kebutuhan komunikasi masyarakat dunia menjadi berkurang, melainkan kebutuhannya semakin bertambah. Mengapa kalau kebutuhannya bertambah kok bisa menurun penggunaannya? Jawabannya adalah karena telah hadir media baru yang jauh lebih hebat daripada media kabel tembaga. Media tersebut adalah fiber optik.

Saat ini khususnya di negara maju, infrastruktur komunikasi yang dibangun di sana sebagian besar sudah menggunakan media fiber optik. Infrastruktur komunikasi bagi mereka sangatlah penting, maka dari itu fiber optik yang memang benar-benar andal banyak sekali digunakan di sana. Meskipun tidak semurah kabel tembaga, namun media ini jauh lebih *powerful* daripada media kuno tersebut.

Sebenarnya Apa Fiber Optik Itu?

Fiber optik secara harafiah memiliki arti serat optik atau bisa juga disebut serat kaca. Fiber optik memang berupa sebuah serat yang terbuat dari kaca, namun jangan Anda samakan dengan kaca yang biasa Anda lihat. Serat kaca ini merupakan serat yang dibuat secara khusus dengan proses yang cukup rumit yang kemudian dapat digunakan untuk melewati data yang ingin Anda kirim atau terima.

Jadi media fiber optik itu sendiri merupakan sebuah serat seukuran rambut manusia yang terbuat dari bahan kaca murni, yang kemudian dibuat bergulung-gulung panjangnya sehingga menjadi sebetuk gulungan kabel. Setelah terjadi bentuk seperti ini, maka jadilah media fiber optik yang biasa Anda gunakan sehari-hari.

Bagaimana Fiber Optik Ini Dapat Melewati Data Anda?

Mungkin Anda sudah menangkap maksud dari fiber optik secara garis besar, yaitu media komunikasi data yang terbuat dari kaca. Pertanyaan selanjutnya adalah bagaimana sepotong kaca dapat me-

miliki kemampuan melewatkan data Anda? Apakah sepotong kaca dapat melewati pulsa-pulsa listrik? Atau dalam bentuk apa data Anda dibawa melalui sepotong kaca ini?

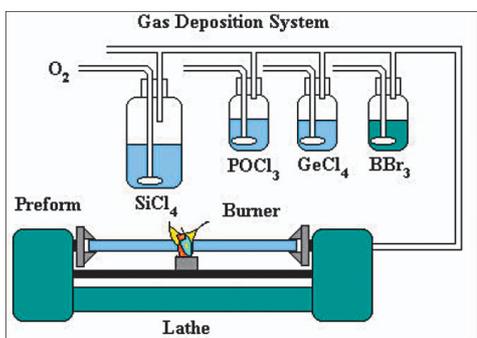
Jika berhubungan dengan alat-alat optik, maka alat-alat tersebut akan erat sekali hubungannya dengan cahaya dan sistem pencahayaan. Jika serat optik yang digunakan sebagai media, maka yang akan lalu-lalang di dalamnya tidak lain dan tidak bukan adalah cahaya.

Seberkas cahaya akan digunakan sebagai pembawa informasi yang ingin Anda kirimkan. Cahaya informasi tersebut kemudian ditembakkan ke dalam media fiber optik dari tempat asalnya. Kemudian cahaya akan merambat sepanjang media kaca tersebut hingga akhirnya cahaya tadi tiba di lokasi tujuannya. Ketika cahaya tiba di lokasi tujuan, maka pengiriman informasi dan data secara teori telah berhasil dikirimkan dengan baik. Dengan demikian, maka terjadilah proses komunikasi di mana kedua ujung media dapat mengirim dan menerima informasi yang ingin disampaikan.

Apa Saja Komponen Sistem Komunikasi Fiber Optik?

Sebuah sistem komunikasi tentu tidak hanya didukung oleh satu dua komponen atau perangkat saja. Di dalamnya pasti terdapat banyak sekali paduan komponen yang saling bekerja sama satu dengan yang lainnya. Perpaduan dan kerja sama tersebut akan menghasilkan banyak sekali manfaat bagi berlangsungnya transfer informasi. Dengan demikian, jadilah sebuah sistem komunikasi.

Sistem komunikasi biasanya terdiri



Bahan-bahan kimia pembuat serat kaca sangat berperan penting dalam menghasilkan media yang benar-benar tidak menghambat pergerakan cahaya.

dari lima komponen utama, *transmitter*, *receiver*, medianya itu sendiri, bentuk informasi yang dibawa melalui media, dan penguat sinyal. Baik di media kabel, media wireless, media optik semuanya menerapkan sistem yang sama. Misalnya di media wireless, yang menangani pekerjaan transmitter dan receiver adalah perangkat *Access Point* atau perangkat wireless client biasa. Yang menjadi medianya adalah udara bebas yang dapat membawa informasi sinyal-sinyal frekuensi radio.

Di dalamnya terdapat proses modulasi agar sinyal-sinyal informasi yang sebenarnya dapat dimungkinkan dibawa melalui udara. Dan setibanya di lokasi tujuan, proses demodulasi akan terjadi untuk membuka informasi aslinya kembali. Jika berjalan dalam jarak yang jauh maka penguat sinyal pasti dibutuhkan.

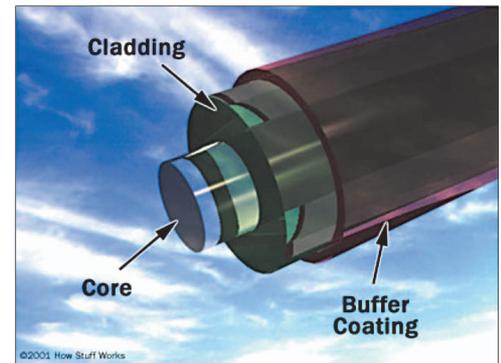
Proses komunikasi pada sistem fiber optik juga mengalami hal yang sama seperti sistem komunikasi yang lainnya. Lima komponen utama dalam sistem komunikasi fiber optik adalah sebagai berikut:

- **Cahaya pembawa informasi**

Inilah sumber asal-muasal terjadinya sistem komunikasi fiber optik. Cahaya, komponen alam yang memiliki banyak kelebihan ini dimanfaatkan dengan begitu pintarnya untuk membawa data dengan kecepatan dan *bandwidth* yang sangat tinggi. Semua kelebihan dari cahaya seakan-akan dimanfaatkan di sini. Cahaya yang berkecepatan tinggi, cahaya yang kebal terhadap gangguan-gangguan, cahaya yang mampu berjalan jauh, semuanya akan Anda rasakan dengan menggunakan media fiber optik ini.

- **Optical Transmitter**

Optical transmitter merupakan sebuah komponen yang bertugas untuk mengirimkan sinyal-sinyal cahaya ke dalam media pembawanya. Di dalam komponen ini terjadi proses mengubah sinyal-sinyal elektronik analog maupun digital menjadi sebuah bentuk sinyal-sinyal cahaya. Sinyal inilah yang kemudian bertugas sebagai sinyal korespondensi untuk



Irisan kabel fiber optik secara umum akan tampak seperti gambar di atas. Namun biasanya ada beberapa jenis kabel yang memiliki fitur khusus akan tampak berbeda dari ini.

data Anda. Optical transmitter secara fisik sangat dekat dengan media fiber optic pada penggunaannya. Dan bahkan optical transmitter dilengkapi dengan sebuah lensa yang akan memfokuskan cahaya ke dalam media fiber optik tersebut.

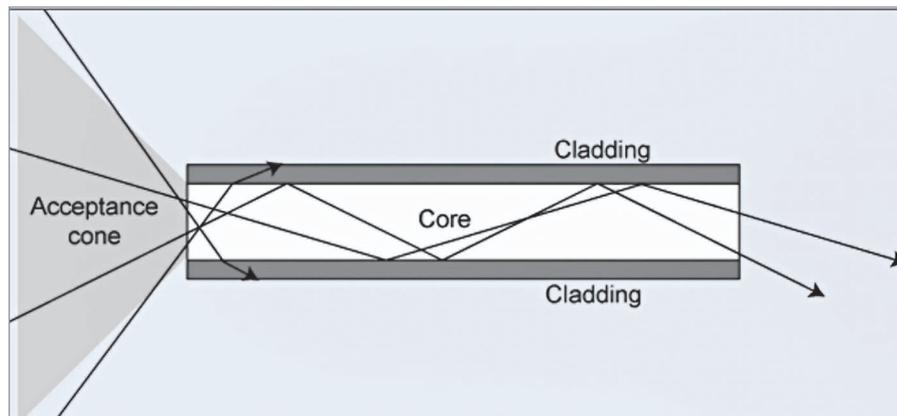
Sumber cahaya dari komponen ini bisa bermacam-macam. Sumber cahaya yang biasanya digunakan adalah *Light Emitting Diode* (LED) atau *solid state laser diode*. Sumber cahaya yang menggunakan LED lebih sedikit mengonsumsi daya daripada laser. Namun sebagai konsekuensinya, sinar yang dipancarkan oleh LED tidak dapat menempuh jarak sejauh laser.

- **Fiber optic cable**

Komponen inilah yang merupakan pemeran utama dalam sistem ini. Kabel fiber optik biasanya terdiri dari satu atau lebih serat fiber yang akan bertugas untuk memandu cahaya-cahaya tadi dari lokasi asalnya hingga sampai ke tujuan. Kabel fiber optic secara konstruksi hampir menyerupai kabel listrik, hanya saja ada sedikit tambahan proteksi untuk melindungi transmisi cahaya. Biasanya kabel fiber optic juga bisa disambung, namun dengan proses yang sangat rumit. Proses penyambungan kabel ini sering disebut dengan istilah *splicing*.

- **Optical receiver**

Optical receiver memiliki tugas untuk menangkap semua cahaya yang dikirimkan oleh optical transmitter. Setelah cahaya ditangkap dari media fiber optic, maka sinyal ini akan decode menjadi sinyal-sinyal digital



Cahaya-cahaya yang berupa informasi akan merambat melalui kabel fiber optic sejauh kekuatan cahaya tersebut ditembakkan dari asalnya.

yang tidak lain adalah informasi yang dikirimkan. Setelah di-*decode*, sinyal listrik digital tadi dikirimkan ke sistem pemrosesnya seperti misalnya ke televisi, ke perangkat komputer, ke telepon, dan banyak lagi perangkat digital lainnya. Biasanya optical receiver ini adalah berupa sensor cahaya seperti *photocell* atau *photodiode* yang sangat peka dan sensitif terhadap perubahan cahaya.

- **Optical regenerator**

Optical regenerator atau dalam bahasa Indonesianya penguat sinyal cahaya, sebenarnya merupakan komponen yang tidak perlu ada ketika Anda menggunakan media fiber optik dalam jarak dekat saja. Sinyal cahaya yang Anda kirimkan baru akan mengalami degradasi dalam jarak kurang lebih 1 km. Maka dari itu, jika Anda memang bermain dalam jarak jauh, komponen ini menjadi komponen utama juga. Biasanya optical generator disambungkan di tengah-tengah media fiber optik untuk lebih menguatkan sinyal-sinyal yang lemah.

Optical generator terdiri dari serat optik yang dilapisi dengan bahan khusus yang dapat menguatkan cahaya laser. Ketika sinyal yang lemah datang menghampiri bagian yang dilapisi khusus tersebut, energi dari laser lemah tersebut akan membuat molekul dari bahan tadi berubah menjadi sinar-sinar juga. Molekul tambahan tadi kemudian akan memancarkan sinar-sinar yang baru,

yang lebih kuat dengan karakteristik yang hampir sama dengan sinar lemah yang sebelumnya datang. Secara garis besar, regenerator ini merupakan penguat dari sinyal yang diumpankan ke dalamnya.

Apa Keuntungan Fiber Optik Dibanding Media Lain?

Media fiber optik memang telah lama ada dalam dunia komunikasi. Aplikasinya pun sudah cukup banyak meskipun belum seberkembang dan seluas kabel UTP atau kabel tembaga. Mengapa demikian? Karena media ini cukup mahal untuk dimiliki. Tidak semua orang mampu menggunakan media ini karena harganya yang tidak murah. Namun di balik semua itu, sebenarnya media fiber optik memiliki segudang kelebihan dibanding media lain. Kelebihan tersebut bahkan bisa membuat tonggak sejarah baru dalam kehidupan manusia. Media ini tidaklah menjadi mahal jika Anda bisa memanfaatkan semua kelebihannya. Berikut ini adalah kelebihan-kelebihan media fiber optik dibandingkan dengan media lain:

- **Lebih ekonomis untuk komunikasi jarak jauh**

Untuk keperluan media komunikasi dengan jarak yang sangat jauh, dengan kecepatan yang sangat tinggi dan dengan bandwidth yang cukup lebar, maka fiber optik dapat dikategorikan sebagai media yang murah dibandingkan dengan media kabel tembaga atau bahkan *wireless*.

Memang biaya kepemilikannya jauh lebih mahal pada saat kali pertama, namun semua itu akan terbayar dengan kenyamanan menggunakannya, reliabilitasnya, kecepatannya, kapasitasnya, jarak tempuhnya, dan banyak lagi kelebihan lain yang bisa Anda rasakan.

Media kabel tembaga memiliki keterbatasan jarak yang cukup signifikan dibandingkan dengan media fiber optic. Maka dari itu, jika Anda bermaksud membangun jaringan komunikasi yang berskala metropolitan dan bahkan berskala internasional, media fiber optik menjadi sebuah opsi yang sangat murah, dibandingkan dengan media tembaga.

- **Lebih kecil ukurannya**

Dari namanya saja, fiber optik atau serat optik, mungkin Anda sudah bisa menduga kalau media fiber optik ini adalah media yang sangat kecil. Hanya berupa serat yang terbuat dari bahan optik atau kaca. Ternyata memang benar dugaan Anda. Dalam wujud aslinya media yang mampu membawa informasi dengan kapasitas "tak terhingga" secara teori ini tidak jauh lebih besar dari sehelai rambut. Jika Anda pernah memancing, mungkin Anda tahu ciri dari benang pancing, yaitu bening dan tipis. Seperti itulah wujud serat optik yang hebat itu.

Banyak sekali keuntungan yang bisa didapat dari wujudnya yang kecil ini. Dengan penampang yang kecil, maka ukuran fisik dari media ini secara keseluruhan juga tidak terlalu besar. Jika dibundel, maka dalam ukuran bundel yang tidak begitu besar, Anda bisa mendapatkan cukup banyak helaian serat optik di dalamnya. Tentu keuntungan ini akan sangat berguna bagi Anda karena tidak perlu repot-repot menyediakan jalur bentangan kabel yang besar, Anda juga tidak perlu menarik berkali-kali utasan-utas kabel untuk berbagai keperluan karena didalam satu kabel saja sudah tersedia banyak sekali media pembawa data. Berbagai keperluan transmisi seperti misalnya sinyal-sinyal TV dan

telephony dapat sekaligus dibawa juga.

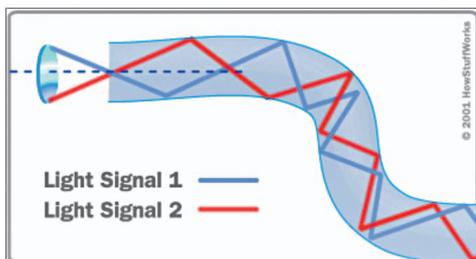
Selain itu, dengan ukuran yang kecil Anda bisa membuat pembungkusnya menjadi lebih tebal, sehingga lebih tahan terhadap gangguan dari luar. Dengan ukurannya yang kecil pula Anda tidak akan kesulitan untuk mengaturnya ketika digunakan. Semua itu mungkin tidak bisa Anda dapatkan di media manapun kecuali menggunakan media fiber optic.

- **Penurunan kualitas sinyal lebih sedikit**

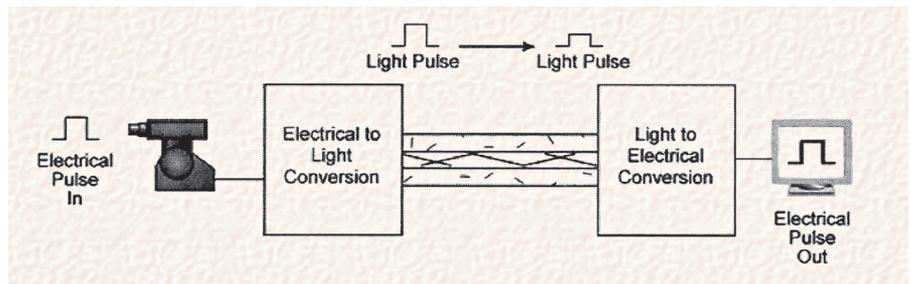
Jika menggunakan media kabel tembaga, maka Anda akan mengenal lebih banyak apa yang disebut dengan degradasi sinyal transmisi. Menurunnya kualitas sinyal-sinyal yang ditransmisikan akan mengganggu kelancaran proses komunikasi data. Hal ini akan sering ditemui jika Anda menggunakan media kabel tembaga untuk keperluan transmisi data baik jarak jauh maupun jarak dekat. Sinyal-sinyal yang dibawa melalui jalur ini tentu tidak pernah dapat dipastikan keutuhannya. Pengirim tidak akan pernah tahu apa yang terjadi di tengah perjalanannya. Yang pasti banyak sekali faktor pengganggu yang dapat menyebabkan kualitas sinyal menurun.

Apakah jalur komunikasi melewati jalur listrik tegangan tinggi, atau melalui kabel yang kurang baik instalasinya, atau melalui terminasi-terminasi yang lembap, atau melalui perangkat-perangkat penguat yang tidak baik kelistrikkannya, semua itu bisa menjadi penyebab terganggunya sinyal data Anda.

Di dalam sistem komunikasi menggunakan fiber optik, sinyal informasi yang lalu-lalang di dalamnya adalah berwujud cahaya. Mengapa cahaya?



Jumlah cahaya yang merambat di dalam media fiber optik tidak hanya terbatas satu cahaya saja.



Sinyal-sinyal listrik digital dimanipulasi menjadi sebetuk cahaya, kemudian dikirimkan ke lokasi tujuannya, inilah inti dari komunikasi fiber optik.

Karena media ini relatif lebih tebal terhadap gangguan dari luar. Tidak banyak faktor yang dapat menimbulkan interferensi terhadap sinyal cahaya tersebut. Cahaya tidak akan terganggu oleh listrik bertegangan tinggi, tidak akan terganggu oleh suhu udara baik panas maupun dingin, dan juga tidak terganggu oleh frekuensi radio di sekitarnya.

Dengan kondisi seperti ini, penurunan kualitas sinyal cahaya relatif lebih kecil dan sedikit dibandingkan dengan media komunikasi lainnya. Keuntungan yang didapat dari kelebihan ini adalah data yang dilewatkan di dalamnya lebih terjamin keutuhannya, suara yang dibawa di dalamnya untuk komunikasi telepon lebih bersih, sinyal-sinyal TV yang dilewatkan di dalamnya akan lebih jernih sampai di penerimanya.

- **Daya listrik kecil**

Untuk membawa informasi dalam bentuk sinyal cahaya, daya listrik yang dibutuhkan relatif tidak terlalu besar. Sinyal cahaya yang relatif lebih tebal terhadap gangguan dari luar tidak perlu ditransmisikan dengan daya listrik yang tinggi seperti yang terjadi pada media komunikasi kabel tembaga. Hanya butuh daya yang rendah saja, maka sinyal informasi bisa tiba di tujuan dengan selamat. Bahkan daya listrik tersebut sebenarnya tidak pernah melewati media serat optik tersebut, karena yang membawa informasi tersebut tidak membutuhkan bantuan pulsa-pulsa listrik. Dengan demikian, media ini akan menghemat banyak sekali daya listrik yang harus Anda bayar.

- **Sinyal digital**

Karena tidak ada sinyal listrik yang

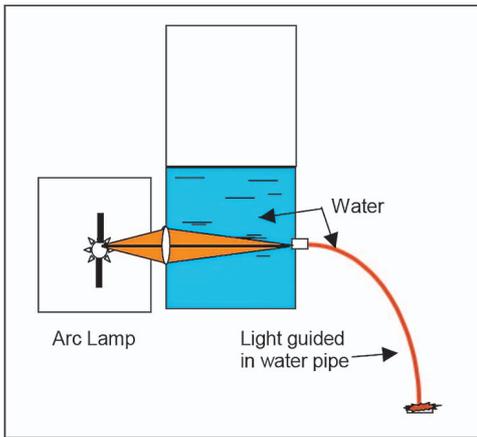
digunakan untuk membawa data, media fiber optik sangat cocok digunakan dalam sistem digital seperti misalnya komputer. Mengapa demikian? Karena komputerisasi beserta perangkat-perangkatnya banyak mengandalkan logika-logika digital. Media cahaya yang membawa informasi bukanlah sebuah sinyal analog yang harus melewati proses perubahan sinyal digital menjadi analog dan sebaliknya (ADC/DAC), melainkan adalah sinyal-sinyal digital yang terdiri dari informasi logika 0 dan 1.

Dengan demikian, informasi yang dibawanya tidak perlu melewati proses ADC/DAC lagi. Keuntungan dari fitur ini adalah data yang dikirimkan tidak akan banyak mengalami penurunan kualitas dan tidak banyak kesalahan yang terjadi akibat konversi ini.

- **Tidak mudah termakan usia**

Media fiber optik tidak digunakan untuk melewati sinyal-sinyal listrik. Bisa dipastikan didalam jalur komunikasi ini Anda tidak akan tersengat listrik sekecil apapun. Dengan demikian, media ini tidak akan mengalami kepanasan dan penipisan akibat tegangan listrik yang lewat di dalamnya. Ini menandakan media fiber optik akan jauh lebih berumur panjang dibandingkan dengan kabel tembaga biasa.

Seperti dijelaskan di atas, fiber optik terbuat dari serat kaca murni. Perlu Anda ketahui, bahan seperti kaca tidak akan mudah mengalami korosi seperti halnya tembaga. Jika bahan seperti tembaga bisa mengalami korosi jika ditempatkan pada daerah yang bersifat korosif, tidak



Asal mula sistem komunikasi yang menggunakan cahaya berawal pada tahun 1841 ketika seseorang bernama Daniel Colladon melakukan percobaan perambatan cahaya menggunakan air sebagai mediana.

demikian dengan fiber optik. Anda bebas meletakkannya di mana saja tanpa takut menjadi cepat rusak. Media fiber optik bisa ditanam di tanah jenis apapun atau digantung di daerah manapun dibutuhkan tanpa harus cemas. Dengan demikian, dapat disimpulkan media fiber optik jauh lebih lama usianya dibandingkan dengan media tembaga, jika tidak terjadi hal-hal di luar prediksi.

● Ringan dan fleksibel

Ukurannya yang sangat kecil, hampir seperti seutas rambut, membuat media komunikasi ini merupakan media fisik yang paling ringan, dibandingkan dengan kabel tembaga dan media lainnya. Dengan kelebihan seperti ini, aplikasi media fiber optik akan jauh lebih banyak dan lebih terbuka bebas dibandingkan dengan media kabel tembaga. Media ini dapat dibentang di tempat-tempat yang lebih tersembunyi, di tempat-tempat yang sulit dijangkau, dan banyak lagi.

Selain itu, media ini juga sangat fleksibel. Jika Anda pernah tahu bentuk dan karakteristik dari seutas benang pancing yang bening, seperti itulah fiber optik. Anda bebas meleku-lekukkannya, melilit-lilitkannya tanpa takut patah, asalkan tekukan tidak terlalu tajam sudutnya. Dengan bentuk yang fleksibel dan ringan seperti ini, media fiber optik akan menciptakan aplikasi-aplikasi baru

yang sebelumnya tidak pernah terpikirkan oleh manusia.

Contoh aplikasi fiber optik yang paling umum saat ini adalah fiber optik digunakan sebagai kamera digital sederhana untuk menangkap gambar dari dalam tubuh manusia. Aplikasi di bidang medis ini menjadi tonggak sejarah baru bagi dunia pengobatan dan kesehatan karena sebelumnya semua pekerjaan “melihat-lihat” tersebut sangat sulit dilakukan tanpa operasi. Aplikasi fiber optik yang lain misalnya melakukan pemantauan dalam sistem mekanis roket, pesawat terbang, kereta api supercepat, dan banyak lagi. Kerusakan yang terjadi di dalam perangkat-perangkat tersebut tidak akan mudah ditemukan jika tidak ada alat bantu seperti fiber optik. Dengan keuntungan ini, fiber optik menjadi sangat populer hingga sekarang.

● Komunikasi lebih aman

Media fiber optik merupakan media yang sangat ideal jika Anda menginginkan media yang sangat aman. Mengapa demikian? Hal ini dikarenakan informasi yang lewat di dalam media fiber optik tidak mudah untuk disadap atau dikacaukan dari luar. Sinyal informasi yang berupa cahaya tidak akan mudah untuk ditransfer ke jalur lain untuk disadap. Sinyal cahaya pun tidak akan mudah dikacaukan dengan menggunakan frekuensi pengacau atau medan elektromagnetik. Maka dari itu, media ini cukup aman untuk Anda gunakan. Meskipun cukup aman, media ini tidak sulit untuk dimonitor. Jadi sangat ideal, bukan?

Jalan Tol untuk Data Anda

Informasi dibawa dengan seberkas cahaya. Mendengarnya saja rasanya sudah cukup canggih untuk kita. Tapi sebenarnya, teknologi ini memang sangat hebat dan juga bermanfaat sekali. Data Anda tidak lagi dibawa dengan menggunakan pulsa-pulsa listrik atau frekuensi radio, tetapi dengan media yang terbilang cukup reliabel yaitu cahaya. Cahaya relatif cukup kuat

terhadap segala gangguan, baik gangguan medan elektromagnetik, gangguan cuaca, gangguan frekuensi radio, gangguan suhu, gangguan pulsa-pulsa listrik, dan banyak lagi. Selama mediana tidak terganggu secara fisik, maka cahaya akan terus berjalan sampai ke tujuannya. Kecepatannya pun tidak perlu diragukan lagi karena secara teori, kecepatan media ini adalah TANPA BATAS.

Namun, yang masih menjadi kendala dalam penggunaan media fiber optik adalah tidak lain masalah biaya. Berapa *budget* yang harus Anda sediakan untuk membeli, instalasi, menggunakan, dan merawat media ini bukanlah persoalan sepele. Karena media ini cukup mahal baik kepemilikannya maupun perawatannya. Maka itu, media jenis ini hanya dipakai untuk tujuan dan kalangan tertentu saja yang memang benar-benar membutuhkan media komunikasi berskala besar.

Meskipun demikian, jangan dulu pesimis. Seiring dengan berkembangnya kebutuhan media komunikasi, media jenis ini juga akan menyesuaikan diri nantinya. Tunggu saja tanggal mainnya di mana Anda bisa menikmati media fiber optik seperti halnya kabel UTP saat ini. Selamat menunggu!

Pada edisi berikutnya akan dibahas lebih detail lagi mengenai bagaimana cahaya merambat dalam serat optik, bagaimana sebuah serat optik dibungkus dan dibuat agar dapat melewatkan cahaya dengan baik, apa saja konektor-konektor yang ada, dan banyak lagi. Selamat belajar! ■

LEBIH LANJUT

- <http://electronics.howstuffworks.com/fiber-optic.htm>
- <http://inventors.about.com/library/inventors/blfiberoptics.htm>
- <http://www.play-hookey.com/optics/fiber1.html>
- <http://www.fiberopticonline.com/content/homepage/>
- <http://www.us.schott.com/fiberoptics/english/products/healthcare/imagingfiberoptics/index.html>

Dengan sedikit usaha, Anda bisa membuat KDE semakin mirip dengan Windows, Mac OS, atau bahkan *operating system* zanier. Kita lihat bagaimana!

Gunung Sarjono



Mengubah KDE

► KDE dan Gnome mempunyai tampilan dan cara penggunaan sendiri, yang tidak hanya membuat mereka berbeda dengan lingkungan grafis yang lain, tetapi juga berbeda di antara keduanya. Bagaimana jika Anda ingin KDE semakin mirip dengan Explorer?

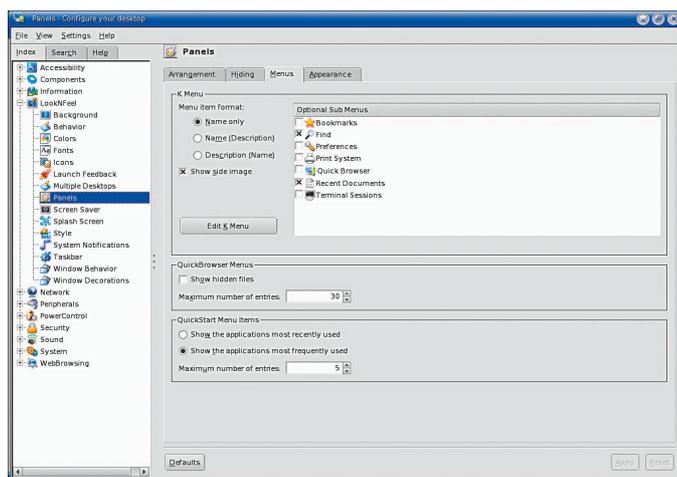
KDE merupakan surga bagi para tweaker, sehingga banyak opsi untuk semuanya. Sebagai perbandingan, Gnome berfokus pada penggunaan dan lebih sedikit opsi yang tersedia

sehingga lebih statis. Kali ini, kita akan melihat seberapa dekat kita bisa membuat KDE mirip dengan lingkungan desktop yang lain dengan mengubah opsinya, dan berapa banyak opsi yang tersedia.

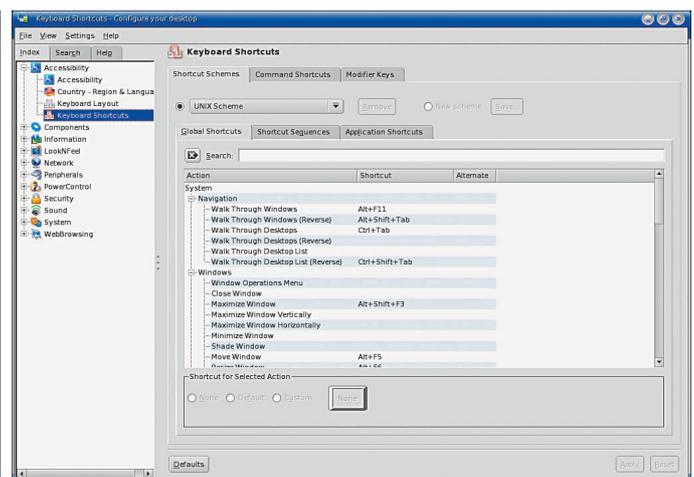
Ada dua cara untuk membuat KDE semakin mirip dengan Windows: instalasi *skin* khusus yang mirip dengan Windows, atau mengubah opsi secara manual. Dari keduanya, yang pertama adalah yang paling mudah, tetapi sering

kali berakhir menjadi yang paling susah. Menggunakan *skin* Windows memang bisa membuat sistem Anda mirip dengan Windows: tombol Start, icon My Computer, dan sebagainya. Namun, *skin* all-in-one tersebut kadang tidak bekerja dengan baik dan akhirnya menyebabkan lebih banyak masalah dibanding kegunaannya.

Jika Anda kurang sabar dan ingin KDE semakin mirip dengan Windows dengan sedikit usaha, ikuti panduan sederhana



Anda bisa mengatur format menu Kicker supaya semakin mirip dengan Windows.



Buat *shortcut* keyboard sendiri atau pilih model yang sudah ada.

berikut. Pertama, kita akan mengubah tampilan bar judul jendela. Pada Linux, ini disebut *window decoration* dan dikontrol melalui KDE Control Centre. Jika Anda menggunakan Mandrake, itu ada di K Menu, di bawah *System|Configuration|Configure Your Desktop*. KDE Control Centre berisi banyak opsi konfigurasi utama untuk tampilan dan sentuhan KDE, jadi biarkan jendela ini tetap terbuka.

Window Decorations

Untuk mengganti window decorations, buka opsi LookNFeel di sebelah kiri dan pilih Window Decorations. Theme *default* mungkin Plastik, tetapi kebanyakan distro datang dengan Redmond

sebagai alternatif. Jika Anda memilihnya dan mengklik *Apply*, Anda akan melihat tombol *minimize*, *maximize*, dan *close* tradisional Windows muncul di kanan atas jendela. Anda bahkan bisa membuat title bar semakin mirip melalui opsi *Colours* di bawah *Look and Feel* dan pilih Redmond 2000.

Pada waktu di KDE Control Centre, buka opsi Panel. Di sinilah tempat Anda mengonfigurasi bagaimana Kicker (bar di bawah) tampil dan bekerja, dan ada empat tab pada layar: *Arrangement*, *Hiding*, *Menus*, dan *Appearance*. Kita mulai dengan *Arrangement* dulu. Ukuran default Kicker biasanya adalah Normal, tetapi pengguna Windows lebih familiar dengan ukuran 'Small', jadi

pindahlah ke situ. Berikutnya, dari tab *Hiding*, hilangkan pilihan '*Show right panel-hiding button*' untuk menghilangkan tanda panah di sebelah kanan Kicker.

Dari tab *Menu*, Anda mungkin ingin mengubah jumlah *recent application* yang ditampilkan menjadi nol, kecuali jika Anda penggemar berat ini. Dari tab *Appearance*, ubah latar tombol K Menu menjadi *Default*. Selagi di situ, klik tombol *Advanced Options* yang ada di bawah dan ubah *Applet Handles* menjadi *Hide* supaya list Window dan System tray tidak mempunyai handle di sebelah mereka.

Kita sudah dulu dengan KDE Control Centre untuk saat ini, jadi Anda bisa

KDE CONTROL CENTER-LOOKNFEEL

■ KDE Control Center merupakan tempat untuk mengubah *setting* yang mempengaruhi keseluruhan lingkungan KDE. Anda bisa membukanya dengan menggunakan item Control Center pada K Menu, atau dengan perintah *kcontrol*. Setting dibagi ke dalam beberapa kategori, di mana masing-masing berisi beberapa halaman setting. Untuk menampilkan halaman setting, perluas kategori dengan mengklik tombol plus (+) di sebelahnya, dan kemudian klik nama halaman yang Anda inginkan. Halaman setting kemudian muncul di

sebelah kanan, dan Anda bisa mengubah setting sesuai keinginan. Perubahan tidak akan terasa sampai Anda mengklik tombol *Apply*. Jika setelah melakukan perubahan Anda mau mengembalikan setting seperti semula, cukup klik *Reset*. Pada LookNFeel, Anda akan menemukan setting yang mempengaruhi tampilan desktop dan aplikasi KDE.

Background

Bagian ini mengatur warna atau gambar yang digunakan sebagai latar desktop Anda. Setting ini bisa diaplikasikan ke

semua *virtual workspace*, atau hanya satu saja. Ada sejumlah *wallpaper* yang datang bersama KDE yang bisa digunakan sebagai latar atau Anda bisa memasukkan sendiri.

Colors

Ini adalah tempat di mana Anda mengubah warna untuk aplikasi KDE. Secara default terdapat banyak *scheme* warna yang terinstalasi bersama dengan KDE, dan Anda bisa mencari yang lain di kde-look.org. Anda juga bisa membuatnya sendiri. Di sini Anda juga bisa mengubah ketajaman dan memilih apakah warna KDE akan diterapkan ke aplikasi non-KDE, supaya tampilan keseluruhan lebih konsisten.

Fonts

Di sini Anda bisa mengontrol beragam setting font untuk aplikasi KDE. Anda juga bisa mengubah setting anti-aliasing, termasuk *range font* yang tidak termasuk dalam anti-aliasing.

Icons

Ini adalah tempat di mana Anda bisa mengatur icon themes dan setting lain yang berhubungan dengan icon. Icon themes baru bisa di-*download* dari kde-look.org, dan diinstalasi di sini. Di lain pihak, Anda bisa menghapus icon themes dengan menyorot mereka pada daftar dan mengklik *Remove*. Anda juga bisa



KDE Windows Makeover—salah satu yang dapat Anda gunakan untuk membuat KDE mirip dengan Windows.

menutupnya jika mau. Yang perlu dilakukan sekarang adalah memperbaiki Kicker itu sendiri—terutama jam dan *virtual desktop*. Jadi, klik kanan jam dan pilih *Configure Clock*. Ganti jenis jam menjadi *Plain Clock*, lalu hilangkan pilihan *Date display*. Anda juga mungkin ingin mengubah menjadi yang dapat lebih dibaca, seperti Sans12. Jenis jam ini merupakan yang paling mirip dengan Windows.

Pada panel itu sendiri, klik panah kecil di kiri atas virtual desktop, lalu klik Remove Pager dari menu yang muncul. Windows—salah satu kekurangannya menurut kami—tidak mempunyai virtual desktop, jadi ini perlu dihilangkan jika

menentukan ukuran icon untuk beragam penggunaan pada KDE dan efek yang digunakan ke icon.

Launch Feedback

Di sini Anda bisa menentukan jenis cursor dan/atau taskbar feedback yang Anda inginkan untuk menjalankan aplikasi. Di sini Anda juga bisa menentukan durasi feedback. Sebagai contoh, setting default untuk cursor *bouncing* adalah 30 detik, atau pada waktu aplikasi telah dimuat.

Screen Saver

Di sini Anda bisa mengonfigurasi *screen-saver*. Anda bisa mengonfigurasi *timeout* sebelum dijalankan, dan apakah memerlukan *password* untuk membuka layar.

Splash Screen

Ini adalah tempat di mana Anda bisa menginstalasi, menghilangkan dan mengetes *splash screen* yang tampil pada startup KDE. Splash screen lain bisa di-download di kde-look.org.

Style

Bagian ini memungkinkan Anda untuk mengubah *style*. KDE disertai dengan beragam *style*, dan yang lain bisa di-download dari kde-look.org. Ini juga adalah tempat di mana Anda bisa meng-enable atau disable opsi interface seperti menu transparan, menampilkan

Anda ingin semakin mirip dengan Windows!

Shortcut Keyboard

Salah satu aspek yang belum kita ubah adalah shortcut keyboard, karena KDE mempunyai sistem yang sangat powerful untuk mengontrol ini. Sama seperti tampilan, shortcut keyboard diatur melalui KDE Control Centre (lihat di kategori Accessibility). *Setting default* mungkin adalah pilihan KDE sendiri, tetapi Anda bisa mengubahnya menjadi Mac, Windows atau Unix biasa dengan menggunakan *preset* mereka sendiri.

Jika mau, Anda bisa membuat shortcut sendiri. Di sinilah KDE menunjukkan kekuatan yang sebenarnya. Tidak suka

icon pada tombol dan tooltip. Beberapa *style* mempunyai opsi konfigurasi yang lebih banyak dibanding yang lain.

System Notifications

Pada bagian ini Anda bisa mengatur bagaimana Anda akan diberitahu pada waktu terjadi *event* tertentu, bisa melalui bunyi beep atau yang lain, atau melalui kotak popup.

Taskbar

Bagian ini memungkinkan Anda untuk mengonfigurasi opsi yang berhubungan dengan taskbar. Anda bisa mengatur apakah menampilkan jendela dari semua desktop, mengelompokkan task yang sama dan tindakan apa yang akan dilakukan tombol mouse.

Window Behavior

Ini adalah tempat di mana Anda bisa mengonfigurasi opsi yang berhubungan dengan perilaku window manager KDE, yaitu KWin. Anda juga bisa menentukan tindakan apa yang ingin Anda berikan ke tombol tertentu dan mouse.

Window Decorations

Di sini Anda bisa mengonfigurasi window decorations. Anda bisa mengubah *style* dan juga menempatkan tombol pada posisi yang diinginkan. Beberapa window decorations mempunyai opsi yang lebih banyak dibanding yang lain.

[Ctrl]+[V] untuk mem-paste teks? Ubah menjadi [Ctrl]+[P], ubah menjadi [F1], atau supaya teman Anda bingung, ubah menjadi [P]. Anda juga bisa mengubah perintah generik yang lain, seperti Back, Forward, Zoom In, Reload, Save dan banyak lagi—aplikasi KDE mewarisi ini, yang artinya Anda bisa membuat satu perubahan di Accessibility dan menggunakannya pada semua program.

Untuk perubahan yang lebih ekstrim, buka opsi Keyboard Layout di sebelah kiri dan kemudian pilih tab Xkb Options. Sekarang, apakah Anda ingin tombol Windows berfungsi juga sebagai [Alt]? Apakah Anda ingin [Shift] untuk membatalkan [Caps Lock] seperti pada Windows, atau mengabaikannya seperti pada OS X? Ubah sesuka Anda.

Meskipun perubahan yang kita lakukan sama sekali tidak sama dengan Windows, paling tidak sudah mendekati sehingga orang-orang yang tidak familiar dengan Linux tidak akan begitu merasa kesulitan. Namun, jika Anda tidak berpindah dari Windows—atau jika Anda sudah bosan dengan tampilan dan kesan Windows—maka ada banyak cara untuk mengubah tampilan KDE. Sebagai contoh, di bagian *Look and Feel|Behaviour* pada KDE Control Centre, Anda bisa membuat KDE untuk menampilkan menu bar di bagian atas layar—setting yang populer dari kalangan Mac.

Anda juga harus melihat bagian Window Behaviour, yang memungkinkan Anda untuk mengonfigurasi bagaimana window bertindak pada waktu Anda mengklik mereka, apa yang terjadi pada waktu Anda mengklik ganda title bar (defaultnya adalah 'Shade', yang menyembunyikan window, hanya menampilkan title bar), dan bahkan bagaimana Anda mau window baru muncul pada layar. Default-nya adalah Smart yang menempatkan window di bagian layar yang kosong, tetapi Cascade, Random dan Centred juga populer. ■

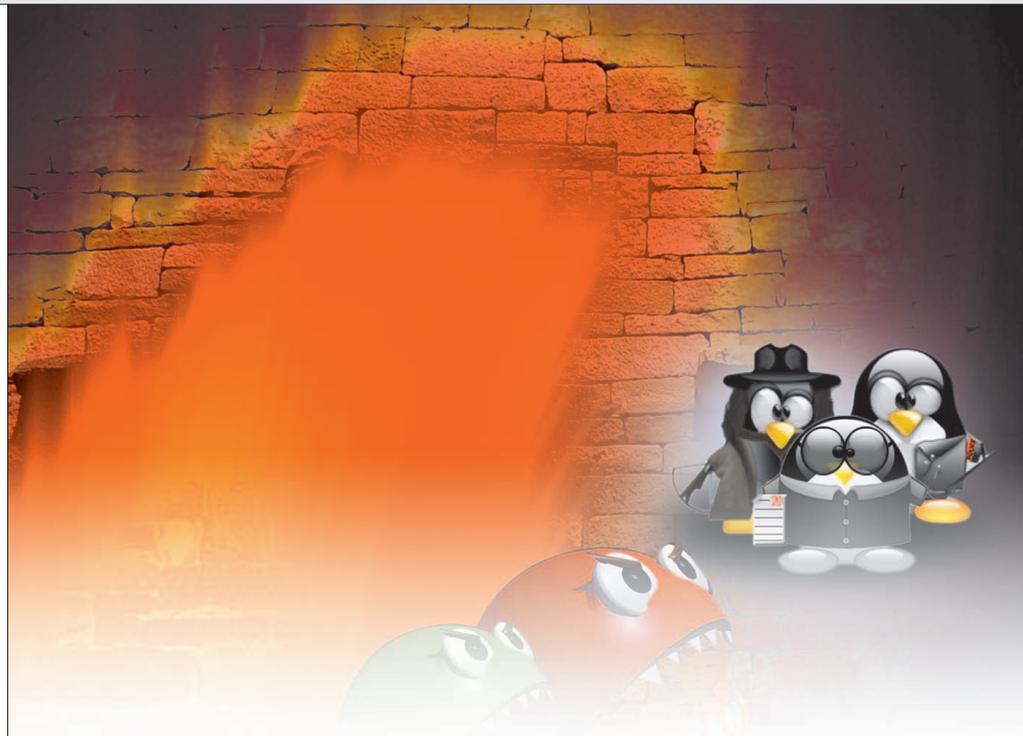
LEBIH LANJUT

- <http://kde.org>
- <http://kde-look.org>

Operating system Linux dan keluarganya yang lain memang cukup terkenal akan kekebalannya terhadap gangguan dari luar. Salah satu yang membuktikan pernyataan tersebut adalah fasilitas IPTables.

Hayri

Bagian 1 dari 2 Artikel



IPTables Firewall Canggih pada Linux

► Keamanan jaringan, PC, server-server, dan perangkat komputer Anda yang lainnya memang merupakan faktor yang cukup penting untuk diperhatikan saat ini. Jika beberapa dekade yang lalu keamanan jaringan masih ditempatkan pada urutan prioritas yang rendah, namun akhir-akhir ini perilaku tersebut harus segera diubah. Palsanya, kejahatan dengan menggunakan bantuan komputer, media komunikasi, dan perangkat elektronik lainnya meningkat sangat tajam belakangan.

Hal ini sangat kontras dengan perkembangan kebutuhan perangkat komputer untuk kehidupan sehari-hari yang juga semakin meningkat. Tidak hanya di dalam kegiatan bisnis saja, kehidupan rumah tangga pun sudah sangat relevan jika dilengkapi dengan sebuah komputer. Maka dari itulah, mengapa keamanan jaringan komputer dan PC menjadi begitu penting untuk diperhatikan saat ini.

Apalagi jika kebutuhannya sudah berhubungan dengan kegiatan bisnis, dan kegiatan bisnis tersebut banyak berhubungan dengan server yang dapat diakses dari mana saja atau dengan

koneksi Internet yang aktif 24x7. Tentu keamanan komunikasi data harus menjadi prioritas nomor satu. Mengapa demikian, karena semua fasilitas tersebut bisa juga diartikan sebagai titik celah baru menuju ke jaringan pribadi Anda.

Anda tidak bisa membiarkan begitu saja perangkat komputer Anda tanpa perlindungan dalam dunia Internet yang sebenarnya. Jika Anda biarkan, tentu segala macam jenis pengganggu akan bercokol di komputer Anda. Mulai dari virus sampai *hacker* yang menanam *backdoor* akan menggunakan komputer Anda sebagai alat bersenang-senang.

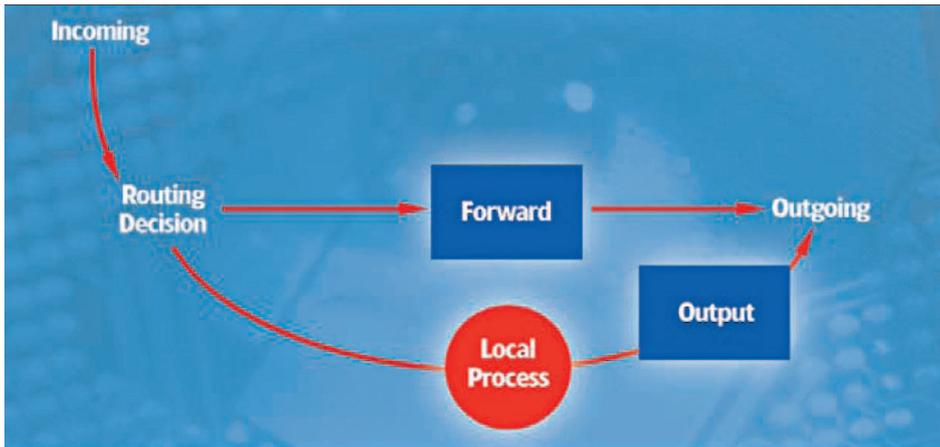
Sangat penting memang untuk rajin melakukan *patch* dan *update* terhadap *software-software bug* yang Anda gunakan di komputer Anda. Karena hal ini cukup menolong untuk sedikit menyulitkan para *hacker* dan pengganggu lain untuk bisa bersenang-senang dengan komputer Anda. Namun rasanya, *patch* yang *up-to-date* saja belum cukup untuk melindungi *resource* Anda yang berharga di dalam komputer. Maka dari itu, rasanya cukup penting untuk Anda bisa membatasi apa dan

siapa saja yang boleh masuk dan keluar dari dan ke perangkat komputer Anda. Semua proses ini bisa Anda lakukan dengan mengandalkan sebuah sistem pengaman khusus yang biasanya disebut dengan istilah *firewall* atau *IP filter*.

Apakah Firewall?

Mungkin banyak para praktisi komputer yang sudah sangat akrab dengan istilah ini. Namun rasanya, cukup adil untuk memberikan sedikit penjelasan singkat mengenai *firewall*, bagi para pendatang baru di dunia komputer. Firewall atau dalam arti harafiahnya adalah tembok api merupakan sebuah sistem yang memiliki tugas utama menjaga keamanan dari jaringan komputer dan semua perangkat yang ada di dalamnya. Firewall adalah sebuah sistem pengaman, jadi firewall bisa berupa apapun baik *hardware* maupun *software*.

Firewall dapat digunakan untuk memfilter paket-paket dari luar dan dalam jaringan di mana ia berada. Jika pada kondisi normal semua orang dari luar jaringan Anda dapat bermain-main ke komputer Anda, dengan firewall semua itu dapat diatasi dengan mudah.



Proses IP filtering dengan menggunakan *firewall* dan sejenisnya terjadi sebelum paket masuk diproses lebih lanjut atau sebelum paket keluar dilempar ke *interface* tujuannya.

Firewall merupakan perangkat jaringan yang berada di dalam kategori perangkat Layer 3 (*Network layer*) dan Layer 4 (*Transport layer*) dari protokol 7 OSI layer. Seperti diketahui, layer 3 adalah layer yang mengurus masalah pengalamatan IP, dan layer 4 adalah menangani permasalahan port-port komunikasi (TCP/UDP). Pada kebanyakan firewall, filtering belum bisa dilakukan pada level data link layer atau layer 2 pada 7 OSI layer. Jadi dengan demikian, sistem pengalamatan MAC dan *frame-frame* data belum bisa difilter. Maka dari itu, kebanyakan firewall pada umumnya melakukan filtering dan pembatasan berdasarkan pada alamat IP dan nomor port komunikasi yang ingin dituju atau diterimanya.

Firewall yang sederhana biasanya tidak memiliki kemampuan melakukan filterin terhadap paket berdasarkan isi dari paket tersebut. Sebagai contoh, firewall tidak memiliki kemampuan melakukan filtering terhadap e-mail bervirus yang Anda *download* atau terhadap halaman web yang tidak pantas untuk dibuka. Yang bisa dilakukan firewall adalah melakukan blokir terhadap alamat IP dari mail server yang mengirimkan virus atau alamat halaman web yang dilarang untuk dibuka. Dengan kata lain, firewall merupakan sistem pertahanan yang paling depan untuk jaringan Anda.

Tetapi, apakah hanya sampai di situ saja fungsi dari perangkat firewall? Ternyata banyak firewall yang memiliki

kelebihan lain selain daripada filtering IP address saja. Dengan kemampuannya membaca dan menganalisis paket-paket data yang masuk pada level IP, maka firewall pada umumnya memiliki kemampuan melakukan translasi IP address. Translasi di sini maksudnya adalah proses mengubah sebuah alamat IP dari sebuah alamat yang dikenal oleh jaringan diluar jaringan pribadi Anda, menjadi alamat yang hanya dapat dikenal dan dicapai dari jaringan lokal saja. Kemampuan ini kemudian menjadi sebuah fasilitas standar dari setiap firewall yang ada di dunia ini. Fasilitas ini sering kita kenal dengan istilah *Network Address Translation* (NAT).

Dengan menggunakan firewall yang dipadukan dengan fasilitas NAT, maka

komputer dan jaringan di belakangnya sudah cukup aman dibandingkan tidak sama sekali. Mengapa menggunakan NAT jaringan Anda dapat selangkah lebih aman? Bagaimana cara kerja NAT akan dibahas pada edisi berikutnya.

Bagaimana Membuat Firewall?

Firewall bisa Anda dapatkan dengan berbagai cara. Jika tidak ingin repot-repot membuat dari nol, Anda harus mengeluarkan uang yang cukup banyak untuk membeli perangkat keras firewall yang sudah jadi dan tinggal Anda pasang saja di jaringan. Tetapi perlu diingat, tidak semua perangkat keras firewall dapat bekerja hebat dalam melakukan IP filtering. Jadi akan percuma saja uang yang Anda keluarkan jika Anda membeli firewall yang tidak andal.

Jika Anda mau sedikit repot, namun hasilnya mungkin akan memuaskan Anda, buat saja sendiri perangkat firewall Anda. Yang Anda perlukan hanyalah sebuah PC dengan processor dan memory yang lumayan besar dan sebuah aplikasi firewall yang canggih dan lengkap yang dapat memenuhi semua kebutuhan Anda.

Aplikasi firewall yang lengkap dan canggih pada umumnya juga mengharuskan Anda mengeluarkan kocek yang tidak sedikit. Seperti misalnya *Checkpoint* yang sudah sangat terkenal dalam aplikasi firewall, untuk memilikinya Anda harus merogoh kocek

netfilter

firewalling, NAT, and packet mangling for Linux

[www](#) | [ftp](#) | [svn](#) | [lists](#) | [bugzilla](#) | [patchwork](#) | [people](#) | [planet](#)

About

[Coreteam](#)
[Contributors](#)
[History](#)
[License](#)
[Thanks](#)

Projects

[iptables](#)
[libnetlink](#)
[libnetfilter_log](#)
[libnetfilter_queue](#)
[libnetfilter_conntrack](#)
[conntrack](#)
[ipset](#)
[nf-hipac](#)
[patch-o-matic-ng](#)

Downloads

[SVN Repository](#)
[ftp Server](#)
[rsync Server](#)

News

[Yasuyuki Kozakai joins core team](#)
[planet.netfilter.org](#)

The netfilter.org project

What is netfilter.org?

netfilter.org is home to the software of the packet filtering framework inside the [Linux](#) 2.4.x and 2.6.x kernel series. Software commonly associated with netfilter.org is [iptables](#).

Software inside this framework enables packet filtering, network address [and port] translation (NAPT) and other packet mangling. It is the re-designed and heavily improved successor of the previous Linux 2.2.x [ipchains](#) and Linux 2.0.x [ipfwadm](#) systems.

netfilter is a set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack.

iptables is a generic table structure for the definition of rulesets. Each rule within an IP table consists of a number of classifiers (iptables matches) and one connected action (iptables target).

netfilter, ip_tables, connection tracking (ip_conntrack, nf_conntrack) and the NAT subsystem together build the major parts of the framework.

Main Features

Didalam situs <http://iptables.org>, Anda akan mendapatkan banyak sekali sumber referensi. Selain itu, Anda juga bisa men-download source programnya di sini.

```

david@macha:~ (pts/13)
iptables -A INPUT -s 127.0.0.1 -j ACCEPT
iptables -A INPUT -s 10.0.0.0/8 -j ACCEPT
#iptables -A INPUT -d 194.159.156.0/26 -j DROP
iptables -t nat -A PREROUTING -m state --state INVALID -j DROP

####
# Allow internal machines to access external gw IPs
####

iptables -t mangle -A PREROUTING -d 194.159.156.0/26 -s 10.0.0.0/8 -j MARK --set
-mark 7

iptables -t mangle -A PREROUTING -s 127.0.0.1 -j ACCEPT
iptables -t mangle -A PREROUTING -d 10.0.0.0/8 -s 10.0.0.0/8 -j ACCEPT
iptables -t mangle -A OUTPUT -d 10.0.0.0/8 -j ACCEPT
iptables -t mangle -A OUTPUT -j MARK --set-mark 100

iptables -t nat -A POSTROUTING -p tcp --dport 3128 -d 10.1.1.4 -j SNAT --to 10.1
.1.1
iptables -t nat -A POSTROUTING -m mark --mark 7 -j SNAT --to 10.1.1.1
iptables -t nat -A POSTROUTING -o lo -j ACCEPT
iptables -t nat -A POSTROUTING -m mark --mark 100 -j SNAT --to 194.159.156.14
53,1 18%

```

Sekumpulan *rule* dibuat dengan menggunakan halaman *console* tidak bisa dianggap remeh, karena meskipun hanya berupa teks-teks saja IPTables memiliki banyak sekali fitur.

yang lumayan banyak pula.

Namun jika Anda pecinta produk-produk *open source* dan sudah sangat familiar dengan lingkungan *open source* seperti misalnya *operating system* Linux, ada satu aplikasi firewall yang sangat hebat. Aplikasi ini tidak hanya canggih dan banyak fasilitasnya, namun aplikasi ini juga tidak akan membuat kantong Anda dirogoh dalam-dalam. Bahkan Anda bisa mendapatkannya gratis karena aplikasi ini pada umumnya merupakan bawaan *default* setiap distro Linux. Aplikasi dan sistem firewall di sistem *open source* tersebut dikenal dengan nama IPTables.

Dengan menggunakan IPTables, Anda dapat membuat firewall yang cukup canggih dengan program *open source* yang bisa dengan mudah Anda dapatkan di Internet. Memang perlu diakui, firewall dengan menggunakan IPTables

cukup sulit bagi pemula baik di bidang *networking* maupun pemula di bidang *operating system* Linux. Namun jika Anda pelajari lebih lanjut, sebenarnya firewall ini memiliki banyak sekali fitur dan kelebihan yang luar biasa.

Apa Itu IPTables?

IPTables merupakan sebuah fasilitas tambahan yang tersedia pada setiap perangkat komputer yang diinstall dengan sistem operasi Linux dan keluarganya. Anda harus mengaktifkannya terlebih dahulu fitur ini pada saat melakukan kompilasi kernel untuk dapat menggunakannya. IPTables merupakan fasilitas tambahan yang memiliki tugas untuk menjaga keamanan perangkat komputer Anda dalam jaringan. Atau dengan kata lain, IPTables merupakan sebuah firewall atau program IP filter *build-in* yang

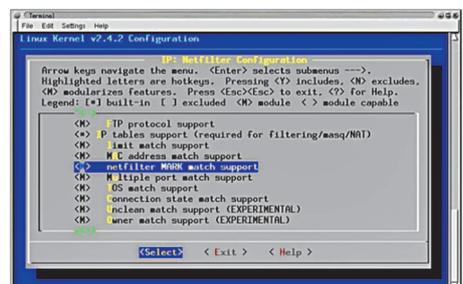
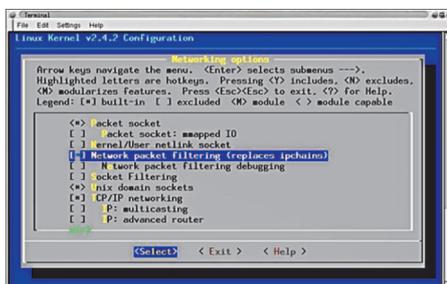
disediakan oleh kernel Linux untuk tetap menjaga agar perangkat Anda aman dalam berkomunikasi.

Mengapa Linux bersusah payah menyediakan fasilitas ini untuk Anda? Karena dari dulu Linux memang terkenal sebagai *operating system* yang unggul dalam segi keamanannya. Mulai dari kernel Linux versi 2.0, Linux sudah memberikan fasilitas penjaga keamanan berupa fasilitas bernama *ipfwadm*. Kemudian pada kernel 2.2, fasilitas bernama *ipchain* diimplementasikan di dalamnya dan menawarkan perkembangan yang sangat signifikan dalam menjaga keamanan.

Sejak kernel Linux memasuki versi 2.4, sistem firewall yang baru diterapkan di dalamnya. Semua jenis firewall *open source* yang ada seperti *ipfwadm* dan *ipchains* dapat berjalan di atasnya. Tidak ketinggalan juga, IPTables yang jauh lebih baru dan canggih dibandingkan keduanya juga bisa berjalan di atasnya. Maka itu, IPTables sangatlah perlu untuk dipelajari untuk Anda yang sedang mempelajari *operating system* Linux atau bahkan yang sudah menggunakannya. Karena jika menguasai IPTables, mengamankan jaringan Anda atau jaringan pribadi orang lain menjadi lebih hebat.

Di mana Anda Mendapatkan IPTables?

Untuk mendapatkan fasilitas IPTables, hal yang pertama harus dilakukan adalah memeriksa kernel versi berapa yang Anda gunakan. Jika menggunakan kernel Linux versi 2.4 ke atas, maka Anda boleh tenang karena fasilitas IPTables sudah merupakan *default* di dalamnya. Namun jika Anda menggunakan kernel di bawah itu, maka Anda harus melakukan modifikasi dan



Beginilah pengaturan kernel untuk mengaktifkan fasilitas IPTables Anda. Setelah terpilih semua untuk dipasang, simpan konfigurasi dan kompilasi kernel Anda. Setelah selesai IPTables siap digunakan.

editing pengaturan kernel yang rasanya cukup sulit dan memakan waktu lama. Maka dari itu, gunakanlah operating system Linux dengan kernel Linux 2.4 ke atas saja untuk lebih menghemat waktu dan tenaga.

Sebenarnya ada dua bagian penting yang bisa membuat perangkat komputer Anda menjadi sebuah firewall yang menggunakan fasilitas IPTables, yaitu pengaturan kernel dan penginstalan program IPTables itu sendiri. Jadi dengan demikian, untuk menginstal IPTables pada PC Anda, kedua bagian tersebut harus selalu dipenuhi.

Seperti telah dijelaskan di atas, versi kernel yang cocok untuk menghantarkan fasilitas ini untuk Anda adalah Linux dengan kernel 2.4 keatas. Apabila sebelumnya Anda menggunakan program Ipchain atau Ipfwadm, ada sebuah modul tambahan di dalam kernel 2.4 yang dapat tetap menggunakan pengaturan Anda yang lama pada program IPTables. Namun sebaiknya jika memang sudah memungkinkan, Anda harus membiasakan diri untuk menggunakan perintah dan ekspresi-ekspresi yang ada pada IPTables, karena IPTables jauh lebih hebat dibandingkan keduanya.

Namun jika Anda sudah memutuskan program firewall mana yang Anda gunakan, maka Anda hanya dapat mengaktifkan satu jenis firewall saja pada kernel level. Apakah itu IPTables, Ipchain, atau ipfwadm. Anda tidak dapat mengaktifkan ketiganya secara

bersamaan (melihat orang, namun disarankan untuk selalu menggunakan fasilitas IPTables. Setelah semua parameter pendukung ditambahkan dalam kernelnya, kompilasi kernel Anda, maka sesaat kemudian komputer Anda telah siap untuk diinstal program IPTables.

Setelah kernel selesai dimodifikasi (jika memang belum dikonfigurasi mendukung IPTables) langkah berikutnya adalah menginstal programnya. Anda dapat men-download programnya di link <http://www.netfilter.org/>. Bagaimana cara melakukan instalasi dan kompilasi kernelnya akan dibahas pada edisi berikutnya.

Istilah-istilah dan Ekspresi yang Ada pada IPTables

Istilah-istilah ekspresi di dalam firewall bawaan Linux ini memang sangat banyak. Setiap ekspresi pada umumnya mewakili satu fungsi spesifik untuk melakukan tugas menjaga keamanan. Meskipun banyak yang sudah sering terdengar pada aplikasi firewall lain atau pada perangkat-perangkat keras firewall, namun IPTables juga memiliki banyak sekali ekspresi yang merupakan ciri khasnya. Berikut ini adalah beberapa istilah dan ekspresi yang paling umum digunakan di dalam IP filtering:

● Drop/Deny

Ketika ada paket yang terkena *policy* seperti ini, maka paket tersebut langsung dihapus tanpa banyak basa-basi lagi. Tidak ada tindakan lebih lanjut lagi terhadap data yang telah dihapus dan tidak ada informasi balasan apakah paket tersebut benar-benar menghilang.

● Reject

Policy ini sebenarnya memiliki fungsi yang sama dengan *drop/deny*, namun bedanya policy ini akan mengirimkan pemberitahuan kepada si pengirimnya bahwa paket datanya ditolak.

● State

Policy ini memiliki fungsi untuk memberikan sebuah status kepada paket informasi yang melewatinya, dan kemudian status tersebut akan dibandingkan dengan paket yang lain. Sebagai contoh jika sebuah

paket merupakan paket pertama yang dilihat oleh IPTables, maka akan dianggap sebagai paket baru yang akan membuka jalan komunikasi. Informasi status ini dapat dimonitor menggunakan sistem *connection tracking* yang akan menyimpan semua informasi *state* tersebut.

● Chain

Chain merupakan seperangkat aturan yang saling berkaitan atau berantai yang dikenakan pada paket-paket data yang keluar-masuk. Setiap Chain memiliki kegunaan yang spesifik dan juga area penempatan yang spesifik.

● Table

Table merupakan kumpulan informasi pengaturan dan fasilitas yang ada pada IPTables. Di dalam aplikasi ini, terdapat tiga jenis table, yaitu tabel NAT, tabel Mangle, dan tabel Filter. Masing-masing tabel memiliki tugasnya masing-masing dalam aplikasi ini, misalnya tabel filter berfungsi untuk menampung pengaturan yang bertugas melakukan filtering paket, sedangkan tabel NAT untuk menampung informasi translasi NAT.

● Match

Satu kata ini dapat memiliki dua arti ketika berada dalam aplikasi firewall seperti IPTables. Arti pertama adalah dalam membuat sebaris aturan parameter yang dimasukkan haruslah match atau cocok. Misalnya dalam membuat sebuah aturan harus memasukkan alamat source IP dengan alamat yang sesuai format, baik alamat *network range* maupun alamat *single host*. Arti kedua adalah jika sebuah paket cocok dengan seluruh aturan yang dibuat, maka dapat dikatakan dengan istilah match.

● Target

Target merupakan seperangkat aturan yang akan melakukan eksekusi untuk mencapai tujuan akhir. Biasanya target ada di dalam aturan-aturan yang Anda buat. Jika aturan-aturan yang Anda buat Match seluruhnya dengan paket yang ditentukan, maka target akan bekerja mengeksekusi sesuatu hingga tujuan



Anda juga bisa menikmati pengaturan program ini melalui halaman program GUI khusus yang akan memudahkan Anda.



Bahkan Anda bisa mengonfigurasi IPTables melalui halaman web dengan bantuan program Bifrost. Namun sayangnya, program ini tidak didistribusikan secara gratis.

akhirnya tercapai. Contoh dari target misalnya jika Match maka paket dengan alamat IP 1.1.1.1 harus di-DROP atau di NAT atau diteruskan, dan sebagainya. Tujuan akhir seperti DROP, NAT, atau yang lainnya tadilah yang disebut dengan target.

● Rule

Rule atau aturan merupakan sebuah baris aturan atau lebih yang di dalamnya berisi apa saja yang ingin Anda kenai tujuan akhir atau target yang Anda buat. Misalnya alamat IP tujuan 1.1.1.1 dengan nomor port 25 dikenakan target DROP. Pemeriksaan yang dilanjutkan dengan sebuah tindakan inilah yang disebut dengan istilah *Rule*.

● Ruleset

Ruleset merupakan kumpulan dari rule yang Anda buat yang kemudian dipasang pada implementasi IP filtering. Dalam kasus pada IPTables sebuah ruleset sudah meliputi seperangkat aturan pada tabel filter, tabel NAT dan tabel mangle. Dan semuanya berada dalam satu urutan CHAIN yang dibuat sebelumnya. Pada umumnya, ruleset ditulis pada file konfigurasi atau sejenisnya.

● Jump

Jump merupakan sebuah instruksi yang akan mengarahkan sebuah rule

untuk menuju ke target tertentu. Instruksi jump pasti ada dalam setiap target pada rule IPTables, kecuali Anda menggunakan CHAIN yang lain sebagai tujuan akhir dari sebuah rule. Ketika sebuah paket Match dengan rule yang dibuat, maka instruksi jump akan bekerja mengarahkan paket tersebut ke sebuah target atau ke CHAIN yang lainnya untuk diproses lebih lanjut.

● Connection tracking

Connection tracking merupakan sebuah fasilitas untuk memonitor atau melacak koneksi-koneksi atau aliran paket yang lalu-lalang melalui firewall. Fasilitas ini biasanya digunakan pada perangkat yang memiliki kekuatan *processing* dan memory yang tinggi. Jika perangkat Anda tidak memiliki spesifikasi yang cukup, sebaiknya tidak menggunakan fasilitas ini. Dengan adanya fasilitas ini, keuntungannya adalah firewall Anda akan lebih aman dan dapat termonitor dengan baik.

● Accept

Eksprei ini sebenarnya merupakan sebuah target yang merupakan kebalikan dari fungsi target DROP dan DENY. *Accept* menandakan bahwa apabila ada paket yang MATCH dengan rule yang dibuat maka paket tersebut akan dile-

watkan ke tujuan yang diinginkan.

● Policy

Ada dua arti yang menggambarkan istilah policy dalam dunia IP filtering. Pertama, policy diartikan sebagai sebuah peraturan akhir yang akan mengarahkan paket-paket yang tidak MATCH dengan rule apapun ke tujuan akhirnya. Pengertian inilah yang akan kita pakai untuk istilah policy pada pembahasan selanjutnya. Arti kedua adalah security policy atau peraturan keamanan yang biasanya dimiliki oleh implementer dari sistem firewall. Contohnya sebuah perusahaan memiliki peraturan dimana pegawai dengan tingkat staff tidak diperbolehkan mengakses Internet, atau para *supervisor* tidak diperbolehkan membuka halaman intranet. Semua itu merupakan *security policy* yang idealnya harus didokumentasikan dengan baik.

Fasilitas Hebat yang Cukup Rumit

IPTables memang sangat hebat. Banyak sekali fasilitas dan kemampuan yang dapat diberikannya untuk mengamankan PC dan jaringan milik Anda dibelakangnya. Namun saking hebatnya, terkadang pengguna menjadi cukup sulit untuk mempelajarinya pada awal pemakaiannya. Namun setelah Anda kuasai logikanya, maka IPTables bisa menjadi tameng yang kuat untuk Anda gunakan dalam menahan serangan dari luar. Dengan IPTables yang terkonfigurasi dengan baik, maka Anda boleh sedikit lebih tenang karena PC Linux milik Anda sudah jauh lebih aman daripada sebelumnya. Selamat mencoba!

Pada edisi selanjutnya akan dibahas mengenai cara instalasi secara umum, pengaturan sederhana program IPTables dan sedikit trik-triknya. Selamat belajar! ■

LEBIH LANJUT

- www.netfilter.org
- www.linuxguruz.com/iptables/howto/iptables-HOWTO.html
- <http://www.faqs.org/docs/iptables/>

Tingkat keamanan yang tinggi tidak selalu ditandai oleh jumlah petugas kemanan yang semakin banyak. Justru terletak dari teknologi yang digunakan. Bila petugas keamanan bertambah banyak, tapi penjahat semakin pintar menyamarkan diri dan barang bawaannya, tetap saja dapat terjadi kejahatan.

Fadilla Mutiarawati



Tingkat Keamanan Makin Ketat dengan Teknologi yang Tepat

► Penjahat dari hari ke hari sudah semakin pintar. Banyak kejahatan yang dilakukan menggunakan teknologi canggih. Bahkan tidak jarang berlomba dengan teknologi kemanan itu sendiri. Misalnya saja sebuah virus yang menyerang komputer Anda. Semakin hari semakin buas. Dan program antivirus pun semakin hari juga semakin canggih berusaha untuk selalu menandingi. Begitu pula dengan virus yang semakin hari juga terus dikembangkan untuk menggagalkan satu antivirus dengan antivirus yang lain.

Begitu pula penjahat semakin canggih alat kemanan, cara kerja mereka pun semakin canggih dan lihai. Sayangnya, di Indonesia tingkat kemanan yang sangat ketat jarang sekali ditemukan kecuali pada tempat-tempat tertentu saja. Misalnya, bandara, kantor konsulat, atau gedung-gedung khusus. Kebanyakan pihak kemanan sebuah gedung hanya menerapkan pemeriksaan alakadarnya atau sekadar formalitas dengan

alat *metal detector*. Yang terkadang aktif terkadang mati. Bahkan yang terkadang sangat mengganggu kenyamanan adalah seseorang diminta untuk memperlihatkan isi tasnya pada petugas kemanan. Padahal hal ini sebenarnya dapat dihindari. Dengan teknologi yang tepat, tidak hanya tingkat kemanan yang meningkat, melainkan pengunjung juga akan merasa lebih nyaman.

Perangkat apa saja sebenarnya yang dapat digunakan untuk meningkatkan kemanan? Banyak sekali dengan menggunakan kamera CCTV atau mungkin dengan menggunakan sinar X. Sedangkan untuk keamanan tempat-tempat tertentu, dapat saja menggunakan teknologi *biometrics* yang kini sudah mulai marak digunakan. Sebagian dari teknologi tersebut memang masih tergolong cukup mahal. Tapi untuk melindungi sesuatu yang sangat berharga, rasanya nilai teknologi tersebut tidak akan terlalu berarti.

CCTV

CCTV adalah teknologi yang cukup konvensional yang sudah lebih dulu hadir. Dengan kamera CCTV yang sangat mungil, seorang petugas kemanan dapat memantau keadaan. Dan bila ada kejahatan terjadi, rekaman pada CCTV cukup dapat dijadikan barang bukti. Oleh sebab itu, keberadaan CCTV banyak digunakan pada tempat-tempat yang rawan akan kejahatan pencurian seperti



X-Ray yang biasa digunakan untuk memeriksa bagasi di bandara.



Dengan X-Ray, tidak perlu lagi penggeledahan yang tidak sopan.

supermarket, dan mesin ATM.

Bentuk kamera yang semakin hari semakin kecil membuatnya sangat fleksibel untuk diletakkan di mana saja. Belum lagi instalasi CCTV tidak terlalu sulit. Bahkan, jika diinginkan kini juga sudah tersedia CCTV yang tidak menggunakan kabel.

Keberadaan CCTV sebagai alat keamanan kadang menyulitkan kadang tidak. Untuk keamanan yang butuh pantauan ketat, tentu akan membutuhkan kehadiran SDM sebagai operator atau petugas pemantau. Sedangkan bila CCTV hanya digunakan sebagai alat dokumentasi atau bukti di kemudian hari. Petugas operator hanya perlu merekamnya.

Biometrics

Teknologi *biometrics* adalah teknologi keamanan yang menggunakan bagian tubuh sebagai identitas. Dunia medis mengatakan bahwa ada berapa bagian tubuh kita yang sangat unik. Artinya, tidak dimiliki oleh lebih dari satu individu. Contohnya saja sidik jari atau retina mata. Meskipun bentuk atau warna mata bisa saja sama, namun retina mata belum tentu sama. Begitu juga dengan suara dan struktur wajah. Bagian-bagian unik inilah yang kemudian dikembangkan sebagai atribut keamanan.

Sebagai bagian dari teknologi keamanan, biometrics memiliki dua fungsi sekaligus yang dapat dijalankan terpisah maupun secara bersamaan. Yang pertama sebagai pencatat ID atau sebagai alat verifikasi (*password*).

Teknologi biometrics hampir dapat diterapkan di mana saja. Mulai untuk melindungi sebuah barang tertentu dari akses yang tidak diinginkan, seperti komputer. Sampai untuk melindungi

sebuah ruangan yang ramai dari orang-orang tertentu. Misalnya, untuk mengetahui keberadaan teroris atau penjahat lain di bandara.

Cara kerja teknologi keamanan yang satu ini hampir sama dengan teknologi keamanan lain yang sangat bergantung kepada sensor. Sensor yang digunakan pada teknologi biometrics cenderung mahal dan semakin akurat ketajamannya maka akan semakin mahal.

Selain sensor, bagian yang tidak kalah penting dari biometrics adalah data. Bagaimana Anda menyimpan data pada sebuah sistem sangat penting. Sebab biometrics adalah teknologi yang bergantung kepada data. Bila data yang disimpan tidak aman atau lengkap, kemungkinan adanya penyusup ke sistem ini akan lebih besar.

Menurut sistemnya biometrics sendiri terbagi atas tiga macam, yaitu:

1. Sistem yang menyimpan data langsung pada alat.

Dengan sistem ini, data akan disimpan pada media penyimpanan yang berada dalam alat detektor. Jika sewaktu-waktu mesin harus di-*reset* atau dikembalikan ke posisi awal, maka data yang ada dapat saja ikut terhapus. Sehingga petugas harus meng-input ulang. Jika data yang dimasukkan sangat banyak tentu akan sangat merepotkan, lain halnya bila data tidak terlalu banyak. Biometrics dengan sistem ini sangat cocok untuk diterapkan pada sebuah alat tertentu yang tidak digunakan oleh banyak orang atau untuk melindungi sebuah ruang khusus, yang juga tidak diakses oleh banyak pengunjungnya.

2. Sistem yang menyimpan data pada jaringan.

Sistem yang kedua memanfaatkan jaringan untuk menyimpan datanya. Sistem yang kedua sangat efektif bagi aplikasi yang memang dipergunakan untuk banyak *user*. Misalnya saja untuk data absen karyawan atau siswa. Bentuk fisik yang ditampilkan oleh alat juga tidak perlu terlalu besar. Karena data tidak akan diproses langsung pada alat. Melainkan dikirim dahulu ke sebuah jaringan baru kemudian diproses dan disimpan. Sistem ini memang membutuhkan waktu lama.

Tetapi cukup efektif untuk data yang besar. Karena tidak akan terkena risiko data hilang pada saat proses reset pada alat harus dilakukan.

3. Sistem yang menyimpan data pada sebuah chip.

Sistem yang terakhir ini menggunakan media tambahan berupa chip untuk menyimpan data si pemilik ID. Sehingga untuk menggunakannya seseorang harus membawanya. Untuk sistem yang terakhir ini, akan sangat efektif diterapkan untuk yang memiliki pengguna sangat banyak atau bila alatnya hendak diletakkan di tempat umum. Misalnya saja untuk keamanan di mesin ATM atau hanya sekadar sebagai ID masuk dalam sebuah gedung.

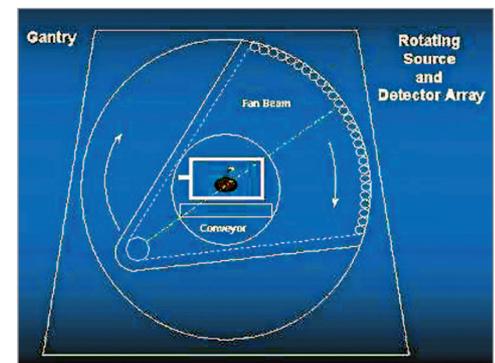
Sedangkan bagian tubuh yang saat ini sudah mulai digunakan sebagai ID atau password adalah:

● Sidik Jari

Ini adalah bagian tubuh yang penggunaannya sangat populer baik sebagai ID maupun sebagai password. Sensor yang digunakan untuk men-*scan* sidik jari sangat bervariasi. Ada sensor yang hanya dapat memeriksa satu sidik jari saja ada yang dapat memeriksa lebih dari satu sidik jari.

Luka pada sidik jari dapat mengakibatkan sidik jari sulit dideteksi. Namun, bukan berarti tidak bisa. Selama luka tersebut tidak terlalu dalam ada beberapa sensor yang masih dapat mengenalinya. Tentu saja sensor-sensor dengan ketajaman seperti ini akan lebih mahal harganya ketimbang sensor sidik jari dengan ketajaman biasa.

Penerapan sidik jari sebagai bagian dari sistem keamanan kini sudah se-



CT Scan dapat melihat isi tas dari berbagai perspektif.

makin luas. Bahkan saat ini sudah ada mouse yang penggunaannya membutuhkan sidik jari penggunaannya.

● Geometris Tangan

Lain sidik jari lain pula yang dimaksud dengan geometris tangan atau yang dikenal juga dengan bentuk tangan. Nilai-nilai yang menjadi bagian dari datanya adalah, ukuran tangan, bentuk telapak tangan, sampai bentuk dan ukuran masing-masing jari. Sensor yang digunakan untuk mendeteksi geometris tangan berbeda dengan sensor yang digunakan untuk mendeteksi sidik jari. Cara pengambilan sampel juga lebih rumit, karena harus dilakukan dari berbagai perspektif. Oleh sebab itu, biometrics ini dianggap lebih akurat dan lebih sulit untuk dipalsukan datanya. Namun, proses pengaksesan juga akan berjalan lebih lama. Oleh sebab itu, sebaiknya jangan menggunakan sistem ini untuk ruangan yang terbuka atau untuk aplikasi yang dimanfaatkan oleh banyak orang (seperti absensi).

● Mata

Mata manusia sangat unik. Meskipun secara kasat mata, setiap bola mata manusia hampir sama. Ada dua bagian yang kerap menjadi bagian dari biometrics mata, yaitu retina dan iris mata.

Iris mata lebih mudah penggunaannya dibandingkan dengan retina mata. Untuk menganalisis retina mata, seorang pengguna harus menatap pada fokus yang telah ditentukan dan proses analisis juga tidak akan dapat dilakukan bila user menggunakan kaca mata.

Lain halnya dengan iris mata. Teknologi dengan iris mata tidak sesulit retina mata. User tidak perlu menatap lurus ke fokus. Dan pengguna kaca mata masih dapat dikenali.



X-Ray dengan daya tampung lebih besar beradiasi lebih besar juga.

● Bentuk Wajah

Teknologi biometrics yang menganalisis bentuk wajah sudah juga digunakan di beberapa tempat. Salah satunya bandara. Perangkat yang difungsikan sebagai sensor untuk teknologi ini umumnya adalah kamera CCTV biasa. Dan sistem yang digunakan adalah sistem yang datanya disimpan dalam sebuah jaringan. Sedangkan proses kerjanya adalah sebagai berikut. Gambar yang diperoleh oleh kamera CCTV secara otomatis akan diolah oleh komputer yang terhubung langsung dengan data kepolisian. Setiap wajah yang lewat akan dilihat kecocokannya dengan data yang ada pada jaringan. Jika ada kemiripan, maka nyala alarm akan berbunyi dan memberi tahu kepada petugas.

Untuk menggunakan bentuk wajah sebagai bagian dari sistem keamanan, sampel yang diambil harus lengkap, artinya pengambilan sampel harus dilakukan dari berbagai arah. Sama halnya seperti pada penggunaan geometris tangan.

● Suara

Gelombang suara juga dapat dijadikan identitas yang unik. Namun sayangnya, untuk yang satu ini keadaan sekitar sangat mempengaruhi. Sehingga untuk menerapkannya harus benar-benar di ruangan atau lingkungan yang tidak ramai. Dan semakin tinggi toleransi yang dimiliki oleh sebuah sensor akan membuat harga sensor akan semakin tinggi.

Metal Detector

Ini adalah alat yang paling sering ditemui masyarakat belakangan ini sejak merebaknya isu terror bom di Indonesia. Di mana-mana petugas keamanan baik gedung kantor sampai tempat hiburan dan belanja sibuk menenteng-nenteng



X-Rays.



Metal detector.

alat berwarna hitam. Alat ini biasa ditempelkan pada barang bawaan pengunjung. Untuk mengetahui apakah pengunjung membawa barang berbahaya atau tidak. Selain dengan alat semacam pentungan berwarna hitam, kadang pengunjung juga harus melewati sebuah alat yang menyerupai gawang kecil. Bila pengunjung mengantongi perangkat berbahan logam atau metal seperti ponsel, maka alat itu akan berbunyi nyaring sekali. Begitu juga dengan alat berwarna hitam yang menyerupai pentungan tersebut.

Alat ini dikenal juga dengan sebutan *metal detector*. Fungsinya adalah untuk mengetahui keberadaan komponen logam atau metal yang berada pada targetnya. Pada tempat-tempat tertentu, keberadaan metal detector memang membantu kemanan gedung. Namun, apa yang diamankan oleh metal detector? Tidak lain adalah semua komponen yang mengandung logam. Mulai dari benda tajam seperti pisau, gunting, penggaris sampai pena, dan ponsel. Semuanya akan memancing bunyi sebuah metal detector.

Jika untuk melindungi sebuah tempat dari pengunjung yang membawa sebuah bom. Alat keamanan ini dapat dikatakan kurang efektif, karena bahan kimia tidak akan dapat terdeteksi oleh alat ini. Dan pada umumnya, bom terbuat dari campuran bahan kimia.

Dalam melakukan proses deteksi, metal detector menggunakan kawat

tembaga sebagai pengumpan sinyal. Bila sinyal tersebut bertabrakan dengan logam, maka akan terjadi medan magnet yang menyebabkan *echo* (gema) yang panjang.

Namun, keberadaan metal detector sendiri kini tidak lagi dapat dijadikan satu-satunya komponen keamanan. Karena sangat sering apa yang dibawa oleh pengunjung digeledah. Hal ini tentu saja mengganggu hak privasi seseorang. Oleh sebab itu, bila sebuah institusi ingin menjaga keamanan tempatnya tanpa harus melanggar hak privasi pengunjungnya, maka ia harus menyediakan sebuah alat deteksi lain yang lebih sopan. Salah satu contohnya X-Ray.

X-Ray

Barang apa yang sedang dibawa? Sekali lagi, membuka tas seseorang bukanlah tindakan yang sopan. Karena ada beberapa bawaan yang sifatnya sangat pribadi. Dan tindakan menggeledah tas bukanlah hal yang tepat dilakukan. Meskipun atas nama keamanan. Jika memang ingin meningkatkan keamanan sebuah gedung, maka pihak pengelola gedung harus rela mengeluarkan kocek lebih mahal. Misalnya dengan menggunakan teknologi X-Ray. Dengan teknologi X-Ray, seseorang tidak perlu lagi merasa sungkan. Karena untuk bawaan tertentu tidak akan terdeteksi. Misalnya saja pembalut atau kondom.

X-Ray bukanlah teknologi baru. Kehadirannya sudah lama digunakan oleh masyarakat, khususnya bagi mereka yang pernah melakukan pemeriksaan menyeluruh di rumah sakit. Kemampuannya dalam melihat jauh lebih ke dalam dimanfaatkan dunia kedokteran untuk menelaah lebih jauh tentang apa yang terjadi pada bagian dalam tubuh

manusia.

Namun ternyata, sinar X ini tidak hanya mampu menelaah komponen dalam tubuh manusia, melainkan juga mampu menelaah isi sebuah tas. Baik tas kecil sampai tas besar sekalipun.

Kemampuannya inilah yang kemudian dilirik oleh pelaku sistem keamanan untuk kemudian digunakan sebagai bagian dari komponen penjaga keamanan. Seperti halnya dengan sinar X dalam dunia kedokteran. Sinar X yang digunakan untuk sistem keamanan juga memiliki radiasi. Hanya saja, radiasinya bukan membahayakan si pemilik barang, melainkan barang yang sedang diperiksa. Salah satu yang sangat rentan terhadap radiasi sinar X adalah film. Lembaran film kamera manual sering rusak bila terkena radiasi sinar X.

Namun, lain dengan sekarang. Radiasi yang digunakan sinar X untuk pemeriksaan tidak lagi setinggi dulu. Kini sinar X yang biasa digunakan di bandara contohnya sudah aman untuk digunakan pada film.

Namun bukan berarti boleh diletakkan dalam bagasi pesawat sebab sinar X yang memeriksa bagasi umumnya menggunakan radiasi yang lebih tinggi. Mengingat tumpukan barang yang diperiksa jauh lebih banyak.

Dengan sinar X, setiap jenis barang memiliki warna berbeda. Misalnya bahan organik dengan bahan bukan organik akan tampil dengan warna berbeda. Begitu pula halnya dengan barang yang mengandung metal. Bukan berarti barang organik luput dari perhatian. Umumnya, petugas operator X-Ray sudah mendapatkan pendidikan untuk membedakan bahan organik yang dapat berfungsi sebagai bom atau bukan.

CT Scan

Selain sinar X yang diarahkan searah saja, ada alat keamanan lain yang tidak kalah canggihnya, yaitu CT Scan (*computer tomography scanner*). Teknologi ini menggunakan beberapa sinar X sekaligus untuk memeriksa seluruh dimensi setiap barang. Dengan CT Scan Anda tidak hanya memeproleh gambaran mengenai isi tas saja, melainkan lengkap dengan ukuran dan berat masing-masing perangkat yang ada dalam tas tersebut.



Dengan X-Ray setiap bahan memiliki warna berbeda.

Bila ada sebuah perangkat yang berat atau bentuknya tidak sesuai dengan fungsinya, maka komputer akan memperingati petugas operator CT Scan.

Proses pemeriksaan dengan CT Scan lebih lama ketimbang X-Ray. Namun, data yang dihasilkan memang lebih lengkap. Sebaiknya penggunaan CT-Scan hanya dilakukan untuk orang-orang atau bawaan yang sangat mencurigakan saja. Jangan sampai terjadi antrian yang tidak berarti pada pintu masuk.

RFID

Lain di bandara lain pula di pertokoan. Saat ini keberadaan teknologi *labeling* sudah sangat canggih. Dengan menggunakan label berfrekuensi radio, tidak perlu lagi khawatir produk dari supermarket tersebut kecurian. Karena setiap barang atau produk yang melewati batas akan membuat alarm berbunyi.

Teknologi mana yang akan digunakan? Terserah yang mana saja, asalkan menyesuaikan dengan keadaan. Bila memang ingin menggunakan sebagai *security* sebuah ruangan atau sebagai absensi, kartu dengan cip sidik jari cukup baik.

Namun bila akan menggunakannya untuk memeriksa pengunjung toko Anda atau gedung Anda, sebaiknya carilah teknologi yang sopan. Mungkin sinar X dapat menjadi jawabannya. Jangan menggunakan metal detector jika yang dicari bukanlah benda tajam. Atau dengan tidak sopan menggeledah tas pengunjung toko atau gedung Anda. ■



Mouse dengan sidik jari.

LEBIH LANJUT

- www.findbiometrics.com
- www.iwsinc.com/Biometrics

Atasi driver perangkat yang menyulitkan dan aplikasi *uninstall* yang aneh dengan mengetahui sedikit tentang file INF Windows.

Gunung Sarjono



Bagaimana INF Bekerja?

► *Software* Windows biasanya diinstalasi melalui satu file *executable*, seperti *setup.exe*. File meng-*unzip* semua file yang dibutuhkannya, membuat struktur folder sendiri dan memodifikasi registry Anda supaya sesuai dengan kebutuhan program. Itu tidak masalah jika berjalan

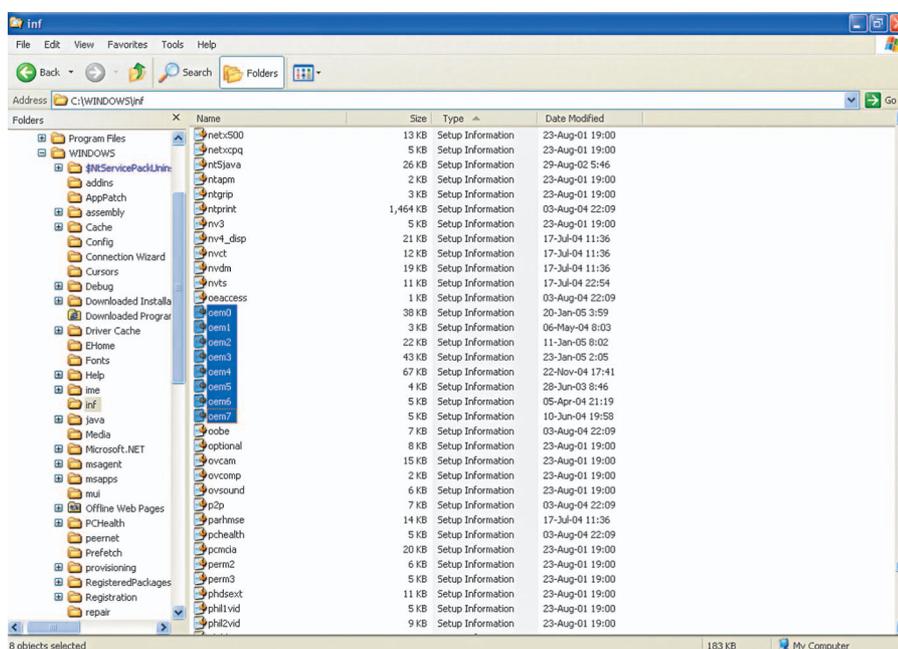
dengan baik, tetapi bagaimana jika program menyebabkan masalah, tidak terinstalasi dengan baik, atau Anda tidak bisa menghapusnya? Kalau begitu Anda harus meminta bantuan kepada pembuatnya, karena tidak ada cara untuk menyesuaikan file *setup.exe* dengan

sistem Anda, atau mengetahui apa sebenarnya yang telah dilakukan.

Namun, masalahnya tidak selalu seperti itu. Banyak driver perangkat, komponen Windows dan program kecil lain yang diinstalasi melalui file *.INF* (Information). Ini adalah file teks biasa yang bisa Anda lihat di Notepad, untuk melihat apa sebenarnya yang terjadi pada proses instalasi, file mana yang di-copy, nilai registry mana yang dibuat dan banyak lagi. Mereka bisa digunakan untuk melakukan instalasi secara manual (klik kanan dan pilih *Install*). Dengan sedikit latihan, Anda bisa membuat file *INF* sendiri untuk menginstalasi program kecil (jika Anda seorang *developer*) atau memastikan semua PC jaringan Anda mempunyai setting registry yang sama, misalnya.

Membuang Driver

Beberapa perangkat USB rewel mengenai instalasi, meminta Anda menjalankan *software setup* sebelum menghubungkan mereka. Jika Anda melanggar, atau menjumpai masalah instalasi yang lain, maka Anda mendapatkan *hardware* tidak bekerja



Lihat file *oemxxx.inf* untuk mengetahui program yang dimasukkan oleh pihak ketiga ke dalam sistem Anda.

dengan baik. Jadi apa yang bisa Anda lakukan selanjutnya? Menghapus dan menginstalasi ulang hardware bisa membantu, tetapi itu bisa lebih sulit dari yang Anda bayangkan. Mengapa? Karena file INF hardware yang asli, dan file driver yang berhubungan, mungkin masih ada di PC Anda. Hubungkan lagi perangkat dan Windows mencari file INF, lalu menginstalasi driver, tidak peduli apa pun yang Anda lakukan.

Setelah Anda mengetahuinya itu mudah diatasi. Buka folder \WIN-

DOWS\inf dan cari file yang berisi nama pabrikan perangkat (atau urutkan berdasarkan tanggal dan cari file yang paling terakhir). Setelah Anda yakin menemukan file yang benar (berbahaya jika salah menghapus, jadi harus 100 persen yakin), gunakan prosedur un-install yang disediakan oleh perangkat, kemudian ganti nama file .INF menjadi .OLD, dan reboot. Windows tidak akan lagi bisa memuat driver yang lama dan meminta Anda untuk memasukkan yang baru. Tidak perlu menunggu sampai

situasi ini muncul baru Anda mulai melihat file .INF. Tidak ada salahnya mengecek untuk melihat program apa saja yang dimasukkan ke sistem Anda. Tempat yang baik untuk memulai adalah file oemxx.inf, karena file ini dimasukkan oleh instalasi hardware dan software pihak ketiga.

File itu sendiri dibagi ke dalam beberapa bagian, masing-masing dengan header dalam kurung kotak. Meskipun file yang lebih besar bersifat sangat teknis, banyak yang bisa Anda ketahui

BAGIAN INF

■ Berikut adalah rangkuman dari bagian-bagian yang digunakan pada file INF. Nama bagian tidak *case-sensitive*, jadi version, VERSION, dan Version adalah nama yang sama-sama valid. Nama-nama bagian berikut disusun berdasarkan urutan mereka pada umumnya di sebagian besar file INF. Namun, bagian-bagian ini disusun secara acak. Setup mencari bagian file INF berdasarkan nama, bukan nomor urutnya, baik itu INF sistem atau yang dibuat oleh *writer*.

Version

Ini adalah bagian yang diperlukan oleh setiap file INF. Untuk instalasi pada Windows 2000 ke atas, dan/atau Windows 9x/Me, bagian ini harus mempunyai entri *Signature* yang valid

SourceDisksNames

Bagian ini diperlukan jika file INF mempunyai bagian SourceDisksFiles yang dibutuhkan. Bagian ini diperlukan untuk menginstalasi perangkat IHV/OEM dan driver mereka. Bagian ini juga diperlukan dalam file INF yang menginstalasi DLL pendukung sebagai pelengkap installer perangkat tambahan atau DLL baru sebagai pelengkap installer OS. Bagian ini juga menunjukkan lokasi harddisk atau CD yang digunakan untuk instalasi. Sebaliknya, file INF dari sistem masing-masing menyebutkan LayoutFile di bagian Version dan menyediakan paling sedikit satu file INF lain yang merinci isi sumber distribusi dan gambaran dari semua komponen software yang diinstalasi.

SourceDisksFiles

Bagian ini menyebutkan lokasi file yang diinstalasi dari media distribusi ke tujuan pada mesin target. File INF yang mempunyai bagian ini juga harus mempunyai bagian SourceDisksNames.

ClassInstall32

Bagian ini menginisialisasi class instalasi perangkat. Bagian ini diperlukan dalam semua file INF class installer. File INF yang menginstalasi perangkat dan driver mereka di pada *class* perangkat yang ditentukan sistem tidak memerlukan bagian ini.

ClassInstall32.Services

File INF biasanya menggunakan bagian ClassInstall32 dengan paling sedikit satu perintah AddService untuk mengontrol bagaimana dan kapan service suatu class dimuat, ketergantungan yang mungkin dipunyai dengan service lain, dan seterusnya.

DestinationDirs

File INF perangkat/driver mempunyai bagian DestinationDirs untuk menentukan direktori tujuan default bagi salinan INF dari file yang terdapat pada media distribusi atau yang terdapat pada file layout INF. Bagian ini diperlukan, kecuali jika file INF menginstalasi perangkat seperti modem atau monitor, yang tidak mempunyai file INF lain, selain miliknya.

ControlFlags

Bagian ini mengontrol apakah *Add Hardware Wizard* menampilkan daftar

Models INF, di mana dari situ user pilih sendiri perangkat (atau model perangkat) yang akan diinstalasi. Bagian ini juga mengontrol apakah file INF hanya digunakan untuk menransfer file dari media distribusi.

Secara umum, kebanyakan file INF untuk driver perangkat atau untuk installer class sistem mempunyai bagian ini sehingga mereka bisa mengeluarkan paling sedikit satu “model” dari daftar (perangkat yang dapat diinstalasi) yang ditampilkan ke user. File INF yang hanya menginstalasi perangkat PnP tidak menampilkan semua informasi model terkait.

Manufacturer

Bagian ini diperlukan untuk perangkat dan driver mereka. Bagian Manufacturer kadang disebut “Table of Contents”, karena masing-masing entrinya menunjukkan *Models* INF yang dibuat *writer*, yang pada akhirnya, menunjuk bagian INF tambahan yang dibuat *writer*, seperti bagian *DDInstall*, *DDInstall.Services*, dan seterusnya.

Models (per Manufacturer)

Bagian ini diperlukan untuk mengidentifikasi perangkat yang driver-nya akan diinstalasi oleh file INF. Ia menentukan pemetaan antara nama generik (string) perangkat, ID perangkat, dan nama dari bagian *DDInstall*. File INF yang menginstalasi satu atau beberapa perangkat dan driver dari satu provider hanya mempunyai satu *Models*, tetapi file INF sistem bisa mempunyai banyak *Models*.

tanpa belajar sama sekali. Sebagai contoh, bagian [Manufacturer] menunjukkan siapa yang membuat file, sementara .FILES menampilkan file yang diinstalasi, [DestinationDirs] menunjukkan ke mana tujuan mereka, dan [AddReg] menampilkan entri registry yang diperlukan instalasi.

Semua itu sangat berharga, terutama jika Anda ingin benar-benar menghapus suatu program atau driver. Namun, Anda harus sangat hati-hati. Menghapus driver yang salah bisa menyebabkan PC Anda

tidak bisa boot, bahkan masuk ke dalam Safe Mode, jadi bekerja dengan file INF hanya untuk yang berani atau ahli saja. Kecuali, jika ada uninstall di dalamnya yang bisa Anda gunakan.

Menghapus program

Beberapa driver, aplikasi atau komponen Windows tidak dilengkapi dengan opsi uninstall, tetapi masih bisa dihapus dengan menggunakan file INF. Anda jangan coba untuk melakukan ini kecuali jika tidak ada pilihan lain. Namun, pada

situasi tertentu ini merupakan cara yang berguna.

Contoh yang aman mari kita ambil Wordpad. Misalkan Anda menggunakan program secara reguler, tetapi sekarang tidak berfungsi dengan baik, dan Anda pikir meng-uninstall dan instalasi ulang bisa membantu. Sayangnya, Anda tidak akan menemukan Wordpad tercantum pada komponen yang dapat di-uninstall di Add/Remove Programs, jadi Anda harus mencari jalan lain-dan itu adalah file INF.

Buka \WINDOWS\inf dan Anda akan

DDInstall

Bagian ini diperlukan untuk melakukan instalasi yang sebenarnya dari perangkat yang terdapat pada bagian Models, bersama dengan driver untuk masing-masing perangkat tersebut. Bagian DDInstall bisa digunakan bersama-sama oleh beberapa Models.

DDInstall.Services

Bagian ini diperlukan sebagai perluasan dari DDInstall untuk driver perangkat Windows 2000 ke atas, termasuk semua driver WDM (kecuali file INF untuk modem dan monitor). Bagian ini mengontrol bagaimana dan kapan service suatu driver dimulai, ketergantungannya (jika ada), dan seterusnya. Bagian ini juga mengatur pencatatan event jika driver perangkat mendukungnya.

DDInstall.HW

Bagian opsional ini menambahkan informasi yang terkait dengan perangkat (dan biasanya, independen terhadap driver) ke registry atau menghapus informasi tersebut dari registry.

DDInstall.CoInstaller

Bagian opsional ini mendaftarkan satu atau beberapa installer pendukung yang terdapat pada media distribusi untuk melengkapi operasional installer sistem atau installer perangkat yang ada. Co-installer adalah DLL Win32 yang disediakan oleh IHV/OEM yang biasanya menulis informasi konfigurasi tambahan ke registry atau melakukan tugas instalasi lain yang memerlukan informasi mesin terkait yang tidak tersedia pada

waktu file INF perangkat dibuat.

DDInstall.FactDef

Bagian ini harus dimasukkan ke dalam file INF perangkat non-PnP yang diinstalasi secara manual. Bagian ini menerangkan setting konfigurasi hardware default dari pabrikan, seperti port I/O, IRQ (jika ada), dan seterusnya.

DDInstall.LogConfigOverride

Bagian ini digunakan untuk membuat konfigurasi pengganti, yang mengambil alih kebutuhan resource hardware yang dilaporkan driver bus perangkat *Plug n Play*.

DDInstall.Interfaces

Jika driver mengeksport suatu fungsi class interface perangkat, akan menghasilkan class interface yang baru. Dekompresi data, file INF-nya bisa mempunyai bagian ini.

InterfaceInstall32

Jika komponen yang diinstalasi, seperti class driver baru, menyediakan satu atau lebih device interface classes baru ke komponen tingkat yang lebih tinggi, file INF-nya bisa berisi bagian ini. Dengan demikian, bagian ini bootstrap seperangkat interface device untuk class yang baru dengan mempersiapkan apapun yang dibutuhkan untuk menggunakan fungsionalitas yang disediakan oleh class interface.

DefaultInstall

DefaultInstall akan diakses jika user memilih memilih "Install" setelah

mengklik kanan file INF.

DefaultInstall.Services

Bagian ini ekuivalen dengan DDInstall.Services, dan digunakan bersama dengan DefaultInstall.

Strings

Bagian ini diperlukan oleh setiap file INF untuk membuat *%strkey%* yang ditentukan dalam INF. Pada semua INF yang disediakan sistem, Strings muncul di bagian akhir untuk mempermudah pemeliharaan dan lokalisasi.

Beberapa bagian yang disebutkan di sini, khususnya dengan Install dalam nama mereka, bisa berisi perintah yang mengacu ke bagian tambahan yang dibuat *writer* INF. Masing-masing perintah melakukan operasi tertentu pada waktu instalasi sesuai yang ditentukan oleh *writer* INF.

Kumpulan entri dan perintah untuk setiap bagian pada daftar sebelumnya adalah bergantung kepada tiap bagian dan ditampilkan dalam *syntax* formal dari referensi untuk masing-masing bagian tersebut. Entri dan perintah tambahan di dalam masing-masing bagian tersebut ditampilkan dalam kurung kotak biasa (tidak dicetak tebal) seperti contoh berikut:

```
[Version]
...
[Provider=%INF-creator%]
...
```

Entri Provider pada bagian [Version] adalah opsional yang tidak harus ada dalam setiap file INF.

```

wordpad - Notepad
File Edit Format View Help
WORDPAD.INF
This is the Setup information file to install wordpad
as an optional component.
Copyright (c) 1993-1997 Microsoft Corporation

[version]
Signature="SCHICAGO"
ClassGUID={00000000-0000-0000-0000-000000000000}
LayoutFile=layout.inf

[DestinationFns]
WordPadCopyFiles = 16422,%ACCESSOR% ; DIRID_PROGRAM_FILES\Program Files\Windows NT\Accessories
WordPadCopyFiles_HELP = 18 ; LOID_HELP
WordPadFilesOld = 16422,%ACCESSOR% ; DIRID_PROGRAM_FILES\Program Files\Windows NT\Accessories
WriteCopyFiles = 11 ; LOID_SYSTEM
WriteFilesOld = 11 ; LOID_SYSTEM

[Optional Components]
MSWordPad

[MSWordPad]
OptionDesc = %MSWORDPADOPT_DESC%
Tip = %MSWORDPADOPT_TIP%
IconIndex = 39 ; Windows Logo mini-icon for dialogs
Parent = AccessStop
CopyFiles = wordPadCopyFiles, wordPadCopyFiles_HELP, writeCopyFiles
DelFiles = wordPadFilesOld, writeFilesOld
AddReg = wordPadReg
ProfileItems = wordPadInstallItems, wordPadUninstallItems
Uninstall = MSWordPadUninstall
Modes = 0,1,2,3
SizeApproximation = 843776

[MSWordPadUninstall]
DelFiles = wordPadCopyFiles, wordPadCopyFiles_HELP, wordPadFilesOld, writeCopyFiles
UpdateInits = wordPadInits_remove
ProfileItems = wordPadUninstallItems, wordPadUninstallCommonItems
DelReg = wordPadReg

[DefaultInstall]
AddReg = wordPad.install.reg, wordPadReg

[wordPadCopyFiles]
wordpad.exe
msword6.wpc
msword6.wpc
write.wpc

```

Cara menghapus program Wordpad yang terdapat pada file wordpad.inf.

menemukan file bernama wordpad.inf. Di situ terdapat bagian bernama [MSWordPadUninstall], yang menangani penghapusan aplikasi. Jika Anda membaca semua perintah yang ada, di situ ditunjukkan bagaimana menghilangkan Wordpad secara manual (file dan entri registry yang dihapus, dan seterusnya).

Terlalu sulit? Tentu saja, dan juga benar-benar tidak perlu karena Windows mempunyai perintah yang akan menjalankan bagian file INF apa pun untuk Anda. Pada kasus ini, klik Start, Run, dan masukkan `RunDll32 advpack.dll, LaunchINFSection \Windows\INF\wordpad.inf, MSWordPadUninstall`. Ingin mengembalikan Wordpad? Klik kanan wordpad.inf dan pilih Install.

Mengatur Jaringan

Bermain-main dengan file INF bisa berguna khususnya pada waktu mengatur jaringan. Jika Anda menggunakan Firewall Windows XP SP2, misalnya, maka penting untuk memastikan semuanya menggunakan aturan yang sama—adalah mimpi buruk jika itu berarti harus mengatur setiap sistem secara individu. Untungnya tidak, karena Microsoft menggunakan file INF. Buka `\WINDOWS\inf\netfw.inf` untuk melihatnya sendiri. Ia berisi bagian untuk setiap profile hardware; [ICF.AddReg.DomainProfile] digunakan ketika PC Anda terhubung ke domain jaringan, [ICF.AddReg.Standard

Profile] digunakan jika tidak.

Sekarang yang perlu Anda lakukan adalah membuat entri registry yang diperlukan ke profile yang tepat.

Sebagai contoh, untuk men-*disable* semua koneksi incoming gunakan HKLM, "SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile", "DoNotAllowExceptions", 0x00010001, 1. Atau jika Anda tidak suka firewall, matikan saja dengan HKLM, "SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile", "EnableFirewall", 0x00010001, 0. Gunakan Yahoo! untuk mencari WFINF_Guide.doc untuk melihat daftar lengkap setting yang bisa Anda gunakan.

Ini hanyalah satu dari banyak cara untuk menggunakan file INF. Ingin mengetahui lebih banyak? Seperti biasa, Yahoo! adakah teman Anda: cari `RunDll32 advpack.dll, LaunchINFSection` Anda akan menemukan tip dalam mengatur sistem. ■

LEBIH LANJUT

<http://www.microsoft.com>

AUTORUN.INF

■ CD-ROM kali pertama diperkenalkan untuk mengganti sejumlah besar disket yang pada saat itu dibutuhkan untuk menginstalasi *software* seperti Microsoft Office. User harus memasukkan CD-ROM ke dalam drive dan kemudian menjalankan perintah, biasanya `setup.exe` atau `install.exe`, untuk memulai instalasi. Dengan diperkenalkannya Windows 95, sebuah fitur baru bernama AutoPlay memungkinkan program otomatis dijalankan dan dimaksudkan supaya CD lebih mudah digunakan. Fitur ini juga memungkinkan dijalkannya CD audio.

Perangkat untuk membuat CD pada awalnya sangat mahal, tetapi harga sekarang telah turun beberapa ratus ribu dan CD-ROM writer sering kali digunakan untuk membuat back-up atau untuk menyimpan file yang diakses secara langsung dari CD tanpa perlu diinstalasi ke harddisk. Di samping itu, CD digunakan sebagai media untuk menyimpan halaman web HTML dan file lain seperti *spreadsheet*, presentasi, audio, video, gambar, dan help (sebagai contoh `winhelp` Microsoft dan `HMTML Help`).

AutoPlay bekerja dengan melihat CD, atau CD-ROM, yang dimasukkan oleh user. Jika itu adalah CD audio maka akan dimainkan, tetapi jika itu adalah CD-ROM yang berisi file `autorun.inf` (pada root directory) maka instruksi yang ada di dalamnya akan dijalankan.

`Autorun.inf` hanya memperbolehkan program (file dengan ekstension `.exe` atau `.com`) yang dijalankan. AutoPlay tidak dimaksudkan untuk menjalankan file lain, seperti `.htm`. AutoPlay juga hanya dimaksudkan untuk bekerja dengan CD-ROM tetapi bisa dibuat supaya bekerja dengan media lain seperti disket dan drive Iomega Zip. File `autorun.inf` biasa untuk menginstalasi *software* ada di root directory dari CD dan berisi tiga baris (dalam format teks ASCII) berikut:

```

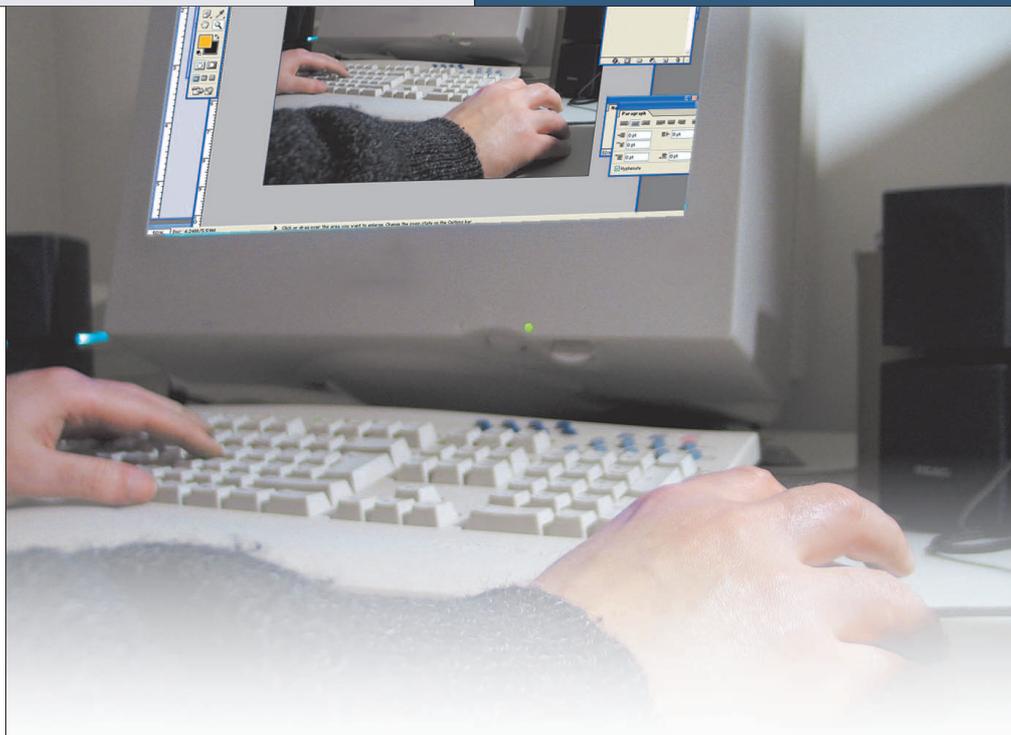
[autorun]
open=setup.exe
icon=setup.exe

```

Setup `.exe` terdapat pada root directory CD.

Batasi pengguna PC Anda dalam menjalankan dan menginstalasi aplikasi. Kita lihat bagaimana melakukan tindakan pencegahan.

Gunung Sarjono



Mengontrol Penggunaan Software

► Dengan adanya sejumlah *user* yang menggunakan PC milik Anda, Anda perlu memikirkan masalah keamanan. Anda juga perlu memastikan integritas keseluruhan sistem. Instalasi aplikasi dan penggunaannya, jika tidak dimonitor, bisa menyebabkan masalah. Pada Windows XP, ada dua jenis *user account*, "Computer Administrator" dan "Limited", yang membatasi apa yang bisa dan tidak bisa dilakukan oleh user. Dengan bantuan Registry, Anda bisa melakukan manajemen user yang selangkah lebih maju. Dengan mengubah *key* dan *value*, Anda bisa menentukan program apa yang bisa dijalankan pada sistem tersebut. Untuk PC rumahan, cara ini bisa digunakan oleh para orang tua yang ingin mengontrol penggunaan program *instant messaging*. Dari sudut pandang keamanan, cara ini bisa mencegah penggunaan program utility yang bisa mempengaruhi konfigurasi PC milik Anda.

Anda bisa membuat larangan supaya user tidak bisa menjalankan aplikasi dan file tertentu. Dengan menggunakan Registry Editor, cari HKEY_CURRENT_

USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer. Value yang akan Anda edit mungkin tidak ada, jadi buatlah dulu. Jika Anda menggunakan Windows XP atau 2000 klik kanan pada panel sebelah anan dan pilih New, DWORD Value lalu beri nama DisallowRun. Beri nilai 1 untuk meng-*enable* larangan aplikasi. Berikutnya, buat key baru HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun. Di dalam key ini, tentukan aplikasi yang tidak boleh dijalankan. Buat String Value yang berurutan untuk masing-masing aplikasi dengan *value* adalah file executable dari aplikasi yang bersangkutan. Sebagai contoh, jika Anda tidak mau MSN Messenger dijalankan maka untuk *value*-nya masukkan "msnmsgr.exe". Ulangi proses untuk masing-masing aplikasi selanjutnya.

Bagi yang menggunakan versi Windows yang lebih lama Anda bisa membuat larangan yang sama, tetapi dengan Registry value yang berbeda. Buka HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\

Policies\Explorer. Buat DWORD Value bernama RestrictRun dan beri nilai 1 untuk meng-*enable* larangan. Kemudian, buat key lagi, HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun, di mana aplikasi yang dilarang akan dimasukkan. Buat *String Value* dengan nomor yang berurutan dengan *value* file executable dari masing-masing aplikasi.

Jika menggunakan versi Windows yang lama Anda bisa mengedit Registry supaya aplikasi real-mode DOS tidak bisa dijalankan. Perubahan ini akan membuat program DOS tidak bisa dijalankan dari dalam interface Windows. Buka HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\WinOldApp dan buat DWORD Value bernama NoRealMode dengan *value* sama dengan 1 untuk meng-*enable* larangan.

Membatasi Startup

Pengaturan ini akan membuat sistem atau user tidak bisa menjalankan program *startup*, dengan mengubah instruksi pada Registry. Untuk melau-

kukan ini per user buka HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer. Buat empat DWORD Values sebagai berikut: DisableLocalMachineRun, DisableLocalMachineRunOnce, DisableCurrentUserRun dan DisableCurrentUserRunOnce. Masing-masing harus diberi nilai 1 untuk meng-enable larangan. Untuk meng-enable item startup Anda bisa menghapus DWORD Value tersebut atau ubah nilai mereka ke 0.

User bisa mencegah program startup dengan menahan tombol [Shift] pada waktu Windows di-load. Anda bisa men-disable-nya. Buka HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. Buat DWORD Value bernama IgnoreShiftOverride dan beri nilai 1.

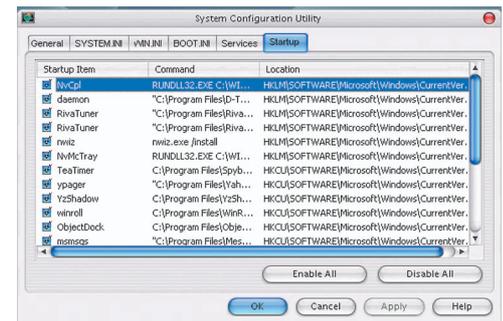
User bisa menghilangkan masalah dengan menggunakan *System Restore*, tetapi mengembalikan *setting* dengan menggunakan tool ini bisa menyebabkan dampak yang berlawanan bagi semua user PC. Untuk itu, Anda mung-

kin ingin mencegah user supaya tidak bisa menggunakan System Restore. Anda bisa mengedit Registry untuk men-disable System Restore, tetapi itu tidak mempengaruhi kemampuan sistem dalam membuat titik system restore.

Cari HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT. Klik kanan Window NT, pilih New, Key dan beri nama SystemRestore. Buat dua DWORD Value, pertama bernama DisableConfig. Beri nilai 1 untuk men-disable interface System Restore dan juga link ke System Restore pada System Properties. Terakhir, buat DWORD Value bernama DisableSR dan beri nilai 1 untuk menghilangkan shortcut System Restore pada Start menu.

Mencegah Program Supaya Tidak Bisa Dijalankan dari Help

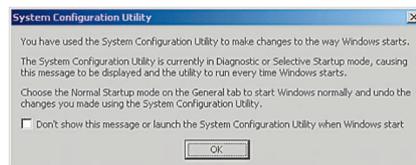
User bisa menjalankan aplikasi dari online Help, tetapi Anda dapat mencegahnya. *Setting* untuk policy ini terdapat pada HKEY_LOCAL_MACHINE\



System Configuration Utility.

SOFTWARE\Policies\Microsoft\Windows\. Buat key dengan nama System, dan kemudian buat *String Value* dengan nama *DisableInHelp*. Jika Anda meng-enable larangan tersebut maka Anda program tidak bisa dijalankan dari Help. Pada waktu meng-enable larangan, masukkan daftar program yang ingin Anda larang. Masukkan nama file executable masing-masing aplikasi, dipisah dengan koma. Sebagai contoh, "DisableInHelp" = "cmd.exe, command.com" akan membuat command prompt dan command tidak dapat dijalankan dari online Help. ■

MEN-DISABLE PROGRAM STARTUP



■ Salah satu cara untuk menyederhanakan konfigurasi adalah dengan men-disable program startup. Dengan menekan tombol [Shift] pada waktu logon, Anda bisa mencegah Windows XP supaya tidak menjalankan program atau shortcut pada folder berikut: systemdrive\Documents and Settings\Username\Start Menu\Programs\Startup, systemdrive\Documents and Settings\All Users\Start Menu\Programs\Startup, windir\Profiles\Username\Start Menu\Programs\Startup, windir\Profiles\All Users\Start Menu\Programs\Startup.

Untuk mendisable program atau shortcut, Anda harus menekan tombol [Shift] sampai icon desktop muncul. Menekan tombol [Shift] merupakan alternatif yang lebih baik dibanding

menghapus atau memindahkan program dan shortcut karena cara ini hanya mempengaruhi user yang bersangkutan.

System Configuration Utility

System Configuration Utility memungkinkan Anda men-disable satu atau beberapa program. Anda juga bisa men-disable suatu program tertentu sehingga tidak dapat menggunakan registry untuk menyimpan informasi. Sebagai contoh, pada komputer x86, Anda bisa menggunakan tool ini untuk men-disable program startup yang 16-bit.

Untuk men-disbale program menggunakan System Configuration Utility, ketik msconfig pada kotak dialog Run, dan kemudian klik OK. Untuk men-disable program, pilih tab General, klik Selective Startup, dan kemudian hilangkan tanda centang pada Process WIN.INI File dan Load Startup Items. Atau, untuk men-disable item tertentu, pilih tab Startup atau WIN.INI, dan kemudian hilangkan tanda centang

pada item yang ingin Anda disable. Anda juga bisa mengklik Disable All pada tab Startup dan WIN.INI untuk men-disable semua item pada masing-masing tab.

Jika Anda mengubah startup dengan menggunakan System Configuration Utility, Windows XP menampilkan pesan berikut pada waktu Anda log on: "You have used the System Configuration Utility to make temporary changes to some of your system settings. To return to normal operations, choose the Normal option on the General tab." Pesan dan System Configuration Utility akan terus muncul setiap kali Anda melakukan log on sampai Anda mengembalikan setting startup dengan mengklik Normal Startup di bagian Startup Selection pada tab General. Untuk mengubah setting secara permanen, Anda harus memindahkan atau menghapus shortcut startuo, mengubah setting Group Policy, atau meng-uninstall aplikasi tersebut.

MENGGUNAKAN REGISTRY UNTUK MENGUBAH TAMPILAN DAN MENINGKATKAN KEAMANAN DESKTOP

■ Dengan menggunakan *setting built-in* pada Windows, Anda bisa mengubah dan mempersonalisasi tampilan PC. Namun, Anda bisa lebih meningkatkan tampilan dan penggunaan sistem dengan mengubah Registry.

Menghilangkan My Computer

Dengan mengedit *key* dan membuat yang baru Anda tidak hanya meningkatkan keindahan Windows, tetapi juga mengubah fungsinya. Sebagai contoh, Anda bisa menghilangkan icon *My Computer* dari *desktop*. Ini memang bukan keamanan yang andal, tetapi cukup untuk mencegah user yang ingin tahu isi harddisk Anda. Perubahan ini juga akan menghilangkan *My Computer* dari Start menu. Cari `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\NonEnum`. Buat atau ubah `DWORD Value` bernama `{20D04FE0-3AEA-1069-A2D8-08002B30309D}` dan beri nilai 1 untuk membuat icon tidak terlihat.

Memperindah Desktop

Jika ingin mempunyai tampilan desktop yang lebih baik Anda bisa mengatur kedalaman warna yang digunakan untuk menampilkan icon. Buka `HKEY_CURRENT_USER\Control Panel\Desktop\WindowMetrics` dan edit `String Value` bernama `Shell Icon BPP`. Anda bisa mengubah nilainya sesuai dengan jumlah warna yang Anda inginkan untuk menampilkan icon. Sebagai contoh, nilai 4 untuk 16 warna, 8 untuk 256 warna, 16 untuk 65536 warna dan 24 untuk 16,7 juta warna. Masih pada lokasi yang sama, edit atau buat `String Value` bernama `Shell Icon Size`. Nilai default-nya adalah 32: ini adalah ukuran icon dalam pixel. Tambahkan atau kurangi nilainya untuk mengubah ukuran icon desktop Anda.

Pada waktu melihat isi folder dalam *Thumbnails view*, Anda bisa mengubah ukuran icon thumbnail dari `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\`. Edit atau buat `DWORD Value` bernama

`ThumbnailSize` dan buat nilainya sesuai dengan ukuran (dalam pixel) icon thumbnail yang Anda inginkan. Anda juga bisa membuat `DWORD Value` bernama `ThumbnailQuality` untuk menentukan kualitas gambar thumbnail yang ditampilkan. Nilai default-nya adalah 90, tetapi nilainya bisa diubah antara 50 sampai 100.

Mengatur Icon

Registry memungkinkan Anda mengatur icon supaya tampil seperti yang Anda inginkan. Dari `HKEY_CURRENT_USER\Control Panel\Desktop\WindowMetrics` Anda bisa mengatur tampilan teks nama icon. Edit `String Value` bernama `IconTitleWrap` dan beri nilai 0 supaya nama tidak dipotong, tetapi muncul dalam satu baris. Ubah nilainya ke 1 supaya teks nama dipotong lagi.

Anda bisa mengubah desain yang digunakan oleh sebagian besar icon dengan mengklik-kanan dan memilih *Properties*. Namun, untuk Recycle Bin tidak ada opsi itu - Anda perlu mengedit Registry jika ingin mengubah tampilannya. Pertama buka `HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\DefaultIcon`. Di situ Anda akan melihat tiga nilai berbeda yang menunjukkan status Recycle Bin yaitu (Default), Empty dan Full. Nilai masing-masing perlu diubah ke lokasi file icon yang ingin Anda gunakan. Pada situs seperti iconarchive.com Anda bisa *download* icon secara gratis, atau membuat sendiri.

Pada waktu menginstalasi aplikasi baru pada Windows XP, aplikasi tersebut secara default disorot pada Start menu sehingga Anda bisa langsung menemukannya. Dengan mengedit Registry Anda bisa mengontrol efek tersebut dan memilih apakah ingin meng-*enable* atau *disable*. Buka `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced` dan buat atau edit `DWORD Value` bernama `Start_NotifyNewApps`, lalu beri nilai 1 untuk meng-*enable* penyorotan. Anda juga bisa mengedit Registry untuk menyorot sebagian program yang terinstalasi seperti Microsoft Office. Buka

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer` dan edit atau buat `DWORD Value` bernama `GreyMSIAds`. Beri nilai 1 supaya penyorotan dilakukan.

Secara default program yang baru terinstalasi tidak akan diurutkan secara abjad, meskipun Anda bisa saja mengklik kanan menu dan memilih *Sort by Name*. Supaya menu selalu muncul secara berurutan buka `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder`, lalu hapus *key Start Menu*. Perubahan ini akan dirasakan pada waktu berikutnya Anda merestart sistem

Menghilangkan Daftar Program dan Nama User

Start menu pada XP sedikit berbeda dengan Windows versi sebelumnya karena jumlah elemen yang dapat diubah lebih banyak. Sebagai contoh, ada daftar shortcut program yang sering digunakan. Untuk menghilangkannya dari pandangan Anda bisa mengedit Registry pada `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`. Buat `DWORD Value` bernama `NoStartMenuPinnedList` dan beri nilai 1 supaya tidak ditampilkan. Untuk menampilkan daftar kembali ubah nilainya ke 0.

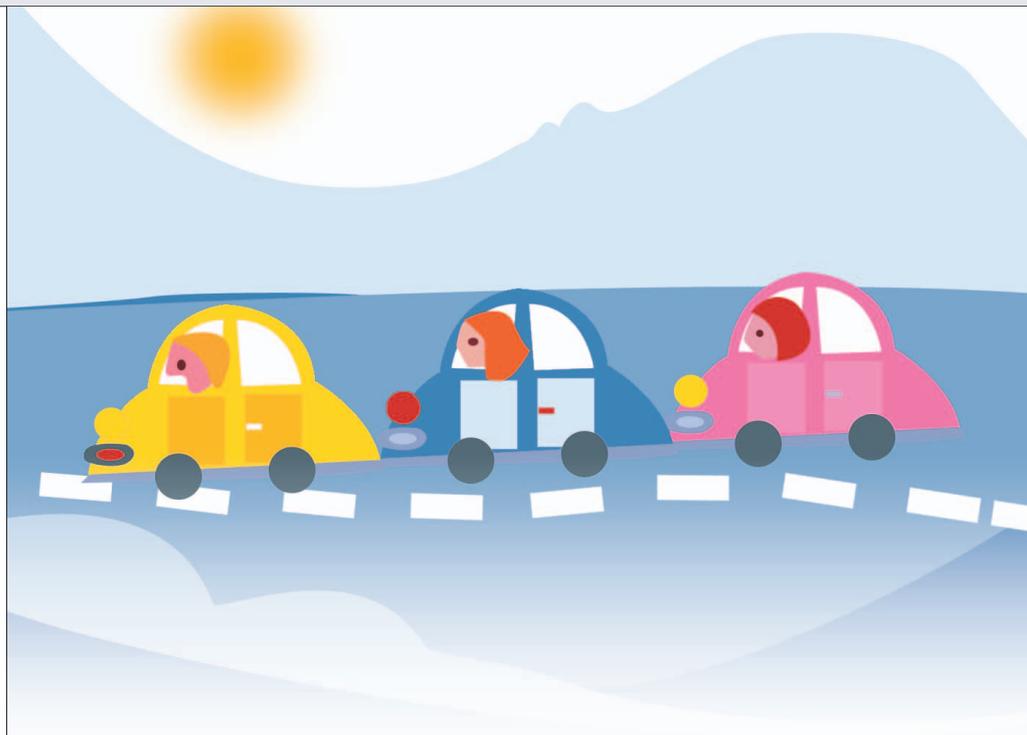
Item lain yang dapat dihilangkan dari pandangan adalah nama user di bagian atas Start menu. Perubahan Registry berguna terutama jika Anda menggunakan theme dan ingin interface nampak sebisa mungkin non-standar. Untuk melakukannya buat *key* baru `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer`. Buat `DWORD Value` bernama `NoUserNameInStartMenu` dan beri nilai 1 untuk memastikan nama user tetap tersembunyi.

LEBIH LANJUT

- <http://www.iconarchive.com/>

Mengatasi kemacetan harus dilakukan dua pihak! Pemerintah menyediakan fasilitas, warga memberikan kesadarannya. Dibantu dengan teknologi yang tepat, setidaknya kemacetan dapat menjadi sesuatu yang jarang ditemui.

Fadilla Mutiarawati



Mengurangi Kemacetan dengan Teknologi yang Tepat

► Bagi Anda di Jakarta, kemacetan lalu-lintas sudah menjadi hal yang biasa. Uniknya, tidak hanya jalan umum saja yang mengalami kemacetan. Jalan tol =jalan bebas hambatan di Jakarta juga ikut mengalami kemacetan. Padahal biaya masuk jalan tol dari tahun ke tahun selalu saja mengalami kenaikan.

Semakin tua usia kota Jakarta, tidak membuat kemacetan semakin dapat teratasi. Justru sebaliknya, di usianya yang semakin matang, Jakarta cenderung bertambah macet saja. Hal ini tentu saja menjadi dilema bagi seluruh warga kota. Karena kemacetan telah memberikan banyak kerugian. Jarak tempuh menjadi jauh lebih panjang dari seharusnya. Terbuangnya waktu bukan satu-satunya kerugian yang harus ditanggung oleh warga, masih banyak hal lain yang tidak kalah merugikannya. Jumlah kendaraan yang terlalu banyak menumpuk di satu titik telah menyebabkan tingkat polusi di titik tersebut meningkat drastis. Belum lagi kerugian material yang ditimbulkan.

Untuk dapat bertahan di kemacetan yang panjang, sebuah kendaraan membutuhkan bahan bakar yang lebih banyak. Ini artinya biaya yang dibutuhkan untuk mengoperasikan sebuah kendaraan di Jakarta dapat lebih mahal. Penggunaan bahan bakar yang boros juga dapat membuat persediaan bahan bakar berkurang.

Sebenarnya, pemerintah sudah menempuh beberapa jalan keluar untuk mengatasi masalah lalu-lintas. Namun, belum ada yang menyelesaikan masalah. Kepadatan terus saja terjadi, bahkan di hari libur (Sabtu-Minggu) sekalipun, kemacetan sudah dapat ditemui.

Terkadang kepadatan lalu-lintas diikuti dengan sikap tidak disiplin pengemudi sehingga membuat kepadatan menjadi semakin tidak terkontrol, seperti yang sering terjadi di perempatan lampu merah. Kebiasaan saling serobot dapat menyebabkan sebuah perempatan menjadi penuh, tidak dapat bergerak. Kalau sudah hal ini terjadi, maka satu-satunya yang dibutuhkan adalah peran polisi lalu-

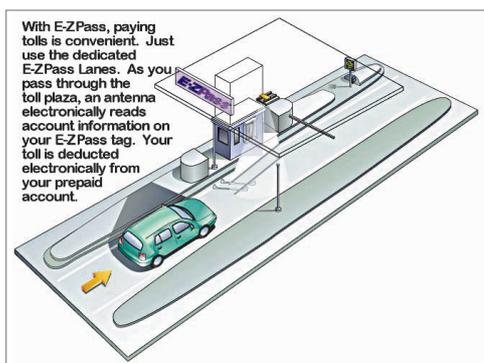
lintas. Namun untuk menuju lokasi sendiri, seorang polantas juga terkadang menemui kesulitan karena jalan sudah terlampau padat.

Sebenarnya, saat ini sudah ada beberapa teknologi yang dapat membantu masyarakat agar tidak selalu terjebak kemacetan. Atau setidaknya membantu menginformasikan kepada polisi untuk bertindak sebelum kemacetan terlanjur parah.

Bahkan dengan adanya teknologi RFID, kemacetan di jalan tol dapat dihindari. Dan dengan memanfaatkan teknologi GPS, Anda dapat memilih jalan yang lebih lancar. Namun selain membahas lebih lanjut mengenai manfaat RFID dengan GPS, masih ada teknologi lain yang lebih sederhana yang dapat dimanfaatkan.

Kamera CCTV

Keberadaan kamera CCTV dapat berfungsi dua arah, baik bagi polisi maupun masyarakat luas. CCTV tidak hanya dapat digunakan untuk jalanan yang



Pintu tol yang menggunakan E-ZPass.

rawan dengan kemacetan saja, tetapi juga jalanan lain yang rawan dengan kejahatan atau rawan kecelakaan.

Saat ini, teknologi CCTV yang digunakan untuk memantau keadaan lalu-lintas sudah dilakukan oleh sebuah perusahaan telekomunikasi sebagai salah satu tambahan pelayanannya. Hasil pengamatan ini dapat diakses oleh siapa saja yang menggunakan kartunya. Selain itu, salah satu stasiun TV swasta juga ada yang menggunakan CCTV untuk menginformasikan keadaan lalu-lintas kepada pemirsanya. Sayangnya, saat ini keberadaan CCTV belum luas. Hanya ada beberapa *spot* saja yang memiliki CCTV.

Bagi kepolisian, kamera CCTV dapat lebih luas lagi penerapannya. Tidak hanya dapat digunakan untuk mengetahui lokasi dan penyebab kemacetan saja. Sebagai pemantau kecelakaan, kamera CCTV dapat membantu polisi untuk mengetahui penyebab kecelakaan. Sedangkan untuk daerah yang rawan kejahatan, kamera CCTV dapat digunakan untuk membantu penyelidikan atau sebagai barang bukti.

Sayangnya untuk menjalankan fungsinya sebagai pemantau, kamera ini membutuhkan seorang operator, baik untuk memantau atau untuk hanya sekedar mengoperasikan. Sehingga bila jumlahnya semakin banyak tentu akan semakin banyak pula petugas yang harus dikerahkan. Kamera CCTV bukanlah sesuatu yang efisien, namun keberadaan cukup membantu.

Tambahkan Radar

Bila kamera CCTV ditambahkan dengan radar, maka akan lebih baik lagi. Masing masing saling memberikan informasi tentang kondisi sebuah jalan. Radar

berfungsi untuk memantau kecepatan laju kendaraan, sedangkan kamera akan dipergunakan bila radar menangkap sinyal yang kurang baik. Bila radar menangkap sebuah atau lebih kendaraan melaju kencang, maka polisi dapat mengetahui di mana dan apa yang sedang terjadi. Bila radar menangkap ada kendaraan yang berjalan lambat, artinya ada kemacetan. Maka petugas dapat langsung melihat CCTV untuk mengetahui lebih jelas mengenai kemacetan tersebut. Dan langsung dapat melakukan tindakan.

Radar tidak perlu diletakkan di semua jalan, namun setidaknya di jalan-jalan utama atau jalan tol, keberadaannya akan sangat membantu.

Radar tidak perlu selalu dipantau, bila ada sesuatu yang mencurigakan radar akan memberikan informasi, maka hanya pada saat itulah petugas beraksi. Bila radar tidak memberikan peringatan apapun, itu bertanda tidak ada yang perlu dikhawatirkan.

Di masa sekarang ini penggunaan radar lebih banyak dipergunakan untuk menangkap kendaraan yang melaju melebihi ambang batas kecepatan yang sudah ditetapkan. Radar juga kadang dipergunakan untuk sekedar menginformasikan pada pengguna jalan kecepatan yang tengah ditempuhnya. Radar banyak jenisnya, ada yang kecil ada juga yang besar. Yang besar umumnya dilengkapi dengan LED atau LCD untuk menampilkan

informasi kecepatan yang dihitung. Sedangkan ada juga radar yang hanya sekedar alat deteksi. Informasi yang diperolehnya tidak ditampilkan melainkan disimpan atau kemudian dikirimkan ke sebuah pusat pantau.

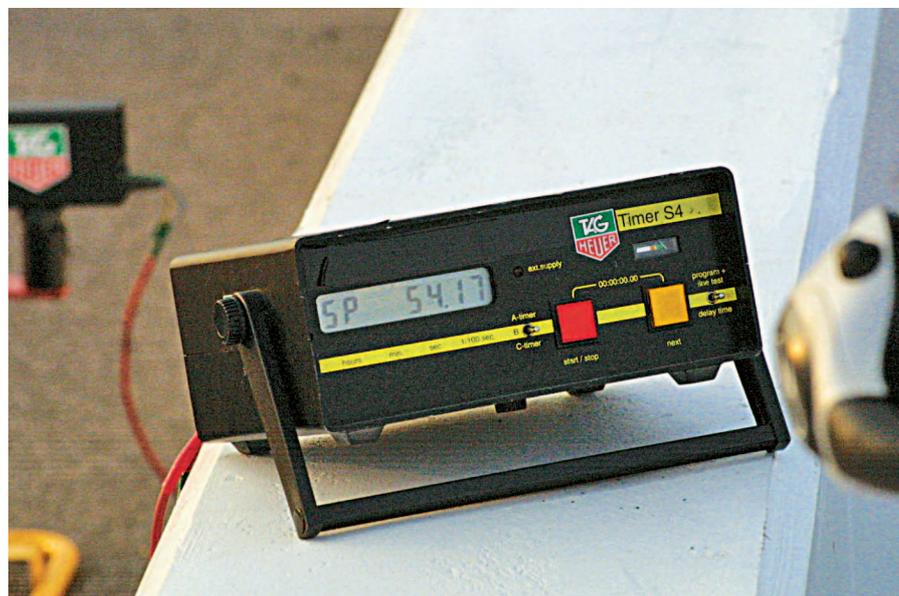
Global Positioning Service (GPS)

GPS bukanlah teknologi baru. Bahkan di Indonesia sendiri keberadaan GPS sudah semakin luas. Mulai dari peneliti, nelayan, sampai supir taksi sudah memanfaatkan teknologi ini.

Teknologi ini memang memiliki banyak kegunaan. Mulai dari mengetahui keberadaan ikan, alat bantu untuk membuat peta sampai alat untuk menghindari kemacetan.

Dengan GPS, seseorang dapat mengetahui keberadaannya di muka bumi. Oleh sebab itu, GPS banyak juga dipergunakan sebagai kompas atau alat penuntun jalan.

Saat ini, sudah banyak mobil mewah yang dilengkapi dengan GPS. Selain berfungsi sbegaaai penunjuk jalan, GPS pada kendaraan juga berfungsi sebagai bagian dari sistem keamanan. Bila sebuah mobil yang dilengkapi dengan GPS dicuri, maka polisi akan dengan mudah menemukannya kembali. Selama alat tersebut aktif pada kendaraan. Pantauan jumlah kendaraan pada sebuah ruas jalan juga dapat ditampilkan pada layar GPS sehingga seseorang yang



Salah satu bentuk radar kecepatan.



Salah stau jalan tol yang menggunakan RFID untuk gerbangnya.

menggunakan GPS dapat mengambil jalan alternatif. Hal ini tentu saja akan mudah mengurangi kemacetan. Sebab seseorang tidak akan melalui jalan yang sudah terlanjur padat.

Harga sebuah alat GPS samapai saat ini memang masih mahal, apa lagi untuk di Indonesia. Dan hal ini rasanya sangat sulit untuk jangka waktu yang lama. Mengingat pemilik kendaraan belum semuanya yang menyadari manfaat GPS. Atau bahkan sebagian orang masih menganggap fungsinya tidak sebanding dengan harga yang ditawarkan.

Tidak hanya jalan umum saja yang mengalami kemacetan di Jakarta, dengan sangat menyesal, jalan tol yang katanya bebas hambatan juga mengalami hal yang sama. Bedanya jika di jalan umum kemacetan sulit dihindari, sebaliknya di jalan tol seharusnya lebih mudah diatasi. Karena selain di jalan tol tidak ada lampu merah yang memberhentikan kendaraan di jalan tol juga tidak terdapat persimpangan. Kemacetan di jalan tol selain oleh kecelakaan atau perbaikan jalan hanya disebabkan oleh jumlah kendaraan yang terlalu banyak atau proses pembayaran yang mengantri terlalu panjang. Oleh sebab itu, teknologi yang dipergunakan juga sebenarnya dapat lebih sederhana.

Radio Frequency Identity (RFID)

Kali pertama RFID diperkenalkan, fungsi utamanya adalah menggantikan label barcode yang sampai saat ini masih dianggap tidak sempurna. Label barcode dapat saja hilang dan rusak sehingga tidak terbaca. Barcode juga membutuhkan sebuah alat baca yang harus dipakai dengan bertatap muka. Sehingga dengan label barcode pencurian masih saja dapat terjadi.

Berbeda dengan RFID. Ia tidak mudah rusak atau copot. Tidak hanya itu, RFID tidak memerlukan tatap muka dengan *reader*-nya untuk dapat terbaca. Sehingga fungsinya dapat juga sebagai bagian dari sistem keamanan.

RFID menggunakan gelombang radio. Hal ini memudahkan seseorang untuk membaca datanya. Bahkan dengan RFID, fungsi kasir dapat tergantikan secara otomatis. Misalnya saja seseorang yang berbelanja di sebuah supermarket hendak membayar belanjanya, maka ia cukup mendorong kereta belanjanya melewati sebuah celah yang dilengkapi dengan alat baca RFID. Alat baca akan langsung mendeteksi apa-apa saja yang telah dibelinya lalu menjumlah dan memotongkan langsung atau menagihkan langsung ke bank atau kartu kredit yang sudah lebih dulu didaftarkan.

Konsep kerja RFID di supermarket

dapat digunakan oleh jalan tol. Agar tidak terjadi kemacetan di pintu masuk. Petugas tol pun tidak perlu disibukkan dengan uang kembalian. Setiap orang atau kendaraan yang sudah jelas pemiliknya dapat dipasangkan RFID. Sehingga setiap kali kendaraan melintas, biayanya langsung dipotong dari tabungan.

Cara ini tidak hanya efektif mengurangi kemacetan di pintu masuk tol saja, tetapi juga dapat mengontrol jumlah kendaraan yang ada di dalam ruas jalan tersebut. Sehingga bila pada hasil pemantauan jumlah kendaraan sudah melebihi ambang batas, jalan tol dapat ditutup sementara.

Konsep ini dapat diterapkan pada jalan tol yang selalu mengalami kemacetan yang seharusnya tidak terjadi. Sesuai dengan fungsi jalan tol sendiri sebagai jalan bebas hambatan, bukan? Contohnya saja jalan tol Ciawi-Jakarta pada akhir pekan yang selalu mengantri. Atau keadaan jalan tol dalam kota yang kini selalu saja macet menyaingi jalan biasa di kanan kirinya.

RFID termasuk teknologi yang murah untuk digunakan dalam jalan tol. Tinggal kemauan para pengguna dan penyedia saja dalam mengubah sistem. Memang akan ada biaya tambahan mulai dari pembuatan kartu tol sampai membangun sistem di jalan tolnya sendiri. Tapi, biaya yang dikeluarkan sebenarnya tidak terlalu besar mengingat sebuah kartu RFID tidak terlalu mahal dan konstruksi pembacanya pun tidak terlalu rumit. Setidaknya biarpun membutuhkan biaya, hal ini dapat meningkatkan kenyamanan pengguna kendaraan. Dan bukankah meningkatkan mutu pelayanan adalah salah satu kewajiban pengusaha jasa TOL itu sendiri?

Sedangkan, nilai kesadaran sendiri harus timbul dari pengguna jalan. Bila memang kapasitas ruang dalam jalan tol sudah penuh, jangan memaksakan untuk tetap menggunakan jalan tol tersebut. Jika hal ini terjadi sia-sia saja sistem yang sudah dibuatkan.

Infra Merah

Sebenarnya untuk jalanan seperti jalan tol yang mengharuskan seseorang untuk membayar, lebih mudah dikontrol ketimbang jalan umum di mana setiap

orang bebas mengaksesnya. Intinya memang hanya di penghitungan jumlah kendaraan yang sedang menggunakan jalan. Jika pengelola jalan tol benar-benar ingin mengurangi kemacetan, maka hanya ada dua cara yang pertama menambah ruas jalan dan yang kedua membatasi jumlah kendaraan di dalamnya. Penambahan ruas jalan sangat sulit. Apalagi untuk jalan tol dalam kota. Oleh sebab itu, pembatasan jumlah kendaraan dapat menjadi salah satu alternatif.

Sayang *kan*, kadang pembatasan jumlah kendaraan jarang dipertimbangkan oleh pengelola jalan tol, karena hal ini berarti mengurangi pendapatan. Namun, apa yang akan membedakan jalan umum biasa dengan jalan tol jika kedua-duanya sama padatnya. Belum lagi untuk masuk jalan tol kini membutuhkan biaya yang semakin hari semakin mahal saja.

Bila mengontrol jalan tol dengan menggunakan RFID masih dianggap mahal, cobalah untuk menggunakan teknologi sinar infra merah. Dengan bantuan sinar infra merah, pengelola jalan tol tidak memerlukan konstruksi sistem yang rumit. Pada sistem di setiap pintu, hanya membutuhkan satu sistem infra merah lengkap dengan *counter* untuk menghitung. Setelah itu, hasilnya langsung masuk ke pusat kontrol dan dikombinasikan dengan jumlah kendaraan yang keluar masuk di pintu-pintu lainnya.

Teknologi ini juga dapat digunakan untuk sistem pembayaran. Namun, untuk memanfaatkan sinar infra merah sebagai bagian dari sistem pembayaran membutuhkan tambahan berupa kartu. Kartu ini dapat berupa kartu isi ulang yang dapat dibeli pengguna jalan tol di mana saja. Dengan kartu ini, pengguna tidak perlu lagi antri menunggu kembalian atau menunggu petugas selesai menghitung jumlah uang. Lebih cepat memang dibandingkan cara konvensional, namun bila dibandingkan dengan RFID tetantu lebih efektif dan efisien RFID.

Dengan sinar infra merah, seseorang harus berhadapan langsung dengan alat baca untuk dapat mengakses. Sedangkan dengan RFID yang menggunakan

gelombang radio, seorang pengguna tidak perlu berhenti. Cukup jalan secara perlahan, nanti alat baca akan menangkap gelombang radio secara otomatis.

E-ZPass

Pemanfaatan RFID untuk mengontrol penggunaan jalan tol sudah diterapkan di beberapa Negara dengan nama E-ZPass khususnya di Amerika Serikat. Seseorang dapat membeli *token* tarif tol dan isi token akan habis sesuai dengan penggunaannya. Penerapan E-ZPass memang belum sepenuhnya digunakan secara luas. Pada setiap jalan tol masih terdapat kombinasi secara manual, yaitu masih ada gerbang yang menggunakan sistem pembayaran kontan (*cash*).

Cara kerja E-ZPass:

1. Setiap kendaraan yang melewati gerbang akan diminta memperlambat kendaraannya (tidak perlu berhenti).
2. Kemudian label atau RFID yang ada di kendaraan akan mengirimkan sinyal kepada alat baca yang ada di gerbang tol.

3. Setelah itu, data yang ada di alat baca dengan bantuan antena diteruskan ke pusat data.
4. Data yang telah ada kemudian diproses, diperiksa dalam waktu singkat. Jika ternyata si pemilik kendaraan masih memiliki token, maka ia boleh melewati gerbang tol. Jika tidak melalui bantuan sebuah rambu, ia akan diminta berhenti untuk membayar token-nya.

Cukup sederhana, bukan? Jika hal ini diterapkan secara keseluruhan, maka antrian dalam jalan tol tentu akan sangat berkurang.

Setiap teknologi memang masih memiliki kekurangannya. Oleh sebab itu, peran serta manusia baik sebagai pengontrol maupun pengguna harus mahir menggunakan teknologi tersebut. Atau setidaknya, manusianya sendiri mau berkesadaran agar menggunakannya dengan baik dan benar. ■

LEBIH LANJUT

● www.ettm.com

KEMACETAN MASALAH BERSAMA

■ Kemacetan lalu-lintas tidak hanya salah pembangun jalan dalam hal ini pemerintah dan swasta (khusus jalan tol). Tetapi, juga masalah seluruh bangsa yang menggunakan jalan. Jalan dibangun untuk memudahkan seseorang menuju tempat tujuan. Namun, saat ini jalan yang ada sudah jauh melebihi dayaampungnya.

Oleh sebab itu, pertumbuhan jumlah kendaraan yang tidak terkontrol juga dapat menyebabkan kemacetan lalu-lintas. Sehingga dapat ditarik kesimpulan bahwa untuk menyelesaikan kemacetan lalu-lintas pemerintah tidak hanya harus melakukan pelebaran jalan. Namun, juga harus memberikan penyadaran pada masyarakat serta memperketat regulasi berkendaraan.

Mengapa harus demikian? Hal ini tentu saja untuk kepentingan hajat hidup orang banyak bukan hanya segelintir orang saja. Sebagian besar yang mampu membeli kendaraan tentu saja warga kelas menengah ke atas. Padahal di lain pihak yang dirugikan terhadap kemacetan tidak hanya kalangan atas, melainkan juga kalangan bawah yang masih mengandalkan kendaraan umum. Baik untuk bekerja, belajar, bersosialisasi, atau bahkan ketika keadaan darurat seperti ke rumah sakit atau kecelakaan.

Dengan lapangnya jalan, tidak hanya lajur lalu-lintas saja yang akan berjalan lancar, laju ekonomi pun akan lebih baik. Karena tidak ada waktu yang terbuang sia-sia di jalan.

Untuk mengentaskan masalah kemacetan lalu-lintas yang dibutuhkan tidak hanya kesadaran penyedia jalan saja, melainkan rasa tenggang rasa masyarakat terhadap hajat hidup orang banyak juga perlu dikembangkan. Sebaik apapun teknologi yang disediakan, jika belum ada kesadaran bersama, maka persoalan ini tidak akan selesai.

“Black box” juri kunci yang selalu dicari pada saat kecelakaan pesawat terjadi. Tidak sesuai dengan namanya yang berarti “kotak hitam”, black box tidak selalu berwarna hitam dan sama sekali tidak ada kaitannya dengan dunia magis.

Fadilla Mutiarawati



Black Box, Kunci Jawaban yang Sangat Canggih

► Setiap terjadi kecelakaan pesawat terbang di manapun kapanpun, para penyelidik selalu mencari sebuah komponen yang dinamakan “black box”. Penemuan komponen tersebut diharapkan dapat menjawab pertanyaan apa saja yang menyebabkan pesawat berada dalam kondisi naas.

Black box atau kotak hitam tidak ada sangkut pautnya dengan dunia magis. Komponen tersebut juga bukan merupakan benda ajaib, melainkan sebuah alat dokumentasi yang menyimpan semua data kondisi pesawat mulai dari awal penerbangan sampai terjadinya kecelakaan.

Kotak hitam sendiri tidak selalu berbentuk kotak persegi panjang dan berwarna hitam. Tapi sangat bervariasi, misalnya berwarna merah dengan bentuk yang tidak kotak persegi panjang. Penamaan ini muncul karena komponen tersebut seperti layaknya sebuah kotak ajaib yang mampu menyimpan semua informasi penting

penerbangan. Sehingga sebab-sebab sebuah kecelakaan dapat diketahui dengan lebih mudah.

Menemukan kotak hitam dalam sebuah kecelakaan pesawat tidak selalu menjadi pekerjaan yang mudah. Kadang kotak pesawat sulit ditentukan lokasinya. Dengan alasan inilah, oleh sebab itu keberadaan kotak hitam terus dikembangkan. Saat ini tidak hanya semakin banyak data yang dapat disimpan oleh kotak hitam, tetapi juga mulai dilengkapi dengan perangkat navigasi yang membuatnya lebih mudah ditemukan.

Tidak hanya itu saja, manfaatnya kini tidak hanya dirasakan oleh penyedia jasa penerbangan saja, melainkan juga jenis transportasi lain, seperti bus atau kapal laut.

Fungsi Kotak Hitam

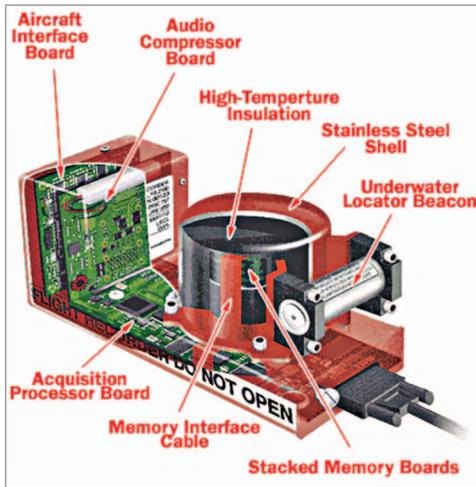
Sejenak sudah dapat Anda ketahui bahwa keberadaan kotak hitam adalah untuk membuat dokumentasi pener-

bangun sebuah pesawat atau apapun yang dimaksud dengan alat transportasi udara.

Dokumentasi apa saja yang dapat disimpan oleh sebuah kotak hitam. Dua jenis data yang paling penting adalah rekaman komunikasi pilot dan co-pilot dan data teknis penerbangan, seperti ketinggian, kecepatan pesawat, tekanan udara, dan masih banyak lagi. Data teknis memiliki sebutan *Flight Data Recorder (FDR)*, dan data rekaman suara



Kotak hitam dalam sebuah pesawat.



Bagian-bagian dalam kotak hitam.

pembicaraan radio dinamakan *Cockpit Voice Recorder (CVR)*.

Data dalam kotak hitam ini nantinya sangat diperlukan untuk kepentingan penyelidikan jika pesawat atau alat transportasi udara tersebut kecelakaan. Sebab pada kecelakaan pesawat pelacakan sebab dan akibat kecelakaan sulit sekali dilacak (banyak saksi yang meninggal dunia). Oleh sebab itu, keberadaan dokumentasi yang tidak mengandalkan campur tangan manusia sangat diperlukan.

Ataupun bila ternyata memang bukan untuk mengetahui penyebab terjadinya kecelakaan, keberadaan kotak hitam juga dapat menginformasikan hal-hal penting lainnya untuk kepentingan evaluasi.

Kotak hitam mulai dipergunakan sejak perang dunia kedua. Awalnya belum menggunakan media pita magnetik. Baru pada tahun 1990, pita magnetik mulai dipergunakan untuk penyimpanan data.

Namun, sekarang medianya juga telah berkembang. Tidak lagi pita magnetik yang digunakan melainkan bahan yang disebut *solid state*. Solid state adalah ruang penyimpanan yang tidak memiliki komponen bergerak. Solid State yang digunakan oleh kotak hitam sama dengan media penyimpanan yang digunakan pada MP3 player Anda ataupun kamera. Hanya saja dengan ruang atau kapasitas yang sangat besar. Dengan solid state, kemungkinan adanya kerusakan dapat diminimalkan. Karena data akan lebih aman dari guncangan

dan panas dibandingkan dengan pita magnetik.

Untuk mengumpulkan data, sebuah kotak hitam banyak memanfaatkan kerja sensor-sensor yang dipasang khusus di pesawat. Keberadaan sensor-sensor ini memiliki tugas yang beragam. Mulai dari sensor ketinggian untuk mengetahui ketinggian pesawat. Sensor akselerasi, temperatur luar dan dalam, kecepatan, tekanan, performa mesin, dan masih banyak lagi. Bahkan dapat mencapai 500 lebih parameter dapat dicatat oleh kotak hitam dalam sekali penerbangan. Panjangnya data yang akan tersimpan cukup bervariasi. Bila menggunakan teknologi solid state, data yang disimpan dapat mencapai 24 jam waktu penerbangan untuk data teknis dan dua jam untuk data rekaman suara. Semakin banyak data yang mampu disimpan oleh kotak hitam, akan sangat membantu penyelidikan sebab kecelakaan di kemudian hari. Baik jika terjadi sebuah kecelakaan besar atau hanya sekadar untuk evaluasi.

Mengapa dua jam saja? Karena pembicaraan atau komunikasi selama penerbangan memang tidak berlangsung dengan non-stop. Oleh sebab itu, alat rekam tidak perlu mendukung waktu yang sama dengan jam terbang. Alat rekam ini umumnya dilengkapi dengan sebuah sensor juga, yaitu sensor suara. Sensor suara hanya akan mengaktifkan fitur perekaman pada saat terdeteksi memang ada suara atau komunikasi terjadi. Jika komunikasi hanya berada dalam keadaan *stand by* atau tidak aktif, maka tidak akan ada data atau suara yang direkam.

Selain pembicaraan yang dilakukan oleh pilot, ada tiga mikrofon lain yang juga digunakan sebagai sumber suara, yaitu headset Co-Pilot, headset crew



Kotak hitam tidak selalu berwarna hitam.

ketiga (jika ada) dan satu lagi mikrofon diletakkan dekat cockpit yang dapat digunakan juga untuk mendengarkan atmosfer ruangan. Sehingga tidak hanya dapat mengetahui apa saja yang sedang disampaikan oleh pilot, tetapi juga dapat menangkap suasana yang sedang terjadi pada ruangan tersebut. Sebelum kemudian suara-suara ini berubah bentuk menjadi digital dan berada dalam kotak hitam. Terlebih dahulu suara ini melalui proses pre-amplifikasi yang dilakukan oleh *Associated control unit* yang ada pada cockpit.

Di Ujung Pesawat

Proses dokumentasi data, baik FDR maupun CVR tidak langsung dilakukan oleh kotak hitam, melainkan terlebih dahulu melewati sebuah perangkat yang terletak dalam *electronic equipment bay* (berfungsi sebagai perangkat perantara antara kotak hitam dengan data pesawat), yaitu *Flight Data Acquisition Unit (FDAU)*.

FDAU ini bertugas mengumpulkan semua data yang dikumpulkan oleh sensor, baru kemudian mengirimkannya ke dalam kotak hitam. FDAU terletak di bawah cockpit. Sedangkan kotak hitam sendiri umumnya diletakkan di ujung pesawat atau tepatnya pada buntut.

Lokasi ini dianggap paling aman untuk menyimpan kotak hitam. Karena umumnya pada setiap kecelakaan pesawat, bagian belakang atau ujung adalah bagian yang paling minim terkena dampaknya.

Peletakan kotak hitam biasanya dilakukan oleh perusahaan pesawat terbang yang membangun pesawat tersebut. Kotak hitam akan diletakkan sangat berdekatan dengan buntut pesawat.



Alat pembaca data pada kotak hitam.

Oranye

Tidak hanya letak saja yang diperhatikan dalam memudahkan investigasi sebuah kecelakaan. Selain keselamatan kotak hitam itu sendiri, menemukan keberadaannya juga sangat penting. Semakin

cepat ditemukan akan semakin baik. Faktor inilah yang membuat penampilan sebuah kotak hitam juga diperhitungkan. Kotak hitam tidak lagi dibuat dengan warna hitam sesuai dengan namanya, melainkan dengan warna-

SALAH SATU CONTOH REKAMAN YANG ADA DALAM SEBUAH KOTAK HITAM:

GIA 152:	Medan Approach, GIA152 passing 150.
MEDAN:	GIA 152 radar contact 43 miles. Descent to 3000ft for Runway 05, reduce speed to 220.
GIA 152:	Descend 3000for Runway 05. Reduce speed to 220 kts., GIA 152.
GIA 152:	Approach, GIA 152, request reason to reduce speed above 10000 to 220kts.
MEDAN:	OK Sir, your traffic departure sir, now start engine, release traffic departure at or before 27.
GIA 152:	152 like to maintain 210 kts... 250kts, and below 10000.
MEDAN:	OK, it's approved.
MNA 241:	MNA 241 passing 10000.
MEDAN:	MNA 241, your position now 11 miles on W-11. Contact 1212. Happy landing.
MNA 241:	Selamat siang. Terima kasih. (Good afternoon. Thank you)
MEDAN:	Any time.
GIA 152:	GIA 152; 3000
MEDAN:	GIA 152, maintain 3000ft for a while. Maintain heading Medan VOR. Traffic now still taxi Runway 23.
GIA 152:	Maintain 3000.
MEDAN:	Merpati 152, you turn left heading 240 vectoring for intercept ILS Runway 05 from right side. Traffic now rolling.
MEDAN:	GIA 152 do you read?
GIA 152:	GIA 152, say again?
MEDAN:	Turn left heading a 240, 235. Now vectoring for intercept ILS Runway 05.
GIA 152:	Roger, heading 235. GIA 152.
GIA 152:	GIA 152 heading 235. Confirm we cleared from a mountainous area?
MEDAN:	Affirm sir! Continue turn left on heading 215.
GIA 152:	On heading 215, GIA.
BOU 683:	Good afternoon, approach. BOU 683 departed left turn
MEDAN:	BOU 683 continue turn left on heading 120 initial 2000ft. -- line missing in transcript --
MEDAN:	GIA 152, turn right heading 046, report established on localizer.
GIA 152:	Turn right heading 040, GIA 152, check established.
MEDAN:	Turning right sir.
GIA 152:	Roger, 152.
MEDAN:	152, confirm you're making turning left now?
GIA 152:	We are turning right now.
MEDAN:	152 OK, you continue turning left now.
GIA 152:	A confirm turning left? We are starting turning right now.
MEDAN:	OK OK.
MEDAN:	GIA 152 continue turn right heading 015.
GIA 152:	Aaaaaa. Allahu-Akbar.

Transkrip pembicaraan (dalam bahasa Inggris) Pesawat Garuda Indonesia 152 dengan pesawat Airbus A300 sebelum mengalami kecelakaan di Medan pada 26 September 1997.

Sumber: aviation-safety.net/investigation/cvr/transcripts/atc_ga152.php.



ULB pada kotak hitam.

warna mencolok, seperti oranye atau merah. Hal ini akan memudahkan pencarian dngan kasat mata karena warna yang sangat mencolok.

Namun untuk menemukan kotak hitam, tidak hanya warna yang mambantu. Sebab kadang kecelakaan pesawat terjadi di tempat-tempat yang sulit dijangkau. Seperti di tengah laut, di belantara hutan, rawa-rawa, atau bahkan di perkotaan yang ramai. Oleh sebab itu, selain penampilan, kotak hitam juga dilengkapi dengan teknologi pelacak khusus.

Teknologi ini dinamakan *Underwater Locator Beacon* (ULB). Kehadiran ULB membantu pencarian yang harus dilakukan ditengah samudra. ULB bentuknya seperti silinder terletak di bagian depan sebuah kotak hitam. Fungsinya adalah sebagai pemancar jika kotak hitam terjatuh ke dasar laut dalam. Yang dipancarkan oleh ULB adalah sinyal ultrasonic yang tidak mampu didengar oleh telinga manusia. Namun, sinyal ini mampu ditangkap oleh radar sonar maupun alat pelacaknya.

Dengan frekuensi 37.5 KHz, ULB mampu memancarkan sinyal dari kealaman 4267m di bawah permukaan laut. ULB telah dilengkapi dengan baterai, sehingga mampu bertahan cukup lama (sekitar enam tahun). Namun, alat tersebut tidak langsung aktif ketika di pasang pada pesawat. Ada sebuah sensor khusus yang diletakkan pada ULB, agar dapat mengatur ULB untuk aktif hanya pada saat menyentuh air. Atau terjadi kontak dengan air. Bila tidak, maka ULB ini tidak akan memancarkan sinyal apapun. ULB sangat

rentan terhadap benturan yang terlalu kencang. Oleh sebab itu, ULB dapat rusak jika ternyata kecelakaan terjadi di daratan.

Bagian utama kotak hitam atau biasa yang disebut *Crash-Survivable memory units* (CSMUs). Komponen utama (memory unit) di mana data FDR dan CVR disimpan, merupakan bagian yang paling terlindungi. Ada tiga lapisan yang membalut bagian ini. Lapisan terdalam yang paling dekat dengan unit memory adalah lapisan aluminium. Lapisan kedua adalah satu inci dry silica yang melindungi memory unit dari panas. Dan yang ketiga adalah lapisan baja atau bahkan titanium setebal 0,25 inci. Ketiga lapisan ini akan melewati serangkaian tes kekuatan sehingga CSMUs mampu bertahan dalam segala macam medan. Dari benturan yang sangat kencang, suhu yang tinggi (1100 C), sampai tekanan yang sangat tinggi, ketahanan terhadap air laut yang cukup lama (30 hari) sampai kemampuannya bertahan bila mengalami bantingan dari tempat yang sangat tinggi.

Membaca Data

Seperti halnya membaca data dari Flash Disk. Membaca data pada kotak hitam tidak jauh berbeda. Yang justru menyulitkan bukan proses pembacaan data, namun menyelamatkan solid state memory itu sendiri yang kadang menjadi kendalanya. Sebab kerusakan yang sangat fatal akan sangat merepotkan. Komponen utama (memory) harus diangkat dan dibersihkan, lalu harus dipasangkan juga dengan perangkat interface yang baru setelah itu proses download pun dapat dilakukan.

Jika saja kerusakan yang terjadi tidak terlalu fatal, maka untuk membaca data pada kotak hitam hanya perlu menan-



Rekaman dalam kotak hitam yang berbentuk pita magnetik.



Salah satu contoh kotak hitam yang hancur.

capkan alat bacanya, dan data pun sudah dapat terbaca.

Lain halnya dengan data audio atau hasil rekaman. Setelah hasil rekaman berhasil diselamatkan. Proses interpretasinya dapat memakan waktu lama. Karena tidak hanya seorang saja yang akan diminta bantuannya, melainkan sebuah tim agar dapat memberikan hasil yang objektif. Anggota tim biasanya terdiri dari orang-orang penerbangan sendiri maupun dari penyelidik.

Kadang banyak masyarakat yang bertanya-tanya mengapa lama sekali proses yang dilakukan untuk mengetahui mengapa sebuah pesawat mengalami kecelakaan. Namun jika sudah memahami seperti apa kotak hitam yang sebenarnya, rasanya pertanyaan ini sudah terjawab. Jangankan untuk mengetahui isinya, menemukan kotak hitam sendiri tidak selalu menjadi pekerjaan yang mudah. Apalagi jika kecelakaan terjadi pada lingkungan yang sangat ramai. Atau benturan yang terlalu keras, sehingga kotak hitam sulit ditemui. Dan untuk dapat menginterpretasikan juga membutuhkan waktu yang tidak sebentar.

Manfaat Lain

Di masa yang akan datang kotak hitam tidak hanya mampu melakukan dokumentasi data dan suara saja, tetapi juga video. Sehingga apapun yang terjadi dalam pesawat dapat terpantau. Tidak hanya suasana dalam ruang pilot saja, melainkan juga suasana dalam kabin penumpang dan crew.

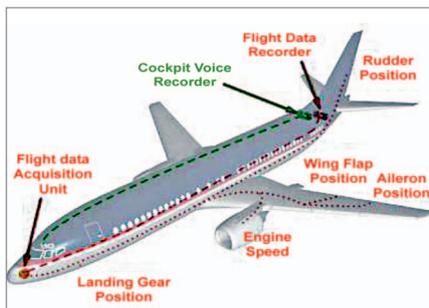
Hal ini tentu akan sangat berguna apalagi bila terjadi pembajakan dalam

pesawat yang mana mulai menjadi sebuah masalah yang sangat perlu dipertimbangkan. Khususnya untuk penerbangan-penerbangan besar.

Keberadaan kotak hitam untuk menyimpan dokumentasi penerbangan telah membantu para penyelidik untuk mengetahui apa yang menjadi penyebab terjadinya kecelakaan udara. Oleh sebab itu, keberadaan kotak hitam dicoba untuk juga diterapkan pada jenis kendaraan lain. Tentu saja dengan tujuan yang sama juga.

Salah satu bentuk kendaraan yang rencananya juga akan memanfaatkan keberadaan kotak hitam adalah kendaraan darat. Seperti mobil, bus, dan kereta. Dengan tujuan yang sama, yaitu untuk mengetahui apa yang menjadi penyebab jika kecelakaan terjadi. Tentu saja hasil dokumentasi tersebut akan membuat kondisi transportasi menjadi lebih baik dari hari ke hari.

Dan ternyata tidak hanya kendaraan saja yang dapat menggunakan kotak hitam. Manusia pun sedang dipersiapkan kotak hitamnya tersendiri. Kotak hitam yang dinamakan SenseCam ini mampu bertahan selama 12 jam. Dengan mengambil rekaman gambar sebanyak 2000 frame atau sebesar 128 MB. Sehingga apapun bentuk kecelakaan yang Anda alami, baik besar maupun kecil dapat diketahui atau diselidiki penyebabnya. Bagaimana siapakah Anda? ■



Letak kotak hitam dalam pesawat.

LEBIH LANJUT

- aviation-safety.net/
- www.l-3ar.com/

Untuk mengontrol lalu-lintas udara, radar saja tidak cukup. Mulai dari pengamatan cuaca yang harus jeli sampai penjadwalan menggunakan landasan, baik untuk lepas landas atau mendarat. Membutuhkan instrumen lain yang tidak kalah pentingnya.

Fadilla Mutiawarati



Lebih dari Sekadar Radar

► Beberapa tahun belakangan ini, di mana lebaran dan natal sering berdekatan, dunia transportasi kita selalu saja disibukkan. Hal ini dikarenakan membludaknya masyarakat yang melakukan perjalanan, baik perjalanan pulang kampung, berlibur, atau masih dalam tugas. Tentu saja keadaan ini tidak hanya menambah jadwal keberangkatan suatu armada, namun juga terjadinya peningkatan armada. Mulai dari armada udara, laut, dan darat.

Keramaian tersebut tidak hanya mendorong petugas untuk meningkatkan keamanan penumpang, melainkan juga meningkatkan keselamatan armada itu sendiri. Karena pada umumnya, membludaknya para penumpang di akhir tahun juga akan berdampak pada rawannya kecelakaan.

Kecelakaan yang paling sering terjadi adalah dikarenakan beban armada yang berlebihan atau sering disebut juga *overload*. Dan penyebab kedua yang sering muncul adalah padatnya arus lalu-lintas dapat juga membuat kecelakaan terjadi.

Untuk di darat, polisi sibuk melemburkan diri untuk ekstra perhatian pada masa-masa tersebut. Di laut, petugas

pelabuhan juga sibuk melakukan hal ini. Namun, untuk armada laut yang paling sering terjadi adalah kecelakaan karena beban yang berlebihan.

Di udara petugas bandara di samping harus ekstra teliti dan jeli, mereka juga harus sangat waspada. Karena landasan yang biasanya menampung penerbangan sedikit harus bertambah berkali lipat di akhir tahun.

Betapa sibuknya bandara. Jumlah pesawat bertambah banyak, di mana lintasan yang ada dalam jumlah yang tetap. Namun hal ini ternyata masih dapat terpantau, karena pada setiap bandara manapun ada yang dinamakan pusat kontrol. Sehingga arus lalu-lintas di bandara dapat berjalan dengan baik.

Pusat kontrol lalu-lintas udara tidak hanya mengontrol arus lalu-lintas pesawat saja, melainkan juga cuaca. Jika cuaca kurang baik, maka pesawat akan diminta untuk tidak *take off* dulu. Teknologi yang digunakan oleh pusat kontrol udara sangat banyak. Tidak hanya radar dan pemantau cuaca saja. Masih banyak hal lain yang sangat penting pada pengontrolan lalu-lintas udara.

Maraknya kecelakaan lalu-lintas udara belakangan ini juga membuat masyarakat bertanya-tanya tentang kinerja penerbangan kita, baik maskapai yang menyediakan transportasi tersebut maupun kinerja bandara tempat pesawat mendarat dan lepas landas. Sebenarnya seperti apa prosedur terbang itu? Mengapa kecelakaan sangat sering terjadi?

Prosedur Terbang

Banyak kecelakaan terjadi dikarenakan pilot atau maskapai penerbangan yang tidak taat pada prosedur penerbangan. Di samping memang kondisi pesawat yang kurang baik, prosedur terbang sangat penting. Karena di dalamnya selain berisi laporan tujuan juga



Seperti ini kiranya tampilan pada radar cockpit.



Suasana dalam TRACON.

terdapat laporan cuaca terakhir. Dan prosedur terbang erat kaitannya dengan pusat kontrol. Ini artinya, kelancaran penerbangan akan sangat bergantung kepada prosedur terbang tersebut. Seperti apa prosedur terbang?

Prosedur terbang yang harus dijalani oleh seorang pilot sangat banyak. Hal ini tidak hanya untuk menjamin kelancaran penerbangan, tetapi juga keamanan pesawat dan penumpang. Prosedur terbang harus ditaati oleh maskapai, pilot, dan penumpang.

Prosedur terbang di seluruh dunia sama, kecuali prosedur terbang yang dimiliki oleh Singapore Airline. Prosedur terbang di Indonesia mengacu pada prosedur terbang yang dibuat oleh FAA (*Federal Aviation Administration*) di Amerika Serikat.

Untuk mengatur arus lalu-lintas udara, kontrol lalu-lintas dibagi atas lima divisi:

1. **Air Traffic Control System Command Center (ATCSCC):** Divisi ini mengamati semua arus lalu-lintas, cuaca sampai rute penerbangan yang berada dalam jangkauannya.
2. **Air Route Traffic Control Centers (ARTCC):** Divisi ini berada di setiap bandara untuk mengamati pesawat yang berada dalam jangkauan radarnya. Setiap pesawat yang terbang

akan berpindah dari satu ARTCC ke ARTCC lainnya.

3. **Terminal Radar Approach Control (TRACON):** Divisi ini memantau pesawat yang berada pada posisi menjauh dan mendekat pada bandara.
4. **Air Traffic Control Tower (ATCT):** Divisi ini yang memantau dan mengontrol pesawat selama di bandara serta pada saat lepas landas dan mendarat.
5. **Flight Service Station (FSS):** Ini adalah divisi terakhir tempat pusat informasi mengenai cuaca, jadwal, rute, dan *flight plan*. Semua pilot harus melapor ke sini sebelum terbang. Dan FSS jugalah yang akan menangani saat pesawat dalam keadaan darurat.

Masing-masing divisi memiliki tugasnya masing-masing. Dan masing-masing divisi memiliki perangkat sendiri-sendiri. Perangkat utama yang ada di setiap divisi adalah radar. Radar ini memiliki peran yang sangat penting. Oleh sebab itu, pada saat sebuah pesawat terbang, keberadaannya tidak pernah lepas dari pantauan radar yang satu ke radar berikutnya. Bahkan dalam pesawat sendiri juga terdapat radar untuk memantau ruang angkasa di sekitarnya.

TMA Software

Untuk membantu pusat kontrol dalam menentukan jadwal pendaratan pesawat, NASA bersama FAA mengembangkan sebuah aplikasi yang dinamakan *Traffic Management Advisor* (TMA). Dalam menentukan di mana dan kapan sebuah pesawat mendarat, TMA akan terlebih dahulu melihat data dan memperhitungkan kemampuan serta kondisi angin di sekitar bandara.

Tujuan dari aplikasi ini untuk mengatur waktu yang tepat dan landasan yang baik untuk pendaratan. Agar rute penerbangan dapat berjalan sesuai rencana.

FAST Software

Selain TMA, ada salah satu teknologi yang keberadaannya terus mengalami perkembangan, yaitu adanya perangkat lunak FAST. FAST yang juga dikembangkan oleh NASA merupakan singkatan dari *Final Approach Spacing Tool*. Aplikasi ini sendiri ada dua macam yang satu disebut pasif FAST yang satu lagi disebut Aktif FAST. Aplikasi ini berfungsi dalam membuat *flight plan* bagi pesawat yang akan landing.

Aplikasi ini membantu pesawat dalam memilih landasan untuk landing atau mendarat. Namun pilot bebas menerima atau menolaknya, tentu dengan pertimbangan teknis yang matang. Sebab dalam memberikan saran, aplikasi FAST telah mempertimbangkan ukuran pesawat, performa dan gerakan angin. Dalam membuat perhitungan, FAST juga mempertimbangkan *flight plan* yang sudah ada serta pengamatan pada radar.

Aplikasi FAST akan memperhitungkan dengan teliti apa yang disarankannya agar landasan tidak *overload*, dan pesawat tidak mengalami penundaan sama halnya seperti TMA. Namun FAST terus dikembangkan hingga kini ada yang namanya aktif FAST. Jika dengan pasif FAST fungsinya tidak jauh berbeda dengan TMA, yaitu menyarankan *runway landing* dan urutannya. Dengan aktif FAST pesawat memiliki data lain berupa *display heading*, kecepatan, serta saran putaran. ■

LEBIH LANJUT

- www.faa.gov